UNOFFICIAL CONSOLIDATION OF DIRECTIVE DI144-2007-08 OF 2012, DIRECTIVE DI144-2007-08(A) OF 2016 AND DIRECTIVE DI144-2007-08(B) OF 2016

DIRECTIVE DI144-2007-08 OF 2012, DIRECTIVE DI144-2007-08(A) OF 2016 AND DIRECTIVE DI144-2007-08(B) OF 2016 OF THE CYPRUS SECURITIES AND EXCHANGE COMMISSION FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

ORDER OF PARAGRAPHS

Directive for the Prevention of Money Laundering and Terrorist Financing

188(I)/2007

144(I)/2007

The Cyprus Securities and Exchange Commission, in accordance with the powers vested in it by virtue of section 59 of the Prevention and Suppression of Money Laundering Activities Law, section 20 of the Investment Services and Activities and Regulated Markets Law and for the purposes of harmonization with the actions of European Community titled:

Official Journal of the EE: L 309/15 of the 25th November 2005

(a) "Directive 2005/60/EC of the European Parliament and 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"· and

Official Journal of the EE: L 214/29 of the 4th August 2005

(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 customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis"·

issues the following Directive:

PART I

INTRODUCTORY PROVISIONS

Short title

1. This Directive will be cited as the Directive for the Prevention of Money Laundering and Terrorist Financing.

Definitions

2. For the purposes of this Directive, unless the context shall prescribe otherwise:

"board of directors" means the board of directors of the Financial Organisation;

64(I)/2001
157(I)/2002
71(I)/2004
187(I)/2004
44(I)/2007

"Commission" means the Cyprus Securities and Exchange Commission established and operating pursuant to the Cyprus Securities and Exchange Commission (Establishment and Responsibilities) Law;

"company" means a company of limited liability by shares, established under Company Law or a company established in another member state under the law applicable in its place of establishment or a company established under the Cooperative Societies Law;

"compliance officer" means the person referred to paragraph 9;

"MOKAS" means the Unit for Combating Money Laundering established according to section 54 of the Prevention and Suppression of Money Laundering Activities Law;

"Law" means the Prevention and Suppression of Money Laundering Activities Law;

"regulated market" has the meaning attributed to this term by section 2 of the Investment Services and Activities and Regulated Markets Law;

"Financial Organisation" means:

(a) the Cypriot Investment Firm or CIF, as defined in section 2 of the Investment Services and Activities and Regulated Markets Law;

(b) the third country Investment Firm, according to section 78 of the Investment Services and Activities and Regulated Markets Law; and

200(I)/2004

(c) the Management Company and the Investment Company as these are defined in section 2 of the Open-ended Undertakings for Collective Investments in Transferable Securities (UCITS) and Related Issues Law;

"money laundering and terrorist financing" means the money laundering offences and terrorist financing offences defined in section 2 of the Law.

Without prejudice of the abovementioned provisions, terms used in this Directive that are not interpreted differently shall have the meaning given to them by the Law.

Where in the present Directive reference is made to the Law, this includes the Regulatory Administrative Decisions issued thereof.

Scope

3. This Directive applies to all Financial Organisations.

Supervisory Authority for the application of the Directive

4. The Supervisory Authority for the purpose of application of the present Directive is the Commission, in accordance with section 59 of the Law and section 126 of the Investment Services and Activities and Regulated Markets Law.

PART II
FINANCIAL ORGANISATION'S OBLIGATIONS

Board of directors' responsibilities

5. The board of directors:

(a) Determines, records and approves the general policy principles of the Financial Organisation in relation to the prevention of money laundering and terrorist financing and communicates them to the compliance officer.

(b) Appoints a compliance officer and, where is necessary, assistant compliance officers and determines their duties and responsibilities, which are recorded in the risk management and procedures manual of paragraph 9(1)(c).

(c) Approves the risk management and procedures manual of paragraph 9(1)(c), which is communicated to all employees of the Financial Organisation, that manage, monitor or control in any way the customers' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined.

(d) Ensures that all requirements of the Law, especially article's 58, and of the present Directive are applied, and assures that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement.

(e) Assures that the compliance officer and his assistants and any other person who has been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, have complete and timely access to all data and information concerning customers' identity, transactions' documents and other relevant files and information maintained by the Financial Organisation so as to be fully facilitated in the effective execution of their duties.

(f) Ensures that all employees are aware of the person who has been assigned the duties of the compliance officer, as well as his assistants, to whom they report, according to paragraph 9(1)(e) any information concerning transactions and activities for which they have knowledge or suspicion that might be related to

money laundering and terrorist financing.

(g) Establishes a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the compliance officer, either directly or through his assistants and notifies accordingly the compliance officer for its explicit prescription in the risk management and procedures manual of paragraph 9(1)(c).

(h) Ensures that the compliance officer has sufficient resources, including competent staff and technological equipment, for the effective discharge of his duties.

(i) Assesses and approves the Annual Report of paragraph 10 and takes all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report.

Obligations of the internal audit department

6. The internal audit department of the Financial Organisation reviews and evaluates, at least on an annual basis, the appropriateness, effectiveness and adequacy of the policy, practices, measures, procedures and control mechanisms applied for the prevention of money laundering and terrorist financing. The findings and observations of the internal auditor are submitted, in a written report form, to the board of directors which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected. The minutes of the abovementioned decision of the board of directors and the

internal auditor's report are submitted to the Commission at the frequency specified in paragraph 9(4) of the Directive DI144-2007-01 of the Commission.

Κ.Δ.Π. 426/2007
2.11.2007

Customers' acceptance policy

7. (1) According to paragraph 9(1)(b), a clear customers' acceptance policy is developed and established, which is completely in line with the provisions of the Law and the present Directive. The customers' acceptance policy is prepared after detailed assessment of the risks faced by the Financial Organisation from its customers and/or their transactions and/or their countries of origin or operations, as these are stated in Part IV

(2) The customers' acceptance policy set in an explicit manner, at least the following:

(a) the criteria for accepting new customers;

(b) categories of customers who are not acceptable for establishing a business relationship or an execution of an occasional transaction;

(c) criteria for categorisation of customers on a risk basis in at least three categories:

i. low risk,
ii. normal risk,
iii. high risk.

(3) The customers' categories of subparagraph 2(b) and (c),

take into consideration factors such as the customer's background, type and nature of its business activities, its country of origin, the services and the financial instruments applied for, the anticipated level and nature of business transactions as well as the expected source and origin of funds.

PART III
COMPLIANCE OFFICER

Appointment of compliance officer-assistants of compliance officer (section 69 of the Law)

8. (1) According to paragraph 5(b) a compliance officer is appointed, who belongs to the management of the Financial Organisation so as to command the necessary authority.

(2) According to paragraph 5(b), where it is deemed necessary due to the volume and/or the geographic spread of the services/activities, assistants of the compliance officer are appointed, by geographical district or otherwise for the purpose of assisting the compliance officer and passing internal suspicion reports to him.

(3) The Financial Organisation communicates immediately to the Commission, the names and positions of the persons it appoints as compliance officer and assistants of the compliance officer.

Compliance officer's duties

9. (1) As a minimum, the compliance officer's duties include the following:

(a) Designs, based on the general policy principles of paragraph 5(a), the internal practice, measures,

procedures and controls relevant to the prevention of money laundering and terrorist financing, and describes and explicitly allocates the appropriateness and the limits of responsibility of each department that is involved in the abovementioned.

It is provided that, the above include measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for the purpose of money laundering and terrorist financing (e.g. services and transactions via the internet or the telephone), as well as measures so that the risk of money laundering and terrorist financing is appropriately considered and managed in the course of daily activities of the Financial Organisation with regard to the development of new products and possible changes in the Financial Organisation's economic profile (e.g. penetration into new markets).

(b) Develops and establishes the customers' acceptance policy, according to paragraph 7 and submits it to the board of directors for consideration and approval.

(c) Prepares a risk management and procedures manual regarding money laundering and terrorist financing. The said manual includes, inter alia, the details referred to in paragraphs 5(a), 5(g), 7, 9(1) and Parts IV, V, VI and VII.

(d) Monitors and assesses the correct and effective implementation of the policy, according to paragraph 5(a), the practices, measures, procedures and controls of point (a) and in general the implementation of the risk management and procedures manual of point (c). In this regard, applies appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Financial Organisation) which will provide him all the necessary information for assessing the level of compliance of the departments and employees of the Financial Organisation with the procedures and controls which are in force. In the event that he identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where deems necessary informs the board of directors.

(e) Receives information from the Financial Organisation's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information is received in a written report form (hereinafter to be referred to as "Internal Suspicion Report"), a specimen of such report is attached in the First Appendix.

First Appendix

(f) Evaluates and examines the information received as per point (e), by reference to other relevant information and discusses the circumstances of the case with the informer and, where appropriate, with the informer's

superiors. The evaluation of the information of point (e) is been done on a report (hereinafter to be referred to as "Internal Evaluation Report"), a specimen of which is attached in the Second Appendix.

Second Appendix

(g) If following the evaluation described in point (f), the compliance officer decides to notify MOKAS, then he completes a written report and submit it to MOKAS the soonest possible. A specimen of such report (hereinafter to be referred to as "Compliance Officer's Report to the Unit for Combating Money Laundering") is attached to the Third Appendix.

Third Appendix

It is provided that, after the submission of the compliance officer's report to MOKAS, the accounts involved and any other connected accounts, are closely monitored by the compliance officer and following any directions from MOKAS, thoroughly investigates and examines all the transactions of the accounts.

(h) If following the evaluation described in point (f) the compliance officer decides not to notify MOKAS, then he fully explains the reasons for such a decision on the "Internal Evaluation Report" which is attached in the Second Appendix.

(i) Acts as the first point of contact with MOKAS, upon commencement and during an investigation as a result of filing a report to MOKAS according to point (g).

(ι) Ensures the preparation and maintenance of the lists

of customers categorised following a risk based approach, according to paragraph 7(2), which contains, inter alia, the names of customers, their account number and the date of the commencement of the business relationship. Moreover, ensures the updating of the said lists with all new or existing customers, in the light of additional information obtained.

(j) Detects, records, and evaluates, at least on an annual basis, all risks arising from existing and new customers, new financial instruments and services and updates and amends the systems and procedures applied by the Financial Organisation for the effective management of the aforesaid risks.

(k) Evaluates the systems and procedures applied by a third person on whom the Financial Organisation relies for customer identification and due diligence purposes, according to paragraph 25 and point 4 of the Fourth Appendix, and approves the cooperation with it.

Fourth Appendix

(l) Ensures that the branches and subsidiaries of the Financial Organisation that operate in countries outside the European Economic Area, have taken all necessary measures for achieving full compliance with the provisions of the present Directive, in relation to customer identification, due diligence and record keeping procedures.

(m) Provides advice and guidance to the employees of the Financial Organisation on subjects related to money laundering and terrorist financing.

(n) Acquires the required knowledge and skills for the improvement of the appropriate procedures for recognising, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing.

(o) Determines the Financial Organisation's departments and employees that need further training and education for the purpose of preventing money laundering and terrorist financing and organises appropriate training sessions/seminars. In this regard, prepares and applies an annual staff training program, according to Part VIII. Assesses the adequacy of the education and training provided.

(p) Prepares correctly and submits timely to the Commission the monthly prevention statement of paragraph 11 and provides the necessary explanation to the appropriate employees of the Financial Organisation for its completion.

(q) Prepares the annual report according to paragraph 10.

(r) Responds to all requests and queries from MOKAS and the Commission, provides all requested information and fully cooperates with MOKAS and the

Commission.

(s) Maintains a registry which includes the reports of points (e), (f) and (g), and relevant statistical information (department that submitted the internal report, date of submission to the compliance officer, date of assessment, date of reporting to MOKAS), the evaluation reports of point (d) and all the documents that verify the accomplishment of his duties specified in the present subparagraph.

(2) During the execution of his duties and the control of the compliance of the Financial Organisation with the Law and the present Directive, the compliance officer obtains and utilises data, information and reports issued by international organizations, as these are stated in paragraph 17.

Compliance officer's annual report

10. (1) The Annual Report, prepared by the compliance officer according to paragraph 9(1)(q), is a significant tool for assessing the Financial Organisation's level of compliance with its obligations laid down in the Law and the present Directive.

(2) The Annual Report is prepared and submitted for approval to the board of directors, within two months from the end of each calendar year (the latest by the end of February).

(3) The Annual Report, after its approval by the board of directors, is submitted to the Commission together with the minutes of the meeting, during which the Annual Report has been discussed and approved. It is provided that the said

minutes include the measures decided for the correction of any weaknesses and/or deficiencies identified in the Annual Report and the implementation timeframe of these measures. These minutes and the Annual Report are submitted to the Commission within twenty days from the date of the relevant meeting, and not later than three months from the end of the calendar year.

(4) The Annual Report deals with money laundering and terrorist financing preventive issues pertaining to the year under review and, as a minimum, covers the following:

(a) Information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and the present Directive which took place during the year under review.

(b) Information on the inspections and reviews performed by the compliance officer, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Financial Organisation applies for the prevention of money laundering and terrorist financing. In this regard, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation.

(c) The number of internal suspicion reports submitted

by employees of the Financial Organisation to the compliance officer, according to paragraph 9(1)(e), and possible comments/observations thereon.

(d) The number of Reports submitted by the compliance officer to MOKAS, according to paragraph 9(1)(g) with information/details on the main reasons for suspicion and highlights of any particular trends.

(e) Information, details or observations regarding the communication with the employees on money laundering and terrorist financing preventive issues.

(f) Summary figures, on an annualised basis, of customers' total cash deposits in Euro and other currencies in excess of the set limit of 10.000 Euro (together with comparative figures for the previous year) as reported in the Monthly Prevention Statement of paragraph 11. Any comments on material changes observed compared with the previous year are also reported.

(g) Information on the policy, measures, practices, procedures and controls applied by the Financial Organisation in relation to high risk customers as well as the number and country of origin of high risk customers with whom a business relationship is established or an occasional transaction has been executed.

(h) Information on the systems and procedures applied by the Financial Organisation for the ongoing monitoring of customer accounts and transactions.

(i) Information on the measures taken for the compliance of branches and subsidiaries of the Financial Organisation, that operate in countries outside the European Economic Area, with the requirements of the present Directive in relation to customer identification, due diligence and record keeping procedures and comments/information on the level of their compliance with the said requirements.

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

(k) Information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants.

(l) Results of the assessment of the adequacy and effectiveness of staff training.

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

(n) Information on the structure and staffing of the department of the compliance officer as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

Monthly prevention statement

11. The compliance officer prepares and submits to the Commission, according to paragraph 9(1)(p), on a monthly basis, the Form 144-08-11 which includes details for the total cash deposits accepted by the Financial Organisation, the Internal Suspicions Reports, and the Compliance Officer's Reports to MOKAS, according to paragraphs 9(1)(e) and 9(1)(g), respectively. The completion of the Form provides the opportunity to the Financial Organisation initially to evaluate and, subsequently, to reinforce its systems of control and monitoring of its operations, for the purpose of early identification and detection of transactions in cash which may be unusual and/or carry enhanced risk of being involved in money laundering and terrorist financing operations. The said Form is completed and submitted to the Commission within fifteen (15) days from the end of each month.

PART IV
APPLICATION OF APPROPRIATE MEASURES AND PROCEDURES ON A RISK BASED APPROACH

Application of measures and procedures on a risk based approach

(section 61(2) of the Law)

12. (1) The Financial Organisation applies appropriate measures and procedures, on a risk based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher.

(2) A risk-based approach:

(a) recognises that the money laundering or terrorist financing threat varies across customers, countries, services and financial instruments;

(b) allows the board of directors to differentiate between customers of the Financial Organisation in a way that matches the risk of their particular business;

(c) allows the board of directors to apply its own approach in the formulation of policies, procedures and controls in response to the Financial Organisation's particular circumstances and characteristics;

(d) helps to produce a more cost effective system; and

(e) promotes the prioritisation of effort and actions of the Financial Organisation in response to the likelihood of money laundering or terrorist financing occurring through the use of services provided by the Financial Organisation.

(3) A risk-based approach involves specific measures and procedures in assessing the most cost effective and

proportionate way to manage the money laundering and terrorist financing risks faced by the Financial Organisation. Such measures and procedures are:

(a) identifying and assessing the money laundering and terrorist financing risks emanating from particular customers, financial instruments, services, and geographical areas of operation of the Financial Organisation and its customers;

(b) documenting in the risk management and procedures manual of paragraph 9(1)(c), the policies, measures, procedures and controls to ensure their uniform application across the Financial Organisation by persons specifically appointed for that purpose by the board of directors;

(c) managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;

(d) continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

Identification, recording and evaluation of risks

13. (1) According to paragraph 9(1)(j), the compliance officer has the responsibility to identify, record and evaluate all potential risks. The successful establishment of measures and procedures on a risk-based approach requires the clear communication of the measures and procedures that have

been decided across the Financial Organisation, along with robust mechanisms to ensure that these are implemented effectively, weaknesses are promptly identified and improvements are made wherever necessary.

(2) A risk-based approach involves the identification, recording and evaluation of the risks that have to be managed. The Financial Organisation assesses and evaluates the risk it faces, for usage of the services provided for the purpose of money laundering or terrorist financing. The particular circumstances of the Financial Organisation determine the suitable procedures and measures that need to be applied to counter and manage risk.

(3) In the cases where the services and the financial instruments that the Financial Organisation provides are relatively simple, involving relatively few customers, or customers with similar characteristics, then the Financial Organisation applies procedures that focus on those customers who fall outside the 'norm'.

(4) The identification, recording and evaluation of risk that the Financial Organisation face presupposes the finding of answers to the following questions:

(a) What risk is posed by the Financial Organisation's customers? For example:

i. complexity of ownership structure of legal persons,
ii. companies with bearer shares,

iii. companies incorporated in offshore centres,
iv. politically exposed persons,
v. customers engaged in transactions which involves significant amounts of cash,
vi. customers from high risk countries or from countries known for high level of corruption or organized crime or drug trafficking;

(b) What risk is posed by a customer's behaviour? For example:

i. customer transactions where there is no apparent legal financial/commercial rationale,
ii. situations where the origin of wealth and/or source of funds cannot be easily verified,
iii. unwillingness of customers to provide information on the beneficial owners of a legal person;

(c) How did the customer communicate the Financial Organisation? For example:

i. non face to face customer,
ii. customer introduced by a third person;

(d) What risk is posed by the services and financial instruments provided to the customer? For example:

i. services that allow payments to third persons,
ii. large cash deposits or withdrawals.

(5) The application of appropriate measures and the nature and extent of the procedures of a risk based approach depends on different parameters. Indicative parameters are the following:

(a) the scale and complexity of the services;

(b) geographical spread of the services and customers;

(c) the nature (e.g. non face to face customer) and economic profile of customers as well as of financial instruments and services offered;

(d) the distribution channels and practices of providing services;

(e) the volume and size of transactions;

(f) the degree of risk associated with each area of services;

(g) the country of origin and destination of customers' funds;

(h) deviations from the anticipated level of transactions;

(i) the nature of business transactions.

Design and implementation of measures and procedures to

14. (1) When the Financial Organisation identifies, according to paragraph 13, the risks it faces, then designs and implements

manage and mitigate the risks

the appropriate measures and procedures for the correct management and mitigation, which involve the verification of the customers identity, the collection of information for the construction of their economic profile and monitoring their transactions and activities.

(2) Taking into consideration the assessed risk, a Financial Organisation determines the type and extent of measures it adopts, to manage and mitigate the identified risks cost effectively. These measures and procedures may, for example, include:

(a) adaptation of the customer due diligence procedures in respect of customers in line with their assessed money laundering and terrorist financing risk;

(b) requiring the quality and extent of requisite identification data for each type of customer to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence);

(c) obtaining additional data and information from the customers, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk emanating from the particular business relationship or the occasional transaction; and

(d) on going monitoring of high risk customers' transactions and activities.

(3) The risk assessment and the implementation of the measures and procedures of subparagraph (2) result in the categorisation of customers according to paragraph 7(2)(c). The said categorisation is based on criteria which reflect the possible risk causes and each category is accompanied with the relevant due diligence procedures, regular monitoring and controls.

(4) The category of low risk customers, according to paragraph 7(2)(c)(i), includes the customers prescribed in section 63 of the Law.

(5) The category of high risk customers, according to paragraph 7(2)(c)(iii), includes the customers prescribed as high risk in section 64 of the Law and the Fourth Appendix as well as any other customer determined by the Financial Organisation itself to be classified as such.

(6) According to paragraph 9(1)(j), lists are prepared and maintained for the categories of customers, which contain, inter alia, the customers' names, account numbers, and date of commencement of business relationship. The said lists should be promptly updated with all new or existing customers that the Financial Organisation has determined, in the light of additional information received, that fall under the categories of paragraph 7(2)(c).

(7) The Financial Organisation is, at all times, in a position to demonstrate to the Commission that the extent of measures

and control procedures that applies are proportionate to the risk it faces for the use of services provided, for the purpose of money laundering or terrorist financing.

(8) In view of this, documenting the measures and procedures set out in subparagraphs 2-6 above will assist the Financial Organisation to prove:

(a) the ways used to identify, record and assess the risk of its services being used for money laundering or terrorist financing;

(b) how it has determined the introduction and implementation of specific measures and procedures for the management and mitigation of risks; and

(c) the methods applied for monitoring and improving, whenever deemed necessary, the specific measures, procedures and controls.

Monitoring and improving the measures and procedures

15. The Financial Organisation monitors and evaluates, on an on going basis, the effectiveness of the measures and procedures that have been introduced for compliance purposes with the present Part.

Dynamic risk management

16. Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Customers' activities change as well as the services and financial instruments provided by the Financial Organisation change. The same happens to the financial instruments and the transactions used for money laundering

or terrorist financing. The measures, the procedures and controls are kept under regular review so that risks resulting from changes in the characteristics of existing customers, new customers, services and financial instruments are managed and countered effectively.

Relevant international organisations

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

(a) FATF - www.fatf-gafi.org·

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

(c) the EU Common Foreign & Security Policy (CFSP)- http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm·

(d) the UN Security Council Sanctions Committees - www.un.org/sc/committees/·

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

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

PART V
CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES

Obligation for customer identification and due diligence procedures

(sections 60, 61 and 62 of the Law)

18. (1) In addition to the provisions of sections 60, 61 and 62 of the Law that refer to the obligation for customer identification and due diligence procedures, the Financial Organisation ensure that the customer identification records remain completely updated with all relevant identification data and information throughout the business relationship. The Financial Organisation examines and checks, on a regular basis, the validity and adequacy of the customer identification data and information it maintains, especially those concerning high risk customers. The procedures and controls of paragraph 9(1)(a) also determine the timeframe during which the regular review, examination and update of the customer identification is conducted. The outcome of the said review is recorded in a separate note/form which should be kept in the respective customer file.

(2) Despite the provisions of subparagraph (1) and taking into consideration the level of risk, if at any time during the business relationship, the Financial Organisation becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the customer, then takes all necessary action, by applying the customer identification and due diligence procedures

according to the Law and the present Directive, to collect the missing data and information, the soonest possible, so as to identify the customer and update and complete the customer's economic profile.

(3) In addition to the provisions of subparagraph (1) and (2), the Financial Organisation checks the adequacy of the data and information of the customer's identity and economic profile, whenever one of the following events or incidents occurs:

(a) an important transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the economic profile of the customer;

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

i. change of directors/secretary,
ii. change of registered shareholders and/or beneficial owners,
iii. change of registered office,
iv. change of trustees,
v. change of corporate name and/or trading name,
vi. change of the principal trading partners and/or undertake new major business activities;

(c) a material change in the way and the rules the

customer's account operates, such as:

i. Change in the persons that are authorised to operate the account,
ii. application for the opening of new account for the provision of new investment services and/or financial instruments.

Transactions that favour anonymity

(section 66(3) of the Law)

19. In the case of customers' transactions via the internet, phone, fax or other electronic means where the customer is not 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 Financial Organisation 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.

Failure or refusal to submit information for the verification of customers' identity

(section 62(4) of the Law)

20. (1) Failure or refusal by a customer to submit, before the establishment of a business relationship or the execution of an occasional transaction, the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the customer is involved in money laundering or terrorist financing activities. In such an event, the Financial Organisation does not proceed with the establishment of the business relationship or the execution of the occasional transaction while at the same time the compliance officer considers whether it is justified under the circumstances to submit a

report to MOKAS, according to paragraph 9(1)(g).

(2) If, during the business relationship, a customer fails or refuses to submit, within a reasonable timeframe, the required verification data and information according to paragraph 18, the Financial Organisation terminates the business relationship and closes all the accounts of the customer while at the same time examines whether it is justified under the circumstances to submit a report to MOKAS, according to paragraph 9(1)(g).

Construction of an economic profile

(section 61(1) of the Law)

21. (1) The Financial Organisation is satisfied that it's dealing with a real person and, for this reason, obtains sufficient evidence of identity to verify that the person is who he claims to be.

Furthermore, the Financial Organisation verifies the identity of the beneficial owners of the customers' accounts. In the cases of legal persons, the Financial Organisation obtains adequate data and information so as to understand the ownership and control structure of the customer. Irrespective of the customer's type (e.g. natural or legal person, sole trader or partnership), the Financial Organisation requests and obtains sufficient data and information regarding the customer's business activities and the expected pattern and level of transactions.

However, it is noted that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative.

(2) The verification of the customers' identification is based on reliable data and information issued or obtained from independent and reliable sources, meaning those data, and information that are the most difficult to be amended or obtained illicitly.

(3) A person's residential and business address is an essential part of his identity and, thus, a separate procedure for its verification, according to point 1(c) of the Fifth Appendix, is followed.

(4) It is never acceptable to use the same verification data or information for verifying the customer's identity and verifying its home address.

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

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

(b) the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments;

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

(6) The data and information that are used for the construction of the customer's-legal person's economic profile include, inter alia, the name of the company, the country of its incorporation, the head offices address, the names and the identification information of the beneficial owners, directors and authorised signatories, financial information, ownership structure of the group that the company may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information). The said data and information are recorded in a separate form designed for this purpose which is retained in the customer's file along with all other documents as well as all internal records of meetings with the respective customer. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the customer or alters existing information that makes up the economic profile of the customer.

Identical data and information with the abovementioned are obtained in the case of a customer-natural person, and in general, the same procedures with the abovementioned are followed.

(7) Transactions executed for the customer are compared and

evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the customer and the data and information kept for the customer's economic profile. Significant deviations are investigated and the findings are recorded in the respective customer's file. Transactions that are not justified by the available information on the customer, are thoroughly examined so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting an internal report to the compliance officer, according to paragraph 9(1)(e), and then by the latter to MOKAS, according to paragraph 9(1)(g) .

Specific customer identification issues

Fifth Appendix

22. The Fifth Appendix includes customer identification and due diligence procedures that the Financial Organisation applies for specific customer identification issues.

Simplified customer identification and due diligence procedures

(section 63 of the Law)

23. (1) According to section 63 of the Law, the Financial Organisation, may not apply the provisions of paragraph 18 in respect of the customers referred to the abovementioned section of the Law. It is provided that the Financial Organisation collects sufficient information, so as to decide whether the customer can be exempted according to the provisions of the abovementioned section of the Law. The Financial Organisation when assessing the abovementioned pays special attention to any activity of those customers or to any type of transactions which may be regarded as particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.

(2) The Financial Organisation does not consider that customers or transactions referred to in section 63 of the Law represent a low risk of money laundering or terrorist financing if there is information available to suggest that the risk of money laundering or terrorist financing may not be low.

(3) For the purposes of applying section 63(1)(d) of the Law, public authorities or public bodies of the European Economic Area countries, for which the provisions of paragraph 18 may not be applied, must fulfil all the following criteria:

(a) the customer has been entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation;

(b) the customer's identity is publicly available, transparent and certain;

(c) the activities of the customer, as well as its accounting practices, are transparent;

(d) either the customer is accountable to a community institution or to the authorities of a member state, or appropriate check and balance procedures exist ensuring control of the customer's activity.

Enhanced customer identification and due diligence procedures

(section 64 of the Law)

24. According to section 64 of the Law, the Financial Organisation applies enhanced customer identification and due diligence procedures in respect of the customers referred to in section 64 of the Law and the Fourth Appendix, as well as in other

situations, that pose a high level of risk for money laundering or terrorist financing and are classified by the Financial Organisation as high risk on the basis of its customers' acceptance policy, according to paragraph 7.

Reliance on third parties for customer identification and due diligence purposes

(section 67 of the Law)

25. (1) Without prejudice to the provisions of section 67 of the Law, the Financial Organisation may rely on third parties for the implementation of customer identification and due diligence procedures, as these are prescribed in section 61(1)(a),(b) and (c) of the Law, provided that the third person makes immediately available all data and information, which must be certified true copies of the originals, that were collected in the course of applying customer identification and due diligence procedures.

(2) The Financial Organisation obtains data and information so as to verify that the third person is subject to professional registration in accordance with the competent law of its country of incorporation and/or operation as well as supervision for the purposes of compliance with the measures for the prevention of money laundering and terrorist financing.

(3) The Financial Organisation 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 customers. According to the degree of risk any additional data and information for the purpose of updating the customer's economic profile or for the purpose of examining unusual transactions executed through the account, is obtained from the natural persons (directors,

beneficial owners) who control and manage the activities of the customer and have the ultimate responsibility of decision making as regards to the management of funds and assets.

(4) in the case where the third person of subparagraph (1) is an accountant or an independent legal professional or a trust and company services provider from a country which is a member of the European Economic Area or a third country that the Advisory Authority for Combating Money Laundering and Terrorist Financing has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive, then the Financial Organisation, before accepting the customer identification data verified by the said third person, applies the following additional measures/procedures :

(a) assesses and evaluates, according to paragraph 9(1)(k) the systems and procedures applied by the third person for the prevention of money laundering and terrorist financing;

(b) as a result of the assessment of point (a), is satisfied that the third person implements customer identification and due diligence systems and procedures which are in line with the requirements of the Law and the present Directive;

(c) maintains a separate file for every third person of the present paragraph, where it stores the assessment

report of point (a) and other relevant information (for example identification details, records of meetings, evidence of the data and information of subparagraph (2));

(d) the commencement of the cooperation with the third person and the acceptance of customer identification data verified by the third person is subject to approval by the compliance officer, according to paragraph 9(1)(k);

Ongoing monitoring of accounts and transactions

(section 58(e) and 61(1)(d) of the Law)

26. (1) The Financial Organisation has a full understanding of normal and reasonable account activity of their customers as well as of their economic profile and have the means of identifying transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the Financial Organisation is not able to discharge its legal obligation to identify and report suspicious transactions to MOKAS, according to paragraphs 9(1)(g) and 27.

(2) The procedures and intensity of monitoring accounts and examining transactions are based on the level of risk and, as a minimum, achieve the following:

(a) identifying all high risk customers according to paragraph 7. Therefore, the systems or the measures and procedures of the Financial Organisation are able to produce detailed lists of high risk customers so as to

facilitate enhanced monitoring of accounts and transactions;

(b) detecting of unusual or suspicious transactions that are inconsistent with the economic profile of the customer for the purposes of further investigation;

(c) the investigation of unusual or suspicious transactions from the employees who have been appointed for that purpose; the results of the investigations are recorded in a separate memo and kept in the file of the customer concerned;

(d) all necessary measures and actions must be taken, based on the investigation findings of point (c), including any internal reporting of suspicious transactions/activities to the compliance officer, according to paragraph 9(1)(e);

(e) ascertaining the source and origin of the funds credited to accounts.

(3) The Financial Organisation introduces and implements, where appropriate and proportionate, in view of the nature, scale and complexity of its business and the nature and range of the investment services and activities undertaken in the course of that business, adequate automated electronic management information systems which will be capable of supplying the board of directors and the compliance officer, on a timely basis, all the valid and necessary information for the

identification, analysis and effective monitoring of customer accounts and transactions based on the assessed risk for money laundering or terrorist financing purposes.

(4) The monitoring of accounts and transactions are carried out in relation to specific types of transactions and economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship. Furthermore, the monitoring covers customers who do not have a contact with the Financial Organisation as well as dormant accounts exhibiting unexpected movements.

(5) The automated electronic management information systems may be also used to extract data and information that is missing regarding the customer identification and the construction of a customer's economic profile.

(6) For all accounts, automated electronic management information systems are able to add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g. high risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the customer, the country of his origin, the source of the funds, the type of transaction or other risk

factors. The Financial Organisation gives particular attention to transactions exceeding the abovementioned limits, which may indicate that a customer might be involved in unusual or suspicious activities.

PART VI
RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES TO MOKAS

Reporting of suspicious transactions to MOKAS

(sections 26, 27, 69 and 70 of the Law)

27. Without prejudice to the provisions of section 70 of the Law, the Financial Organisation, in cases where there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, reports, through the compliance officer its suspicion to MOKAS in accordance with paragraph 9(1)(g).

Suspicious transactions

28. (1) The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for money laundering and terrorist financing are almost unlimited. A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Financial Organisation has created for the customer. The Financial Organisation ensures that maintains adequate information and knows enough about its customers' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

Sixth Appendix

(2) A list containing examples of what might constitute suspicious transactions/activities related to money laundering and terrorist financing is attached to the Sixth Appendix. The said list is not exhaustive nor includes all types of transactions that may be used, nevertheless it can assist the Financial Organisation and its employees in recognising the main methods used for money laundering and terrorist financing. The detection by the Financial Organisation of any of the transactions contained in the Sixth Appendix prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

Compliance officer's report to MOKAS

29. (1) All the reports of the compliance officer of paragraph 9(1)(g) are send or submitted to MOKAS by post, facsimile or by hand.

(2) After the submission of a suspicious report of paragraph 9(1)(g), the Financial Organisation may subsequently wish to terminate its relationship with the customer concerned for risk avoidance reasons. In such an event, the Financial Organisation exercises particular caution, according to section 48 of the Law, not to alert the customer concerned that a suspicious report has been submitted to MOKAS. Close liaison with MOKAS is, therefore, maintained in an effort to avoid any frustration to the investigations conducted.

(3) After submitting the suspicious report of paragraph 9(1)(g),

the Financial Organisation adheres to any instructions given by MOKAS and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active.

According to section 26(2)(c) of the Law, MOKAS may instruct the Financial Organisation to refrain from executing or delay the execution of a customer's transaction without such action constituting a violation of any contractual or other obligation of the Financial Organisation and its employees.

(4) Furthermore, after the submission of a suspicious report of paragraph 9(1)(g), the customers' accounts concerned as well as any other connected accounts are placed under the close monitoring of the compliance officer.

Submission of information to MOKAS

30. The Financial Organisation ensures that in the case of a suspicious transaction investigation by MOKAS, will be able to provide without delay the following information:

(a) the identity of the account holders;
(b) the identity of the beneficial owners of the account;

(c) the identity of the persons authorised to manage the account;

(d) data of the volume of funds or level of transactions flowing through the account;

(e) connected accounts;

(f) in relation to specific transactions:

i. the origin of the funds,
ii. the type and amount of the currency involved in the transaction,
iii. the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers,
iv. the identity of the person that gave the order for the transaction,
v. the destination of the funds,
vi. the form of instructions and authorisation that have been given,
vii. the type and identifying number of any account involved in the transaction.

PART VII
RECORD KEEPING

Record keeping and time period of keeping documents/data

(section 68 of the Law)

31. (1) According to section 68(1) of the Law, the Financial Organisation keeps record of the documents/data mentioned in the above section of the Law and are specialised in the present Directive, including those referred to in paragraph 9(1)(k).

(2) According to section 68(2) of the Law, the documents/data of subparagraph (1), are kept for a period of at least five (5) years, which is calculated after the execution of the transactions or the termination of the business relationship.

It is provided that, the documents/data relevant to ongoing investigations are kept until MOKAS confirms that the investigation has been completed and the case has been closed.

Format of records

32. (1) The retention of the documents/data, other than the original documents or their certified true copies that are kept in a hard copy form, may be in other forms, such as electronic form, provided that the Financial Organisation is able to retrieve the relevant documents/data without undue delay and present them at any time, to the Commission or to MOKAS, after a request.

(2) When the Financial Organisation establishes a documents/data retention policy, takes into consideration the requirements of the Law and the present Directive and the potential needs of MOKAS and the Commission.

Certification and language of documents

33. (1) The documents/data obtained, for compliance with the present Directive, are in their original form or in a certified true copy form. In the case that the documents/data are certified as true copies by a different person than the Financial Organisation itself or by the third person mentioned in paragraph 25, the documents/data must be apostilled or notarised.

(2) A true translation is attached in the case that the documents/data of subparagraph (1) are in a language other than Greek or English.

PART VIII
EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

Employees' obligations

(section 58 of the Law)

34. (1) The Financial Organisation's employees can be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing.

(2) The employees cooperate and report, without delay, according to paragraph 9(1)(e), anything that comes to their attention in relation to transactions for which there is a slight suspicion that are related to money laundering or terrorist financing.

(3) According to section 26 of the Law, the Financial Organisation's employees fulfill their legal obligation to report their suspicions regarding money laundering and terrorist financing, after their compliance with subparagraph (2).

Employees' education and training program

35. (1) The Financial Organisation ensures that its employees are fully aware of their legal obligations according to the Law and the present Directive, by introducing a complete employee's education and training program.

(2) The timing and content of the training provided to the employees of the various departments is adjusted according to the needs of each Financial Organisation. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as

well as any other changes in the financial system of the Republic.

(3) The training program aims at educating employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose.

(4) The training program has a different structure for new employees, existing employees and for different departments of the Financial Organisation according to the services that they provide. On-going training is given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

PART IX
FINAL PROVISIONS

Existing clientele

36. Without prejudice to the provisions of section 62(6) of the Law, the Financial Organisation complies with the provisions of the present Directive, regarding its existing clientele, within nine (9) months from the date of enactment of the present Directive.

Repeal of the Commission's existing Directive

37. The Commission's Directive that was issued according to section 60(3) of the Prevention and Suppression of Money Laundering Activities Law of 1996, as amended, is hereby repealed and substituted with the present Directive.

Entry into force

38. The present Directive shall enter into force as of is publication in the Official Gazette of the Republic.

FIRST APPENDIX

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER'S DETAILS

Name:..... Tel:.....

Department:..... Fax:.....

Position:.....

CUSTOMER'S DETAILS

Name:..... .....

Address: ....

..... Date of Birth:.....

Tel:..... Occupation:.....

Fax:..... Details of Employer:.....

.....

Passport No.:..... Nationality:.....

ID Card No.:..... Other ID Details: .....

INFORMATION/SUSPICION

Brief description of activities/transaction:..... .....

....

Reason(s) for suspicion:..... .....

....

Informer's Signature Date

..... ……..……..

FOR COMPLIANCE OFFICER'S USE

Date Received: ..... Time Received: .....Ref.....

Reported to MOKAS: Yes/No ... Date Reported:.....Ref.....

SECOND APPENDIX

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: .....Customer's Details: .....

Informer:.....Department:.....

INQUIRIES UNDERTAKEN (Brief Description)

.....

.....

.....

ATTACHED DOCUMENTS

.....

.....

.....

.....

COMPLIANCE OFFICER'S DECISION

.....

.....

.....

FILE NUMBER.....

COMPLIANCE OFFICER'S SIGNATURE DATE

…… ……

THIRD APPENDIX

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

I. GENERAL INFORMATION

Financial Organisation's Name : _____

Address where customer's account is kept : _____

_____

Date when a business relationship established or occasional transaction was carried out : _____

Type of account(s) and number(s) : _____

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

(A) NATURAL PERSONS

	Beneficial owner(s) of the account(s)	Authorised signatory(ies) of the account(s)
Name(s):	_____	_____
	_____	_____
Residential address(es):	_____	_____
	_____	_____
	_____	_____
	_____	_____
Business address(es):	_____	_____

	_____	_____
	_____	_____
	_____	_____
Occupation and Employer:	_____	_____
	_____	_____
	_____	_____
	_____	_____
Date and place of birth:	_____	_____
	_____	_____
	_____	_____
	_____	_____
Nationality and passport number:	_____	_____
	_____	_____
	_____	_____
	_____	_____

(B) LEGAL ENTITIES

Legal entity's name, country
and date of incorporation: _____
_____
_____

Business address: _____
_____
_____

Main activities: _____
_____

	Name	Nationality and passport number	Date of birth	Residential address	Occupation and employer's details
Registered Shareholder(s)	1. _____ 2. _____ 3. _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
Beneficial Owner(s) (if different from above)	1. _____ 2. _____ 3. _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
Directors	1. _____ 2. _____ 3. _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
Authorised signatory(ies) of the account(s)	1. _____ 2. _____ 3. _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____

III. DETAILS OF SUSPICIOUS ACTIVITIES

Details of suspicious activities should be given

1. _____

2. _____

3. _____

4. Knowledge/suspicion of money laundering or terrorist financing (please explain, as fully as possible the knowledge or suspicion connected with money laundering or terrorist financing)

_____

_____

_____

_____

_____

_____

_____

5. Other information – Other services provided to the customer(s)

_____

_____

_____

_____

_____

_____

_____

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 customer's passport or ID card evidencing identity.
2. For legal entities: Certificates of incorporation, directors and shareholders.
3. All documents relating to the suspicious transaction(s)

FOURTH APPENDIX

HIGH RISK CUSTOMERS

R.A.D. 192/2016

1. Non face to face customers

(a) Whenever a customer requests the establishment of a business relationship or an occasional transaction, a personal interview is recommended during which all information for customer identification should be obtained. In situations where a customer, especially a non-resident of the Republic, requests the establishment of a business relationship or an occasional transaction by mail, telephone or through the internet without presenting himself for a personal interview, the Financial Organisation shall follow the established customer identification and due diligence procedures, as applied for customers with whom it comes in direct and personal contact and obtain the same exact identification information and documents as required by the Law and this Directive, depending on the type of the customer. The said identification information and documents kept by the Financial Organization in its records shall take the following form:

i. Original, or

ii. True copy of the original, where the certification is made by the Financial Organization in cases where it establishes the customer's identity itself, once the original is presented thereto, or

iii. True copy of the original, where the certification is made by third parties, in cases where they establish the customer's identity, pursuant to Article 67 of the Law and the provisions of paragraph 25 of this Directive, or

R.A.D. 262/2016

iv. True copy of the original, where the certification is made by a competent authority or person that, pursuant to the relevant provisions of the laws of their country, is responsible to certify the authenticity of documents or information, or

R.A.D. 262/2016

v. Provided that at least one of the procedures referred to in paragraph (b) below is followed:

   i. Copy of the original, or

   ii. Data and information collected via electronic verification in accordance with the provisions of paragraph (c) below.

R.A.D. 262/2016

(b) Instead of the measure provided for in Article 64(1)(a)(ii) of the Law, other practical procedures, which may be adopted for the implementation of the measure of Article 64(1)(a)(i) of the Law with regard to customers with whom the Financial Organization does not come to immediate and personal contact, are as follows:

i. The first payment of the operations is carried out through an account opened in the customer's name with a credit institution operating and licensed in a third country, which, according to the Advisory Authority's decision, imposes requirements on combating money laundering equivalent to those of the EU Directive.

ii. A direct confirmation of the establishment of a business relationship is obtained through direct personal contact, as well as, the true name, address and passport/identity card number of the customer, from a credit institution or a financial institution with which the customer cooperates, operating in a Member State or in a Third Country, which, according to the Advisory Authority's decision, imposes requirements on combating money laundering equivalent to those of the EU Directive (or a true copy of the confirmation).

iii. Telephone contact with the customer at his home or office, on a telephone number which has been verified from independent and reliable sources. During the telephone contact, the Financial Organization shall confirm additional aspects of the identity information submitted by the customer during the procedure of opening his account.

iv. Communication via video call with the customer, provided the video recording and screen shot safeguards apply to the communication. It is provided that a customer, whose identity was verified hereunder cannot deposit an amount over €2.000 per annum, irrespective of the number of accounts that he keeps with the Financial Organization, unless an additional measure of paragraph (b) of the present or of article 64(1)(a)(ii) of the Law is taken in order to verify his identity. During the internet communication, the Financial Organization shall confirm additional aspects of the identity details submitted by the customer when opening his account.

It is provided that the Financial Organization shall apply appropriate measures and procedures in order to:

1. confirm and monitor both the amount of the customer's deposit and the risk for money laundering or terrorist financing and take additional measures to verify the customer's identity depending on the degree of the risk
2. ensure the normal conduct of business is not interrupted where the amount of the deposit exceeds the amount of €2.000 per annum;
3. warn the customer appropriately and in due time for the above procedure in order to obtain the customer's express consent prior to its commencement.

v. Communication with the customer through at an address that the Financial Organization has previously verified from independent and reliable sources, in the form of a registered letter (For example, such communication may take the form of a direct mailing of account opening documentation to him, which the customer shall return to the Financial Organization or the Financial Organisation may send security codes required by the customer to access the accounts opened through the internet).

R.A.D. 262/2016

(c) Performing an electronic verification:

1. Electronic identity verification is carried out either directly by the Financial Organization or through a third party. Both the Financial Organization and the said third parties cumulatively satisfy the following conditions:

i. the electronic databases kept by the third party or to which the third party or the Financial Organization has access are registered to and/or approved by the Data Protection Commissioner in order to safeguard personal data (or the corresponding competent authority in the country the said databases are kept).

ii. electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information (at least the customer's full name, address and date of birth) and negative information (e.g. committing of offences such as identity theft, inclusion in deceased persons records, inclusion in sanctions and restrictive measures' list by the Council of the European Union and the UN Security Council).

iii. electronic databases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alter.

iv. transparent procedures have been established allowing the Financial Organization to know which information was searched, the result of such search and its significance in relation to the level of assurance as to the customer's identity verification.

v. procedures have been established allowing the Financial Organization to record and save the information used and the result in relation to identity verification.

R.A.D. 262/2016

2. Information must come from two or more sources. The electronic verification procedure shall at least satisfy the following correlation standard:

i. identification of the customer's full name and current address from one source, and

ii. identification of the customer's full name and either his current address or date of birth from a second source.

R.A.D. 262/2016

3. For purposes of carrying out the electronic verification, the Financial Organization shall establish procedures in order to satisfy the completeness, validity and reliability of the information to which it has access. It is provided that the verification procedure shall include a search of both positive and negative information.

R.A.D. 262/2016

(d) It is provided that the Financial Organization evaluates the results in order the conditions of Article 61(3) of the Law to be satisfied. The Financial Organization establishes mechanisms for the carrying out of quality controls in order to assess the quality of the information on which it intends to rely.

R.A.D. 262/2016

(e) The requirements of Article 64(1)(a) of the Law and of this Directive shall also apply to companies or other legal persons requesting to establish a business relationship or an occasional transaction by mail, telephone or through the internet. The Financial Organization shall take additional measures to ensure that the

companies or other legal persons operate from the address of their main offices and carry out legitimate activities in all respects.

2. Accounts in the names of companies whose shares are in bearer form

A Financial Organisation may accept a request for the establishment of a business relationship or for an occasional transaction from companies whose own shares or those of their parent companies (if any) have been issued in bearer form by applying, in addition to the procedures of paragraph 6 of the Fifth Appendix, all the following supplementary due diligence measures:

(a) Takes physical custody of the bearer share certificates while the business relationship is maintained or obtains a confirmation from a bank operating in the Republic or a country of the European Economic Area that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform the Financial Organisation accordingly.

(b) The account is closely monitored throughout its operation. At least once a year, a review of the accounts' transactions and turnover is carried out and a note is prepared summarising the results of the review which must be kept in the customer's file.

(c) If the opening of the account has been recommended by a third person as defined in paragraph 25, at least once every year, the third person who has introduced the customer provides a written confirmation that the capital base and the shareholding structure of the company or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones. If the account has been opened directly by the company, then the written confirmation is provided by the company's directors.

(d) When there is a change to the beneficial owners, the Financial Organisation examines whether or not to permit the continuance of the account's operation.

3. Trusts accounts

(a) Without prejudice of the provisions of section 65(2) of the Law, when the Financial Organisation establishes a business relationship or carries out an occasional transaction with trusts, it must ascertain the legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trustee and beneficial owners, according to the customer identification procedures prescribed in the Law and the present Directive.

(b) Furthermore, the Financial Organisation ascertains the nature of activities and the purpose of establishment of the trust as well as the source and origin of funds requesting the relevant extracts from the trust deed and any other relevant information from the trustees. All relevant data and information should be recorded and kept in the customer's file.

4. 'Client accounts' in the name of a third person

(a) A Financial Organisation may open "client accounts" (e.g. omnibus accounts) in the name of financial institutions from European Economic Area countries or a third country which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it applies procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the European Union Directive. In these cases the Financial Organisation ascertains the identity of the abovementioned financial institutions according to the customer identification procedures prescribed in the Law and the present Directive.

(b) In the case that the opening of a "client account" is requested by a third person acting as an auditor/accountant or an independent legal professional or a trust and company service provider situated in a country of the European Economic Area or a third country which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing has been determined that it applies procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the European Union Directive, the Financial Organisation may proceed with the opening of the account provided that the following conditions are met:

i. The third person is subject to mandatory professional registration in accordance with the relevant laws of the country of operation.

ii. The third person is subject to regulation and supervision by an appropriate competent authority in the country of operation for anti money laundering and terrorist financing purposes.

iii. The compliance officer has assessed the customer identification and due diligence procedures implemented by the third person and has found them to be in line with the Law and this Directive. A record of the assessment should be prepared and kept in a separate file maintained for each third person.

iv. The third person make available to the Financial Organisation obtains all the data and documents prescribed in section 67(3) of the Law.

5. Politically exposed persons' accounts

RAD 192/2016

(a) The establishment of a business relationship or the execution of an occasional transaction with politically exposed persons as interpreted in Article 2(1) of the Law, may expose a Financial Organisation to enhanced risks, especially, if the potential customer seeking to establish a business relationship or the execution of an occasional transaction is a politically exposed person, a member of his immediate family or a close associate that is known to be associated with a politically exposed person.

The Financial Organisation should pay more attention when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards.

(b) In order to effectively manage such risks, the Financial Organisation assess the countries of origin of their customers in order to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the 40+9 requirements of the Financial Action Task Force, according to point 7 of this Appendix.

With regard to the issue of corruption one useful source of information is the Transparency International Corruption Perceptions Index which can be found on the website of Transparency International at www.transparency.org. With regard to the issue of adequacy of application of the 40+9 recommendations of the FATF, the Financial Organisation may retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe) or the International Monetary Fund.

RAD 192/2016

(c) (Deleted)

The meaning ‘politically exposed persons’ includes the following natural persons who are or have been entrusted with prominent public functions’ in a foreign country:

i. heads of State, heads of government, ministers and deputy or assistant ministers,

ii. members of parliaments,

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

iv. members of courts of auditors or of the boards of central banks,

v. ambassadors, chargıs d'affaires and high-ranking officers in the armed forces,

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

(d) Without prejudice to the application, on a risk-sensitive basis, of enhanced customer due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning of point 5(c) of this Appendix for a period of at least one year, the Financial Organisation shall not be obliged to consider such a person as politically exposed.

(e) None of the categories set out in point 5(c) of this Appendix shall be understood as covering middle ranking or more junior officials. ‘Immediate family members’ includes the following:

i. the spouse or the person with which cohabit for at least one year,

ii. the children and their spouses or the persons with which cohabit for at least one year,

iii. the parents.

(f) ‘Persons known to be close associates’ includes the following:

i. any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in point 5(c) of this Appendix,

ii. any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in point 5(c) of this Appendix.

(g) Without prejudice to the provisions of section 64(1)(c) of the Law, the Financial Organisation adopts the following additional due diligence measures when it establishes a business relationship or carry out an occasional transaction with a politically exposed person:

i. Put in place appropriate risk management procedures to enable it to determine whether a prospective customer is a politically exposed person. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for politically exposed persons, seeking and obtaining information from the customer himself or from publicly available information. In the case of legal entities and arrangements, the procedures aim at verifying whether the beneficial owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute politically exposed persons. In case of identifying one of the above as a politically exposed person, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in the Law and the present Directive.

ii. The decision for establishing a business relationship or the execution of an occasional transaction with a politically exposed person is taken by an executive director of the Financial Organisation and the decision is then forwarded to the compliance officer. When establishing a business relationship with a customer (natural or legal person) and subsequently it is ascertained that the persons involved are or have become politically exposed persons, then an approval is given for continuing the operation of the business relationship by an executive director of the Financial Organisation which is then forwarded to the compliance officer.

iii. Before establishing a business relationship or executing an occasional transaction with a politically exposed person, the Financial Organisation obtains adequate documentation to ascertain not only the identity of he said person but also to assess his business reputation (e.g. reference letters from third parties).

iv. The Financial Organisation creates the economic profile of the customer by obtaining the information specified in paragraph 21. The details of the expected business and nature of activities of the customer forms the basis for the future monitoring of the account. The profile should be regularly reviewed and updated with new data and information. The Financial Organisation is particularly cautious and most vigilant where its customers are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks.

v. The account is subject to annual review in order to determine whether to allow its continuance of operation. A short report is prepared summarising the results of the review by the person who is in charge of monitoring the account. The report is submitted for consideration and approval to the board of directors and filed in the customer's personal file.

6. Electronic gambling/gaming through the internet

(a) The Financial Organisation may establish a business relationship or execute an occasional transaction in the names of persons who are involved in the abovementioned activities provided that these persons are licensed by a competent authority of a country of the European Economic Area or a third country which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it applies procedures equivalent to the requirements of the European Union Directive. For this purpose, the Financial Organisation requests and obtains, apart from the data and information required by the present Directive, copy of the licence that has been granted to the said persons by the competent supervisory/regulatory authority, the authenticity of which must be verified either directly with the supervisory/regulatory authority or from other independent and reliable sources.

(b) Furthermore, the Financial Organisation collects adequate information so as to understand the customers' control structure and ensures that the said customers apply adequate and appropriate systems and procedures for customer identification and due diligence for the prevention of money laundering and terrorist financing.

(c) In the case that the customer is a person who offers services (e.g. payment providers, software houses, card acquirers) to the persons mentioned in point 6(a) of the present Appendix, then the Financial Organisation requests and obtains, apart from the data and information required by the present Directive, adequate information so as to be satisfied that the services are offered only to licensed persons. Also, it obtains information necessary to completely understand the ownership structure and the group in which the customer belongs, as well as any other information that is deemed necessary so as to establish the customer's economic profile. Additionally, the Financial Organisation obtains the signed agreement between its customer and the company that is duly licensed for electronic gambling/gaming activities through the internet, by a competent authority of a country mentioned in point 6(a) of the present Appendix,

(d) For all the above cases, the decision for the establishment of a business relationship or the execution of an occasional transaction is taken by an executive director of the Financial Organisation and the decision is then forwarded to the compliance officer. Moreover, the account of the said customer is closely monitored and subject to regular review with a view of deciding whether or not to permit the continuance of its operation. Accordingly, a report is prepared and submitted for consideration and approval to the board of directors and filed in the customer's personal file.

7. Customers from countries which inadequately apply Financial Action Task Force's recommendations

(a) The Financial Action Task Force's ("FATF") 40+9 Recommendations constitute the primary internationally recognised standards for the prevention and detection of money laundering and terrorist financing.

(b) The Financial Organisation applies the following:

i. Exercises additional monitoring procedures and pays special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations.

ii. Transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If a Financial Organisation cannot be fully satisfied as to the legitimacy of a transaction, then a suspicious transaction report is filed to MOKAS, according to paragraph 9(1)(g).

(c) With the aim of implementing the above, the compliance officer consults the country assessment reports prepared by the FATF (http://www.fatf-gafi.org), the other regional bodies that have been established and work on the principles of FATF [e.g. Moneyval Committee of the Council of Europe (www.coe.int/moneyval)] and the International Monetary Fund (www.imf.org). Based on the said reports, the compliance officer assesses the risk from transactions and business relationships with persons from various countries and decides of the countries that inadequately apply the FATF's recommendations. According to the aforesaid decision of the compliance officer, the Financial Organisation applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating from countries with significant shortcomings in their legal and administrative systems for the prevention of money laundering and terrorist financing.

FIFTH APPENDIX

SPECIFIC CUSTOMER IDENTIFICATION ISSUES

1. Natural persons residing in the Republic

(a) The Financial Organisation ascertain the true identity of natural persons who are residents of the Republic Cyprus by obtaining the following information:

i. true name and/or names used as these are sated on the official identity card or passport,
ii. full permanent address in the Republic, including postal code,
iii. telephone (home and mobile) and fax numbers,
iv. e-mail address , if any,
v. date and place of birth,
vi. nationality and
vii. details of the profession and other occupations of the customer including the name of employer/business organisation.

(b) The acceptable method for the verification of the identification of a customer's identity is the reference to an original document which is issued by an independent and reliable source that carries the customer's photo. After the Financial Organisation is satisfied for the customer's identity from the original identification documents presented, it keeps copies of the pages containing all relevant information which are certified, by the Financial Organisation, as true copies of the original documents.

(c) In addition to the name verification, it is important that the customer's permanent address is also verified by using one of the following ways:

i. visit at the place of residence (in such a case, the Financial Organisation's officer who carries out the visit prepares a memo which is retained in the customer's file), and

ii. the production of a recent (up to 6 months) utility bill, local authority tax bill or a bank statement or any other document same with the aforesaid (to protect against forged or counterfeit documents, the prospective customers are required to produce original documents).

(d) In addition to the above, the procedure for the verification of a customer's identity is reinforced if the said customer is introduced by a reliable staff member of the Financial Organisation, or by another existing reliable customer who is personally known to a member of the board of directors. Details of such introductions are kept in the customer's file.

2. Natural persons not residing in the Republic

(a) For customers who are not normally residing in the Republic, in addition to the information collected according to point (1) of the present Appendix, the Financial Organisation, without prejudice to the application on a risk-sensitive basis, requires and receives information on public positions which the prospective customer holds or held in the last twelve months as well as whether he is a close relative or associate of such individual, in order to verify if the customer is a politically exposed person, according to point (5) of the Fourth Appendix.

(b) For those customers not residing in the Republic, passports are always requested and, if available, official national identity cards issued by competent authorities of their country of origin are obtained and certified true copies of the pages containing the relevant information from the said documents are obtained and kept in the customers' files. In addition, it is advised, if in doubt for the genuineness of any document (passport, national identity card or documentary evidence of address), to seek verification of identity with an Embassy or the Consulate of the issuing country or a reputable credit or financial institution situated in the customer's country of residence.

(c) In addition to the aim of preventing money laundering and terrorist financing, the abovementioned information is also essential for implementing the financial sanctions imposed against various persons by the United Nations and the European Union. In this regard, passport's number, issuing date and country as well as the customer's date of birth always appear on the copies of documents obtained, so that the Financial Organisation would be in a position to verify precisely whether a customer is included in the relevant list of persons subject to financial sanctions which are issued by the United Nations or the European Union based on a United Nations Security Council's Resolution and Regulation or a Common Position of the European Union's Council respectively.

3. Joint accounts

In the cases of joint accounts of two or more persons, the identity of all individuals that hold or have the right to manage the account, are verified according to the procedures set in points (1) and (2) of the present Appendix.

4. Accounts of unions, societies, clubs, provident funds and charities

In the case of accounts in the name of unions, societies, provident funds and charities, a Financial Organisation ascertains their purpose of operation and verifies their legitimacy by requesting the production of the articles and memorandum of association/procedure rules and registration documents with the competent governmental authorities (in case the law requires such registration). Furthermore, the Financial Organisation obtains a list of the members of board of directors/management committee of the abovementioned organisations and verifies the identity of all individuals that have been authorised to manage the account according to the procedures set in points (1) and (2) of the present Appendix.

5. Accounts of unincorporated businesses, partnerships and other persons with no legal substance

(a) In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, beneficial owners and other individuals who are authorised to manage the account is verified according to the procedures set in points (1) and (2) of the present Appendix. In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate is obtained.

(b) The Financial Organisation obtains documentary evidence of the head office address of the business, ascertains the nature and size of its activities and receives all the information required according to paragraph 21 for the creation of the economic profile of the business.

(c) The Financial Organisation requests, in cases where exists, the formal partnership agreement and also obtains mandate from the partnership authorising the opening of the account and confirming authority to a specific person who will be responsible for its operation.

6. Accounts of legal persons

(a) Section 65(2) of the Law provides that for customers that are legal persons, it is established that the natural person appearing to act on their behalf, is appropriately authorised to do so and his identity is established and verified according to the procedures set in points (1) and (2) of the present Appendix.

(b) The Financial Organisation takes all necessary measures for the full ascertainment of the legal person's control and ownership structure as well as the verification of the identity of the natural persons who are the beneficial owners and exercise control over the legal person.

(c) The verification of the identification of a legal person that requests the establishment of a business relationship or the execution of an occasional transaction, comprises the ascertainment of the following:

i. the registered number,
ii. the registered corporate name and trading name used,
iii. the full addresses of the registered office and the head offices,
iv. the telephone numbers, fax numbers and e-mail address,
v. the members of the board of directors,
vi. the individuals that are duly authorised to operate the account and to act on behalf of the legal person,
vii. the beneficial owners of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country with equivalent disclosure and transparency requirements.
viii. the registered shareholders that act as nominees of the beneficial owners,
ix. The economic profile of the legal person, according to the provisions of paragraph 21.

(d) For the verification of the identity of the legal person, the Financial Organisation requests and obtains, inter alias, original or certified true copies of the following documents:

i. certificate of incorporation and certificate of good standing of the legal person,
ii. certificate of registered office,
iii. certificate of directors and secretary,
iv. certificate of registered shareholders in the case of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country with equivalent disclosure and transparency requirements,
v. memorandum and articles of association of the legal person,
vi. a resolution of the board of directors of the legal person for the opening of the account and granting authority to those who will operate it,

vii. in the cases where the registered shareholders act as nominees of the beneficial owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the beneficial owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the beneficial owner has been agreed,

viii. documents and data for the verification, according to the provisions of the present Directive, the identity of the persons that are authorised by the legal person to operate the account, as well as the registered shareholders and beneficial owners of the legal person.

(e) Where deemed necessary for a better understanding of the activities, sources and uses of funds/assets of a legal person, the Financial Organisation obtains copies of its latest audited financial statements (if available), and/or copies of its latest management accounts.

(f) For legal persons incorporated outside the Republic, the Financial Organisation requests and obtains documents similar to the above.

(g) As an additional due diligence measure, on a risk-sensitive basis, the Financial Organisation may carry out a search and obtain information from the records of the Registrar of Companies and Official Receiver of the Republic (for domestic companies) or from a corresponding authority in the company's (legal person's) country of incorporation (for foreign companies) and/or request information from other sources in order to establish that the applicant company (legal person) is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and Official Receiver and that it continues to be registered as an operating company in the records of the Registrar of Companies and Official Receiver of the Republic or by an appropriate authority outside the Republic.

It is pointed out that, if at any later stage any changes occur in the structure or the ownership status or to any details of the legal person, or any suspicions arise emanating from changes in the nature of the transactions performed by the legal person via its account, then it is imperative that further enquiries should be made for ascertaining the consequences of these changes on the documentation and information held by the Financial Organisation for the legal person and all additional documentation and information for updating the economic profile of the legal person is collected.

(h) In the case of a customer-legal person that requests the establishment of a business relationship or the execution of an occasional transaction and whose direct/immediate and principal shareholder is another legal person, registered in the Republic or abroad, the Financial Organisation, before establishes a business relationship or executes an occasional transaction, verifies the ownership structure and the identity of the natural persons who are the beneficial owners and/or control the other legal person.

(i) Apart from verifying the identity of the beneficial owners, the Law requires that the persons who have the ultimate control over the legal person's business and assets are identified. In the cases that the ultimate control rests with the persons who have the power to manage the funds, accounts or investments of the legal person without requiring authorisation and who would be in a position to override the internal procedures of the legal person, the Financial Organisation, verifies the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than 10% in the legal person's ordinary share capital or voting rights.

(j) In cases where the beneficial owner of a legal person, requesting the establishment of a business relationship or the execution of an occasional transaction, is a trust set up in the Republic or abroad, the Financial Organisation implements the procedure provided in paragraph 3 of the Fourth Appendix.

7. Investment funds, mutual funds and firms providing financial or investment services

(a) Without prejudice of the provisions of section 63(1) of the Law, the Financial Organisation may establish and maintain business relationships or execute occasional transactions with persons who carry out the above services and activities which are incorporated and/or operating in countries of the European Economic Area or a third country which according to a decision of the Advisory Authority for Combating Money Laundering Offences and Terrorist Financing it has been determined that applies requirements equivalent to those laid down in the European Union Directive, provided that:

i. the said persons possess the necessary license or authorisation from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services, and
ii. are subject to supervision for the prevention of money laundering and terrorist financing purposes.

(b) In the case of the establishment of a business relationship or the execution of an occasional transaction with persons who carry out the above services and activities and which are incorporated and/or operating in a third country other than those mentioned in point (a) above, the Financial Organisation requests and obtains, in addition to the abovementioned, in previous points, documentation and the information required by the present Directive for the identification and verification of persons, including the beneficial owners, the following:

i. a copy of the licence or authorisation granted to the said person from a competent supervisory/regulatory authority of its country of incorporation and operation, whose authenticity should be verified either directly with the relevant supervisory/regulatory authority or from other independent and reliable sources, and

ii. adequate documentation and sufficient information in order to fully understand the control structure and management of the business activities as well as the nature of the services and activities provided by the customer.

(c) In the case of investment funds and mutual funds the Financial Organisation, apart from identifying beneficial owners, obtains information regarding their objectives and control structure, including documentation and information for the verification of the identity of investment managers, investment advisors, administrators and custodians.

8. Nominees or agents of third persons

(a) The Financial Organisation takes reasonable measures to obtain adequate documents, data or information for the purpose of establishing and verifying the identity, according to the procedures set in the previous points of the present Appendix:

i. the nominee or the agent of the third person, and
ii. any third person on whose behalf the nominee or the agent is acting.

(b) In addition, the Financial Organisation obtains a copy of the authorisation agreement that has been concluded between the interested parties.

SIXTH APPENDIX

EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING

A. MONEY LAUNDERING

1. Transactions with no discernible purpose or are unnecessarily complex.

2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the customer.

3. The transactions or the size of the transactions requested by the customer do not comply with his usual practice and business activity.

4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the customer's business activities would not appear to justify such activity.

5. The business relationship involves only one transaction or it has a short duration.

6. There is no visible justification for a customer using the services of a particular Financial Organisation. For example the customer is situated far away from the particular Financial Organisation and in a place where he could be provided services by another Financial Organisation.

7. There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).

8. There are frequent small purchases of a particular financial instrument by a customer who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the customer's instructions, in an account other than his usual account.

9. Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.

10. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.

11. The settlement of any transaction but mainly large transactions, in cash.

12. Settlement of the transaction by a third person which is different than the customer which gave the order.

13. Instructions of payment to a third person that does not seem to be related with the instructor.

14. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on money laundering and terrorist financing.

15. A customer is reluctant to provide complete information when establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with Financial Organisations, names of its officers and directors, or information on its business location. The customer usually provides minimum or misleading information that is difficult or expensive for the Financial Organisation to verify.

16. A customer provides unusual or suspicious identification documents that cannot be readily verified.

17. A customer's home/business telephone is disconnected.

18. A customer that makes frequent or large transactions and has no record of past or present employment experience.

19. Difficulties or delays on the submission of the financial statements or other identification documents, of a customer/legal person.

20. A customer who has been introduced by a foreign Financial Organisation, or by a third person whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on money laundering and terrorist financing.

21. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).

22. The stated occupation of the customer is not commensurate with the level or size of the executed transactions.

23. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

24. Unexplained inconsistencies arising during the process of identifying and verifying the customer (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).

25. Complex trust or nominee network.

26. Transactions or company structures established or working with an unneeded commercial way. e.g. companies with bearer shares or bearer financial instruments or use of a postal box.

27. Use of general nominee documents in a way that restricts the control exercised by the company's board of directors.

28. Changes in the lifestyle of employees of the Financial Organisation, e.g. luxurious way of life or avoiding being out of office due to holidays.

29. Changes the performance and the behaviour of the employees of the Financial Organisation.

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 narcotics trafficking. Legal fund raising methods used by terrorist groups include:

i. collection of membership dues and/or subscriptions,

ii. sale of books and other publications,

iii. cultural and social events,

iv. donations,

v. 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:

i. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.

ii. 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.

iii. The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.

iv. The non-profit organisation provides administrative support to the terrorist movement.

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

i. Inconsistencies between the apparent sources and amount of funds raised or moved.

ii. A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.

iii. A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.

iv. Large and unexplained cash transactions by non-profit organisations.

v. The absence of contributions from donors located within the country of origin of the non-profit organisation.