CENTRAL BANK OF CYPRUS

EUROSYSTEM

PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

DIRECTIVE TO CREDIT INSTITUTIONS IN ACCORDANCE WITH ARTICLE 59(4) OF THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES LAWS OF 2007 TO 2013

(FOURTH ISSUE)

DECEMBER 2013

CONTENTS

Preface

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

(ii). In 1992, Cyprus enacted the first Law by which money laundering deriving from drug trafficking was criminalised. In 1996 Cyprus enacted "The Prevention and Suppression of Money Laundering Activities Law" defining and criminalising money laundering deriving from all serious criminal offences. The Law recognised the important role of the financial sector on the prevention and forestalling of money laundering activities and contained special provisions for measures and procedures that persons involved in financial business should put in place to that effect. The Law was subsequently amended to adopt new international initiatives and standards in the area of money laundering, including the 2nd European Union Directive for the prevention of the use of the financial system for the purpose of money laundering (Directive 91/308/EEC).

(iii). The Law designated the Central Bank of Cyprus as the competent supervisory authority for persons engaged in banking activities and assigned to it the responsibility of supervising and monitoring the compliance of banks with the provisions of the Law with the aim of preventing the use of the services provided by banks for money laundering.

(iv). On 13/12/2007 the House of Representatives enacted "The Prevention and Suppression of Money Laundering Activities Law" (hereinafter to be referred to as "the Law") by which the former Laws on the prevention and suppression of money laundering activities of 1996-2004 were consolidated, revised and repealed. Under the current Law, which came into force on 1 January 2008, the Cyprus legislation was harmonised with the Third European Union Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Directive 2005/60/EC) hereinafter to be referred to as the "European Union Directive". The Basic Law and its subsequent amendments (i.e. 58(I)/2010, 80(I)/2012, 192(I)/2012 and 101(I)/2013) are available at the webpage of the Central Bank of Cyprus http://www.centralbank.gov.cy.

(v). From 1989 up to 1996, the Central Bank of Cyprus issued several circulars to the banks operating in Cyprus, recommending the introduction of specific measures against the use

of the financial system for the purpose of money laundering. As from 1997, the Central Bank of Cyprus, exercising its powers emanating from the Law enacted in 1996, proceeded with the issue of a series of Directives to all banks in Cyprus prescribing the practices and procedures that banks should adopt so as to comply with the requirements of the Law for the implementation of preventive measures against money laundering activities.

(vi). The present Central Bank of Cyprus' Directive (Fouth Edition) (hereinafter to be referred to as "the Directive") is issued to all credit institutions in accordance with Article 59(4) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2013, and aims at laying down the specific policy, procedures and control systems that all credit institutions should implement for the effective prevention of money laundering and terrorist financing so as to achieve full compliance with the requirements of the Law. It is emphasized that the Law explicitly states that Directives are binding and compulsory to all persons to whom they are addressed. Furthermore, the Law assigns to the supervisory authorities, including the Central Bank of Cyprus, the duty of monitoring, evaluating and supervising the implementation of the Law and of the Directives issued to the supervised entities.

1. INTERNAL CONTROL PROCEDURES AND RISK MANAGEMENT

1.1 Obligation to establish procedures

The Law Article 58

1. Article 58 of the Law requires all persons carrying on financial or other business to establish adequate and appropriate systems and procedures, inter alia, for the following:

   (i). Internal control, risk assessment and risk management in order to forestall and prevent money laundering and terrorist financing, and

   (ii). the detailed examination of any transaction which by nature may be considered to be particularly vulnerable to be associated with money laundering or terrorist financing, and in particular, complex and unusually large transactions and all unusual patterns of transactions which have no apparent economic or clear lawful purpose.

2. The Board of Directors, the credit institution's Senior Management and, in the cases of branches of foreign banks operating in Cyprus, the Manager of the Cyprus branch, are responsible for ensuring the implementation of the requirements of the Law and this Directive and the introduction of appropriate systems and internal control procedures for the identification, evaluation, monitoring and effective management of the risks emanating from money laundering or terrorist financing activities according to the nature, size and complexity of their operations.

3. Effective procedures for the prevention of money laundering and terrorist financing include appropriate management oversight, systems and controls, segregation of duties, education and other relevant practices.

4. The Central Bank of Cyprus' "Directive on a Framework of Principles of Operation and Criteria of Assessment of Banks' Organisational Structure, Internal Governance and Internal Control Systems" issued in May, 2006, and its subsequent amendments requires that credit institutions whose shares are listed on the Stock Exchange or operate branches and/or subsidiaries abroad and whose total off balance sheet and on balance sheet assets exceeds 2 bn EUR setup a Compliance Unit which is administratively independent from other units whose responsibilities include risk management, executive or audit responsibilities e.g. Risk Management Unit, Internal Audit Unit and Legal Unit of the credit institution. The aforementioned Directive, amongst others, provides that the Compliance Unit of a credit institution or its Risk Management Unit (where no Compliance Unit has been set up) establishes and applies suitable procedures for the purpose of achieving a timely and on-going compliance of the credit institution with the applicable supervisory and regulatory framework

relating to the prevention of the use of the financial system for the purposes of money laundering and financing of terrorism. In this respect, the Money Laundering Compliance Officer appointed under Article 69 of the Law should organizationally belong to the Compliance Unit or, where such unit has not been established, to the Risk Management Unit.

5. The Money Laundering Compliance Officer ("MLCO") should be appointed by the credit institution's Board, after having obtained the consent of the Central Bank of Cyprus which reserves the right to request his/her substitution if, in its opinion, he/she is not "fit and proper", as laid down in Article 69(1) of the Law, to discharge his/her duties. It should be noted that the MLCO could be the same person as with the Head of Compliance Unit.

6. The MLCO of branches of foreign banks operating in Cyprus report directly to the local manager and the Senior Management of the bank's Head Office at its country of origin.

The Law Articles 59(6)(α)(iv) &(v)

7. According to Article 59(6)(a)(iv) and (v) the Central Bank of Cyprus may, inter alia, request the cessation or removal from his position of any director, manager or official, including the MLCO and the Head of Internal Audit and Compliance Units, in the event of infringement due to his own fault, willful omission or negligence. In addition, it may impose an administrative fine as specified in Article 59(6)(ii) of the Law to a director, manager or official or any other person, in the event of infringement due to his own fault, willful omission or negligence.

8. The Central Bank of Cyprus requires credit institutions to apply the following measures and procedures:

   (i) The Board of Directors determines, records and approves the general policy principles of the credit institution for the prevention of money laundering and terrorist financing which are subsequently communicated to the Senior Management and the MLCO.

   (ii) In case where a credit institution operates branches or subsidiaries in a third country, it has to put in place a Group policy (See Section 9 of this Directive).

   (iii) The credit institution's Senior Management should be aware of the degree of risk of money laundering and terrorist financing that the credit institution is exposed to and whether all the necessary measures for their management and mitigation have been implemented. Consequently, the MLCO has the responsibility to draft and submit to the Board through the Senior Management a brief report recording and evaluating all money laundering and terrorist financing potential risks (having in mind the areas of operation of the credit institution, the development of new products and services, the customer acceptance policy, expansion to new markets/countries, the complexity of legal persons' ownership structure, ways to attract customers, etc.), the measures that

have been taken for their management and mitigation as well as the monitoring mechanisms for the appropriate and effective operation of internal regulations, procedures and controls (See Section 3 of this Directive).

(iv) The MLCO has the responsibility in cooperation with other departments of the credit institution (e.g. the Organisation and Methods Unit) for the design of the internal practices, procedures and controls, as well as the description and explicit allocation of competence and limits of responsibility of each unit that is involved in the prevention of money laundering and terrorist financing. In this connection, a risk management and procedures manual should be prepared, which after being approved by the credit institution's Senior Management, should be communicated to the executives and all the employees that manage, monitor or control in any way the customers' accounts and transactions and have the responsibility for the application of the policy, procedures and controls that have been determined. The risk management and procedures manual covers, inter alia, the credit institution's customer acceptance policy, the procedures for establishing a business relationship, executing one-off transactions, opening of accounts and customer due diligence, including the documents and information that is required for the establishment of a business relationship and execution of transactions, the procedures for the on-going monitoring of accounts and transactions, as well as, the procedures and controls for the identification of unusual and suspicious transactions and their internal reporting to the MLCO. The manual is assessed on a periodic basis and reviewed when deficiencies are found or when the need arises to adapt the credit institution's procedures for the effective management of the risks emanating from money laundering and terrorist financing. It should be noted that any reviews of the manual should be approved by the Senior Management.

(v) Explicit responsibilities and duties are allocated to the credit institution's staff so as to secure the effective management of policy, procedures and controls for the prevention of money laundering and terrorist financing and achieving compliance with the requirements of the Central Bank of Cyprus' Directives and the Law.

(vi) The MLCO, the Alternate MLCO, the Assistant Money Laundering Compliance Officers and other members of staff who have been assigned with the duty of implementing the adopted procedures for the prevention of money laundering and terrorist financing, have full and timely access to all information concerning customers' identity, transactions' records and other relevant files and information maintained by the credit institution so as to be fully facilitated in the effective

discharge of their duties.

(vii) All employees are made aware of the person appointed as MLCO (as well as his alternate) to whom they should report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing activities.

(viii) There is a clear and concise reporting chain, explicitly prescribed in the risk management and procedures manual by which information regarding suspicious transactions is passed without delay to the MLCO, either directly or through his Assistants;

(ix) Explicit policy and procedures are applied and measures are taken for preventing the abuse of new technologies and systems of providing banking services and effecting banking transactions for the purpose of money laundering and terrorist financing (e.g. services and transactions via the internet, telephone or via the Automatic Teller Machines or other modern telecommunication devices).

(x) Appropriate measures are applied so that the risk of money laundering and terrorist financing is appropriately considered and managed in the course of daily activities of the credit institution with regard to the development of new products and possible changes in the credit institution's business profile (i.e. penetration of new markets with the opening of branches/subsidiaries in new countries/regions). It is noted that the Central Bank of Cyprus's Directive on the "Framework of principles of operation and criteria of assessment of banks' organisational structure, internal governance and internal control systems" issued to banks' in May 2006 and as subsequently amended, requires the participation, in an advisory capacity, of the Compliance Unit in the planning of new products and procedures, in matters that call for an operational decision, as well as for the assessment of operational risk which may result from a major development (merger, acquisition, etc), so that the necessary control and risk management mechanisms which will ensure compatibility with the existing rules are established and pursued.

(xi) The Senior Management of the credit institution ensures that the MLCO has sufficient resources, including competent staff and technological equipment, for the effective discharge of his/her duties.

(xii) The Internal Audit Unit reviews and evaluates, **on an annual basis**, the effectiveness and adequacy of the policy, procedures and controls applied by the credit institution for preventing money laundering and terrorist financing and verifies

the level of compliance with the provisions of the Central Bank of Cyprus' Directive and the Law. Findings and observations of the internal auditor are submitted to the Board of Directors' Audit Committee and are notified to the Senior Management and the MLCO of the credit institution who take the necessary measures to ensure the rectification of any weaknesses and omissions which have been detected by the internal auditor. The internal auditor monitors, on an ongoing basis, through progress reports, or other means the implementation of his recommendations.

(xiii) Credit institutions apply explicit procedures and standards of recruitment and evaluation of new employees' integrity.

1.2 Customer Acceptance Policy

9. Credit institutions should develop and establish a clear policy and procedures for accepting new customers, fully in line with the provisions of the Law and the requirements of this Directive. The said policy should be prepared after detailed assessment of the risks faced by each credit institution from its customers and/or their transactions and/or their countries of origin or operations (See Section 3 of this Directive).

10. The MLCO prepares the customer acceptance policy and submits it through the credit institution's Senior Management to the Board of Directors for consideration and approval. Once it has been approved, the said policy is communicated to all staff members.

11. The said policy should set in an explicit manner the criteria for accepting new customers, the types of customers who do not meet the said criteria and are not, therefore, acceptable for entering into a business relationship and should prescribe the categories of customers that should be designated as being of high risk. Due consideration should be given to complex business structures, and the risks that such entities may accumulate, in determining the credit institution's risk appetite and customer acceptance policy and enhanced measures should be required to effectively monitor and mitigate such risks. The said policy should also determine the conditions and related procedures under which a customer relationship should be terminated. The description of the types of customers that are not acceptable for entering into a business relationship and the categories of high risk customers should take into account factors such as their background, type and nature of their business activities, their country of origin, anticipated level and nature of business transactions as well as the expected source and origin of funds. The customer acceptance policy and related procedures should provide for enhanced due diligence for the categories of high risk customers as prescribed in the Law, this Directive (see Section 4.14.2) as well as those customers that the credit institution itself has classified as high risk on the basis of its adopted policy.

2. THE ROLE OF THE MONEY LAUNDERING COMPLIANCE OFFICER

2.1. Appointment of a Money Laundering Compliance Officer ("MLCO")

The Law Article 69(1)

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

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

    (ii) require that any such report be considered in the light of all other relevant information by the MLCO, for the purpose of determining whether or not the information or other matter set out in the report proves this fact or creates such suspicion;

    (iii) allow the MLCO to have access to any information, records and details which may be of assistance to him/her and which is available to the person carrying out financial or other business activities; and

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

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

13. The MLCO should be appointed by the Board, after having obtained the consent of the Central Bank of Cyprus which reserves the right to request his/her substitution if, in its opinion, he/she is no longer "fit and proper", as laid down in Article 69(1) of the Law, to discharge his/her duties. In this connection, the person who has been nominated for appointment to the position of the MLCO should complete the Individual Questionnaire, found in Appendix 1, which includes information regarding the person's career, including the qualifications held and work experience, as well as details of any sanctions or criminal convictions against the person. The said person should act independently and autonomously

to perform the above duties, and depending on the organizational structure of the credit institution, should possess the appropriate seniority so as to command the necessary authority.

14. . Additionally, the credit institution should also appoint an Alternate MLCO who should replace the MLCO in case of absence. Where it is deemed necessary due to the volume and/or the geographic spread of the credit institution's operations, credit institutions may appoint Assistant MLCOs by division, district or otherwise for the purpose of assisting the MLCO and immediately forwarding internal suspicion reports to the MLCO. In light of the aforesaid, credit institutions should communicate to the Central Bank of Cyprus, within ten days from the date of the appointment of the the Alternate MLCO, his name, position and contact details.

The Law
Article 68d(1)

15. Article 68d(1) of the Law requires that every financial group (as specified in Article 68d (2)(a)) appoints a manager from the company of the group which has been incorporated in the Republic and holds the biggest amount of total assets among the companies of the group which have been incorporated in the Republic, as a coordinator, for ensuring the implementation by all the companies of the financial group, including their branches abroad, which are engaged in financial activities, of adequate and appropriate systems and procedures for the effective prevention of money laundering and terrorist financing offenses.

2.2 Duties of the Money Laundering Compliance Officer

16. The role and responsibilities of the MLCO, the Alternate MLCO, as well as those of his Assistants, should be clearly specified by credit institutions and documented in the risk management and procedures manual for the prevention of money laundering and terrorist financing.

17. Furthermore, the Compliance Unit or, where it does not exist, the MLCO should maintain procedures manual for all his tasks/responsibilities.

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

(i) The MLCO has the responsibility, to record and assess on an annual basis all risks arising from existing and new customers, products and services as well as the measures or changes to the systems and procedures implemented by the credit institution for the effective management of the aforesaid risks. The said report should be submitted to the Board of Directors through the Senior Management for consideration and approval. A copy of the said report should be submitted to the Central Bank of Cyprus together with the MLCO's

annual report. In addition to the aforementioned annual briefing of the Senior Management by the MLCO on the risks facing the credit institution, the MLCO is obliged to keep the Senior Management informed of any differentiation of those risks on an on-going basis.

(ii) The MLCO prepares the Customer Acceptance Policy which is submitted through the Senior Management of the credit institution to the Board of Directors for consideration and approval.

(iii) The MLCO has the primary responsibilityfor the preparation of the credit institution's risk management and procedures manual for the prevention of money laundering and terrorist financing. The manual is assessed on a periodic basis and reviewed when deficiencies are found or when the need arises to adapt the credit institution's procedures for the effective management of the risks emanating from money laundering and terrorist financing.

(iv) Without prejudice to the obligations of the Compliance Unit, as set out in paragraph 3 above, the MLCO monitors and assesses whether the policy, procedures and controls that have been introduced for the prevention of money laundering and terrorist financing are correctly and effectively applied. In this regard, the MLCO should apply appropriate monitoring mechanisms (e.g. on-site visits to units/branches) which will provide him/her with all necessary information for assessing the level of compliance of the units /branches of the credit institution with the procedures and controls currentlyin force. In the event that the MLCO identifies shortcomings and/or weaknesses in the application of the requisite procedures and controls, he/she should give appropriate guidance for corrective measures.

(v) The MLCO receives any information from the credit institution's employees which is considered by the latter to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities in the form of an internal report. A specimen of such an internal report (hereinafter to be referred to as "Internal Money Laundering Suspicion Report") is attached, as Appendix 2, to this Directive. All such reports should be registered and kept on a separate file.

(vi) The MLCO evaluates and investigates the information received as per paragraph (v), citing other available sources of information, the discussion of the case with the reporting employee and, where appropriate, with the employee's superior(s). The evaluation of the information reported to the MLCO should be made on a separate form which should be registered and retained on file. A specimen of such a report (hereinafter to be referred to as "Money Laundering Compliance Officer's Internal Evaluation Report") is attached, as Appendix 3, to this Directive.

(vii) If following the evaluation described in paragraph (vi) above, the MLCO decides to

notify the Unit for Combating Money Laundering (MOKAS), then he/she should complete a written report and submit it to MOKAS the soonest possible. A specimen of such a report (hereinafter to be referred to as "Money Laundering Compliance Officer's Report to the Unit for Combating Money Laundering") is attached, as Appendix 4, to this Directive. All such reports should be registered and kept on a separate file.

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

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

(x) The MLCO maintains a registry with statistical information (e.g. district and branch/unit maintaining the customer(s) account(s), date of submission of the internal report, date of assessment, date of reporting to MOKAS) in relation to the Internal Money Laundering Suspicious Reports and the MLCO's reports to MOKAS.

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

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

(xiii) The MLCO ensures that all branches and subsidiaries of the credit institution in non-EU countries have taken all necessary measures for achieving full compliance with the provisions of this Directive in relation to customer identification, due diligence and record keeping procedures.

(xiv) The MLCO must cooperate, coordinate and exchange information with the other MLCOs of the group.

(xv) The MLCO is generally responsible for the timely and correct submission to the Central Bank of Cyprus of the prudential reports referred to in Section 10 of this Directive and for providing the necessary explanations to the employees responsible for the preparation of the aforesaid returns. The MLCO responds promptly to any queries or clarifications requested by the Central Bank of Cyprus in relation to information contained in the aforesaid returns.

(xvi) The MLCO is responsible for examining and deciding on the applications for accepting cash deposits in foreign currency notes (referred to in Section 5.2 of this Directive)

submitted in writing by the responsible officials of the branches/units of the credit institution where the related customers' accounts are maintained. Copies of the applications submitted together with his/her decision must be kept by the MLCO on a separate file as well as the file of the customer concerned.

(xvii) The MLCO keeps records with the full details of customers or group of connected customers (name, address, account number(s), branch(es) maintaining the account(s)) for which he/she has given his/her written approval for a one-off cash deposit or a series of cash deposits in foreign currency notes on a continuous and regular basis. In this respect, the MLCO must keep separate records for customers who are involved in: (i) one-off cash deposits, and (ii) cash deposits on a continuous and regular basis.

(xviii) The MLCO maintains a register of all cases of persons (prospective customers) for which the credit institution declined the establishment of business relationship.

(xix) The MLCO responds to all requests and queries from the Central Bank of Cyprus and provides all requested information and co-operates fully with the Central Bank of Cyprus.

(xx) The MLCO, the Alternate MLCO and the Assistant MLCOs acquire the requisite knowledge and skills for the implementation of appropriate internal procedures for recognising, preventing and reporting transactions/activities suspected to be associated with money laundering or terrorist financing.

(xxi) The MLCO provides advice and guidance to the employees of the credit institution on the correct implementation of procedures and controls to prevent money laundering and terrorist financing.

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

(xxiii) The MLCO maintains the following records in relation to the seminars and other training offered to the credit instituion's employees and assesses the adequacy of the education/training provided.

a. Name of employee per branch/department and position (i.e. management, officers, newcomers, etc)

b. Date of the seminar, title, duration, names of lecturers.

c. Whether the lecture/seminar was organised internally or offered by an external organisation or consultants.

(xxiv) The MLCO assesses the systems and procedures applied by a third person on whom the credit institution relies for customer identification and due diligence purposes (see Section 4.12) or who applies for the opening of "client accounts" (see Section 4.14.2.4 of this Directive).

(xxv) The MLCO maintains a register with the data/information (i.e. name, place of business, area of activity, supervisory authority, date of commencement of business relationship, last review date, next review date, rating) of the third person with whom the credit institution has established a business relationship.

(xxvi) The MLCO assesses the adequacy of the policy and the related measures to prevent money laundering and terrorist financing applied by non-EU banks which apply for the opening of correspondent accounts (see Section 4.14.2.6 of this Directive).

(xxvii) The MLCO ensures that the credit institution prepares and maintains lists of customers classified as low and high risk (as these are determined by the Law, the Central Bank of Cyprus' Directive and the credit institution itself) which should contain the names of customers, their account number(s), the branch/unit maintaining the account(s) and the date of the commencement of business relationship. Moreover, the MLCO ensures the regular updating of the said lists with new or existing customers which the credit institution has decided, in the light of additional information obtained, to classify as high or low risk customers.

(xxviii) The MLCO obtains and utilises, for the purpose of applying the provisions of Section 4.14.2.9 "Customers from countries which do not adequately apply FATF's recommendations", the country assessment reports on money laundering issued by the Financial Action Task Force, regional international bodies which have been established and operate on FATF principles (e.g. Moneyval Committee of the Council of Europe), the International Monetary Fund and the World Bank.

(xxix) The MLCO receives or suggests, depending on the case, corrective measures on issues related to the prevention and suppression of money laundering and terrorist financing in accordance with the findings of the Central Bank of Cyprus.

(xxx) The MLCO evaluates the findings of the Internal Audit Unit regarding the taking of corrective measures on issues related to the prevention and suppression of money laundering and terrorist financing.

(xxxi) The MLCO reviews the information contained in the return submitted to the Central Bank of Cyprus for loans and deposits on the basis of the country of permanent residence of the ultimate beneficial owner of the account and, where appropriate, investigates any trends identified that may raise money laundering or terrorist financing concerns and be prepared to respond to queries raised by the Central Bank of Cyprus.

2.3 Annual Report of the Money Laundering Compliance Officer

19. The MLCO has also the duty of preparing an Annual Report which is a significant tool for assessing a credit institution's level of compliance with its obligations laid down in the Law and the Central Bank of Cyprus' Directives for the prevention of money laundering and terrorist financing.

20. The MLCO's Annual Report should be prepared within two months from the end of each calendar year (i.e. by the end of February, the latest) and should be submitted for consideration to the Board of Directors through the credit institution's Senior Management. In the case of a credit institution operating in Cyprus in the form of a branch, the Annual Report should be submitted to the credit institution's Board of Directors through the Senior Management of its country of origin.

21. The Board of Directors discusses and adopts the Annual Report. The Senior Management of the credit institution will then take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report.

22. A copy of the Annual Report submitted to the Board of Directors, shall also be forwarded at the same time to the Central Bank of Cyprus . Copies of the minutes citing the Board's approval should be also submitted to the Central Bank of Cyprus as soon as possible following the relevant meeting of the Board of Directors.

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

    (i) Information on measures taken and/or procedures introduced to comply with any amendments to the Law and the Central Bank of Cyprus' Directives which took place during the year.

    (ii) Information on the inspections and reviews performed by the MLCO and the credit

institution's Internal Audit Unit, including the number of inspections carried out, the Units inspected and the material deficiencies and weaknesses identified in the credit institution's anti-money laundering and terrorist financing policies and procedures. In this regard, the report should point out the significance of the deficiencies and weaknesses identified, their risk implications, as well as the recommendations made and/or the action taken for rectifying the situation.

(iii) Information on the procedures and the automated/electronic management information systems applied by the credit institution for the ongoing monitoring of customers' accounts and transactions, including the description of their main functions as well as of any weaknesses that have emerged.

(iv) The number of internal money laundering suspicious reports submitted by the credit institution's employees to the MLCO, broken down by district, address and branch and possible comments/observations thereon.

(v) The number of suspicious reports submitted by the MLCO to MOKAS with information on the main reasons for suspicion and any particular trends identified.

(vi) The number of suspicious transactions investigated by the MLCO but for which no report has been submitted to MOKAS.

(vii) Information on circulars and other communication with staff on money laundering and terrorist financing preventive issues.

(viii) Summary figures, on an annualised basis, of customers' total cash deposits and incoming/outgoing funds transfers in Euro and other currencies in excess of 10.000 Euro and 500.000 Euro (or equivalent thereof), respectively (together with comparative figures for the previous year), as reported to the Central Bank of Cyprus in the "Monthly Statement of Large Cash Deposits and Funds Transfers" and comments on material changes observed compared with the previous year.

(ix) Summary figures, on an annual basis, of the customers' total deposits and loans on the basis of the permanent residence of the ultimate beneficial owner of the account, analysing any trends identified that may raise money laundering or terrorist financing risks.

(x) Information on the policy, procedures and controls applied by the credit institution in relation to high risk customers with whom it maintains a business relationship such as companies with bearer shares, trusts, client accounts, politically exposed persons, correspondent accounts for non-EU banks, persons engaged in electronic gambling/gaming through the internet and any others classified by the credit institution as

such. In addition information should be provided on the number of high risk customers with whom the credit institution has a business relationship, per category and country of origin.

(xi) Information on the measures taken by branches/subsidiaries in non EU-countries for achieving full compliance with the provisions of this Directive in relation to customer identification, due diligence and record keeping procedures and comments/information on the level of their compliance.

(xii) Information on the training courses/seminars attended by the MLCO, the Alternate MLCO and the Assistant MLCOs and on any other educational material received.

(xiii) Information on training/ seminars provided to staff during the year, reporting :

- The number of courses/ seminars organised/attended
- their duration,
- the number of employees attending, specifying their seniority i.e. management staff, officers, clerical staff or newcomers etc,
- names and qualifications of the instructor(s), and
- specifying whether the courses/seminars were developed in-house or by an external organisation /consultant.

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

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

(xvi) Information on the structure and staffing of the MLCO's section as well as recommendations for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

(xvii) Copy of the report, as approved by the Board of Directors, which records and evaluates the risks emanating from money laundering for the current year.

(xviii) Copy of the register with the data / information (e.g. name, business address, business area, supervisory authority, date of commencement of business relationship, last review date, next review date, rating) on third persons with whom the credit institution has established a business relationship.

3. THE APPLICATION OF APPROPRIATE MEASURES AND PROCEDURES ON A RISK SENSITIVE BASIS

3.1 Introduction

The Law Article 61(2)

24. The Law requires all persons carrying out financial or other business activities to apply customer identification and due diligence procedures but allows them to determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship, product or transaction. However, the persons engaged in financial or other business activities must be able to demonstrate to the competent supervisory authorities that the extent of the measures is commensurate with the risks from the use of their services for the purposes of money laundering and terrorist financing.

25. A system of procedures and controls on a risk sensitive basis should strike a balance between the cost burden on credit institutions and their customers and the realistic assessment of the risk that the credit institutions' services maybe used for money laundering or terrorist financing. Consequently, applying measures and procedures on a risk sensitive basis enables credit institutions to focus their efforts on those areas where the risk of money laundering and terrorist financing appears to be higher.

26. A risk based approach assists the achievement of the overall objective of preventing the abuse of the banking system for illegal activities, in the following ways:

- recognises that the money laundering or terrorist financing risk for credit institutions varies across customers, countries/territories, products and services;
- allows the Board of Directors and Senior Management to differentiate between customers in a way that matches the risk of their particular business;
- allows the Board of Directors and Senior Management to apply their own approach in the formulation of policies, procedures and controls taking into account the credit institution's particular circumstances;
- helps to produce a more cost-effective system; and
- promotes the prioritisation of efforts and actions of credit institutions taking into account the likelihood of money laundering or terrorist financing occurring;

27. A risk-based approach involves a number of discrete steps in assessing the most cost-

effective and proportionate way to manage the money laundering and terrorist financing risks faced by the credit institution. These are:

- identifying and assessing the money laundering and terrorist financing risks emanating from specific customers, products, services, and geographical areas of operation of the credit institution and of its customers;

- managing and mitigating the assessed risks by the application of appropriate and effective policies, procedures and controls;

- continuous monitoring and improvements in the effective operation of the policies, procedures and controls; and

- documenting, in appropriate manuals, reports and internal circulars, the policies, procedures and controls to ensure their uniform implementation throughout the credit institution by persons specifically appointed for that purpose by the Board of Directors and Senior Management.

3.2 Identifying and Assessing Risks

28. The MLCO has the responsibility to identify, record and evaluate all potential risks. The successful establishment of systems and controls on a risk-based approach requires the full commitment and support of Senior Management and the active co-operation of the business units of the credit institution. There also needs to be a clear communication of policies and procedures throughout the credit institution, along with robust mechanisms to ensure that these are implemented effectively, weaknesses are promptly identified and improvements are made wherever necessary.

29. A risk-based approach starts with the identification, recording and assessment of the risk that has to be managed. Credit institutions need to assess and evaluate the risk of how they might be involved through the potential use of their services by criminals for the purpose of money laundering or terrorist financing. The particular circumstances of each credit institution will determine the suitable procedures and measures that need to be applied to counter and manage risk. In the cases where the business, products and customer base of a credit institution are relatively simple, involving relatively few products and customers, or customers with similar characteristics, then the credit institution should focus on those customers who fall outside the 'norm'. The identification and assessment of risk that each credit institution faces entails answering the following questions:

- What risk is posed by the credit institution's customers? (e.g. complexity of legal persons' ownership structures, companies with bearer shares, companies incorporated in offshore centers, politically exposed persons, customers engaged in a business which involves significant amounts of cash etc).

- What risk is posed by a customer's behaviour (e.g. customer transactions where there is no apparent legal/financial/commercial rationale; situations where the origin of wealth and/or source of funds of the customer cannot be easily verified; unwillingness of customers to provide information on the beneficial owner(s) and controller(s) of a legal person etc).

- How does the way the customer comes to the credit institution affect risk? (e.g. non-face-to-face customers, customer introduced by a third person etc).

- What risk is posed by the products/services the customer is using? (e.g. making payments via electronic funds transfers, large cash deposits or withdrawals, investment products etc).

30. Indicative parameters of a risk based system of controls and procedures are the following:

    - The scale and complexity of a credit institution's activities.
    - The geographical spread of its operations and its customers' activities.
    - The nature and profile of customers as well as of products and services offered.
    - The credit institution's distribution channels and practices.
    - The volume and size of transactions.
    - The degree of risk associated with each area of operations.
    - The country of origin and destination of customers' funds.
    - Deviations from the anticipated level of transactions.
    - The nature of business transactions.

3.3 Design and implementation of controls to manage and mitigate the risks

31. Once a credit institution has identified the risks it faces then it must design and implement the appropriate systems and controls for their management and mitigation in accordance with the

procedures prescribed in this Directive. As regards money laundering and terrorist financing, managing and mitigating the risks involves measures to verify the customer's identity, collecting additional KYC information about the customer to construct his business profile and monitoring his transactions and activity.

32. In order to ensure its policies, procedures and controls on anti-money laundering and terrorist financing are appropriate and effective, having regard to the assessed risk, a credit institution must determine the type and extent of measures it should adopt, to manage and mitigate the identified risks cost-effectively. These measures may, for example, include:
    - Adapting the customer due diligence procedures in line with their assessed money laundering and terrorist financing risk;
    - Requiring the quality and extent of requisite identification data for each type of customer to be of a certain standard (documents from independent and reliable sources, third person information, documentary evidence etc)
    - Obtaining additional customer or business relationship data and information where this is appropriate for the proper and complete understanding of a customer's activities and source of wealth to effectively manage any increased risk emanating from the particular business relationship.
    - On-going monitoring of high risk customers' transactions and activities.

33. The risk assessment and the implementation of the aforementioned measures must result in the classification of customers into three risk categories: low, normal and high risk. Criteria will be attached to each category to reflect the possible risk and each category should be accompanied by the corresponding due diligence procedures, periodic monitoring and controls.

34. Low risk customers are those business relationships prescribed in Article 63 of the Law (see Section 4.6 of this Directive).

35. High risk customers include those business relationships prescribed in Article 64 of the Law and Section 4.14 of this Directive as well as any other business relationship classified by the credit institution itself as such. In this regard, Article 64(2) of the Law provides that enhanced customer due diligence measures should be applied on a risk sensitive basis, in addition to the situations referred to in the Law and this Directive, in other business relationships which by nature present a higher risk of money laundering or terrorist financing.

36. In this connection, credit institutions are required, under the responsibility of the MLCO, to prepare and maintain separate lists of high and low risk customers (as determined by the Law,

this Directive and the credit institution itself) citing the customers' names, account number(s), branch(es) where the account(s) is (are) maintained and date of commencement of business relationship. The said lists should be promptly updated with all new customers or existing customers that the credit institution has decided, in the light of additional information received, to classify under the low or high risk categories.

37. It is repeated that a credit institution should be in a position to demonstrate to the Central Bank of Cyprus that the extent of systems and control procedures that it applies are commensurate to the risk it faces for the use of its services for the purpose of money laundering or terrorist financing.

38. In view of this, documenting the measures set out in paragraphs 32-36 above will assist credit institutions to prove:

- The ways used to identify and assess the risk of their services being used for money laundering or terrorist financing;
- How they have determined the introduction and implementation of specific policies, procedures and controls for the management and mitigation of risks; and
- The methods applied for monitoring and improving, whenever deemed necessary, the specific policies, procedures and controls.

.

3.4 Monitoring and improving the effective operation of credit institutions' internal procedures

39. Credit institutions need to have suitable means of assessing, on a regular basis, that their risk mitigation procedures and controls are working effectively. For that purpose, aspects the credit institution will need to consider are the following:

- Appropriate procedures to identify changes in customer's business profile;
- Reviewing ways in which new products and services may be used by criminals for money laundering or terrorist financing purposes, and how these ways may change;
- Procedures for assessing the adequacy of staff training and awareness;
- Introducing effective compliance monitoring arrangements (as applied by interalia, the Compliance Unit and the Internal Audit Unit);

- Appropriate technology-based and people-based systems;
- Appropriate management information systems;
- Reporting and accountability by responsible officials to the Board of Directors and Senior Management;
- Effectiveness of liaison with the Central Bank of Cyprus and MOKAS.

3.5 Dynamic Risk Management

40. Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Systems and controls should be kept under regular review so that risks resulting from changes in the characteristics of existing customers, new customers, products and services and in the geographical dispersion are managed and countered effectively.

41. Customers' activities change (without always the credit institution being informed) and the credit institution's products and services – and the way these are offered or sold to customers – also change. The same holds for products/transactions deployed by prospective money launderers or terrorist financiers.

3.6 Risk management report

42. The above mentioned actions of the credit institution should be recorded in a risk management report which should be kept fully updated. In this connection, the risk assessment should be performed on an annual basis even in cases where the credit institution considers that there is no need for revising its assessment report. The said report should be submitted on an annual basis to the Board of Directors, through the Senior Management, for approval so that any residual risks are acknowledged thereby reflecting the credit institution's risk appetite. A copy of the said report should be submitted to the Central Bank of Cyprus together with the MLCO's Annual Report.

4. CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES

4.1 Introduction

43. Collecting and maintaining sufficient information about a customer, making use of that information for the purposes of customer identification and the assessment of his/her business profile is the basis of all other procedures for the prevention of money laundering and terrorist financing and is the most effective weapon against the possibility that the services provided by credit institutions are used for the above mentioned illegal purposes. In addition to minimising the risk of a credit institution's services being used for illicit activities, collecting and maintaining sufficient information on a customer's identity allows the early detection and recognition of suspicious transactions/activities and protects the credit institutions from possible fraud and the underlying risks to their financial robustness and reputation.

4.2 When customer identification and due diligence procedures should be applied

The Law Articles 58 and 60

44. Articles 58 and 60 of the Law require persons carrying out financial and other business activities to apply adequate and appropriate systems and procedures in relation to the identification of a customer's identity and exercise of due diligence in the following cases:

(i) when establishing a business relationship;

(ii) when carrying out one-off transactions amounting to EUR 15.000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

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

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

The Law Article 2

45. The Law (article 2) provides the following definitions in relation to the above:

- 'business relationship' means a business, professional or commercial relationship which is connected with the activities of the persons carrying out financial or other business activities in accordance with Article 2 of the Law and which is expected, at the time when the contact is established, to have an element of duration;
- "one-off transaction" means any transaction other than a transaction carried out in the course of an established business relationship formed by a person acting in the course of relevant financial or other business;

- "customer" means a person that attempts to enter into a business relationship or carry out an one-off transaction with another person who carries on financial or other business in or from the Republic.

Regulation (EC) no. 1781/2006

46. In addition, credit institutions are required to establish the identity of their customers in accordance with the procedures provided in the Law and this Directive, in all cases of persons who do not maintain a business relationship with them and request the transfer of funds of an amount equal or greater than 1.000 Euro according to article 5(2) of the Regulation (EC) no 1781/2006 of the European Parliament and of the Council on information on the payer accompanying transfers of funds.

4.3 Customer identification and due diligence procedures

The Law Article 61(1)

47. Article 61(1) of the Law requires that the customer identification and due diligence procedures, include the following:

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

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

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

(iv) Conducting ongoing monitoring of the business relationship, including scrutiny of transactions carried out throughout the course of that relationship, to ensure that these transactions are consistent with the information and data in the possession of the person engaged in financial or other business activities in relation to the customer, the business and risk profile, including the source of funds and ensuring that the documents, data or information held are kept up-to-date.

The Law Article 61(3)

48. Article 61(3) of the Law provides that for the purpose of determining customer identification and due diligence measures, the proof of identity is sufficient if -

(i) It is reasonably possible to establish that the applicant/customer is the person he claims to be; and

(ii) the person who examines the evidence is satisfied, in accordance with the procedures followed under the Law, that the applicant/customer is actually the person who he claims to be.

The Law Article 2

49. The Law (article 2) provides the following definitions in relation to the beneficial owner:

'beneficial owner' means the natural person or natural persons who ultimately own or control the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:

(1) in the case of corporate entities:

(i) the natural person or natural persons who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, of a percentage of 10 % plus one share;

(ii) the natural person or natural persons who otherwise exercise control over the management and direction of a legal entity:

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

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

(ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates, the natural person or natural persons who exercise control over 10 % or more of the property of a legal arrangement or entity;

4.4 Timing of identification

The Law Articles 62(1), 62(2) and 62(4)

50. Article 62(1) of the Law requires that the verification of the identity of the customer and the beneficial owner should be made before the establishment of a business relationship or the carrying out of aone-off transaction as defined in the Law.

51. Despite the above, article 62(2) allows, by way of derogation, the verification of the identity of the customer and the beneficial owner(s) to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is low risk of money laundering or terrorist financing occurring. In such situations

these procedures shall be completed as soon as practicable after the initial contact and before the execution of any transactions.

52. However, article 62(4) explicitly requires that in situations where the person carrying out financial or other business activities is unable to comply with the customer identification and due diligence procedures stipulated in article 61(1)(a) to (c), it may not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, or shall terminate the business relationship, and shall consider whether under the circumstances a report should be filed with MOKAS.

4.5 Exercise of due diligence and updating of identification data of existing customers

The Law Articles 60(d) and 62(6)

53. Article 60(d) of the Law requires persons carrying out financial or other business activities to apply customer identification and due diligence measures when there are doubts about the veracity or adequacy of previously obtained customer identification documents, data or information. Furthermore, article 62(6) of the Law requires the application of customer identification and due diligence procedures not only to new customers but also at appropriate times to existing customers, depending on the level of risk of being involved in money laundering or terrorist financing activities.

54. Credit institutions must ensure that their customer identification records as well as the information that form their business/economic profile remain completely updated throughout the business relationship. In this respect, credit institutions must examine and check on a regular basis the validity and adequacy of the customer identification data and information they maintain, especially those concerning high-risk customers. The policy and the procedures for the prevention of money laundering should determine the timeframe during which the regular review, examination and update of the customer identification data should be conducted, depending on the risk categorisation of each customer. The outcome of the said review should be recorded in a separate note/ form which should be kept in the respective customer file.

55. Despite the above and taking into account the level of risk, if at any time during the business relationship with an existing customer, a credit institution becomes aware that reliable or adequate data and information are missing from the identity and the business/economic profile of the customer, then the credit institution should take all necessary action, by applying the customer identification and due diligence procedures provided in this Directive, to collect the missing data and information, the soonest possible, so as to update and complete the customer's business/economic profile.

56. In addition to the requirement for the update of the customer identification data and information on a regular basis or when it is observed that unreliable or inadequate data and information are being held, credit institutions should check the adequacy of the data and information held with regard to the customer's identity and business/economic profile, whenever one of the following events or incidents occurs:

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

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

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

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

(iii) Change of registered office;

(iv) Change of trustee(s);

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

(vi) Change of the principal trading partners and/or taking-up of new major business activities and/or expansion of activities to other geographical areas.

(3)There is a material change in the way and rules of the operation of the account, such as:

(i) Change in the person(s) that are authorised to operate the account(s); and

(ii) Application for the opening of new account(s) or the provision of new banking service(s) and/or product(s).

(iii) Activation of a dormant account.

(4) Customer's reclassification (e.g. low risk customers to normal or high risk).

(5) In case of identification of negative information about the client in the press or the internet or information submitted by a competent supervisory authority or MOKAS or other credit institution or following investigation which points to the need for an update of the data and information about the customer or to a possible risk reclassification.

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

4.6 Simplified customer identification and due diligence procedures

The Law Article 63(1)

58. Article 63(1) of the Law provides that persons engaged in financial or other business activities may apply simplified due diligence and identification procedures in respect of the following customers, provided that the risk of money laundering or terrorist financing is low and there is no suspicion of money laundering or terrorist financing:

    1. Credit or financial institutions governed by the EU Directive.

    2. A Credit or financial institution carrying out one or more of the financial activities as these are defined in article 2 of the Law and which is situated in a country outside the European Economic Area which:

        (i) following a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing enforces requirements equivalent to those laid down in the European Union Directive, and/or

        (ii) the credit or financial institution is subject to supervision with regard to its compliance with the said requirements.

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

    4. Domestic public authorities of countries of the European Economic Area.

59. It is further provided that in the cases of customers referred to in paragraphs (1) to (4) above, persons carrying out financial or other business activities, may not apply customer identification procedures on the customer or, where applicable, the beneficial owner, neither collect information in relation to the purpose and intended nature of the business relationship or may not verify the identity of the customer and beneficial owner after the establishment of a business relationship or the execution of an occasional transaction. Irrespective of the above, the persons carrying out financial or other business activities are obliged to conduct ongoing

monitoring of the business relationships referred to in paragraphs (1) to (4) above in accordance with the provisions of paragraph (d) of subsection (1) of article 61 and report to MOKAS cases of or attempts to perform suspicious transactions.

The Law
Article 63(2)

60. For the purpose of subparagraph 58(4) above, domestic public authorities of countries of the European Economic Area should fulfill the following criteria:

    (i) they have been entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation;

    (ii) their identity is publicly available, transparent and certain;

    (iii) their activities, as well as their accounting practices, are transparent;

    (iv) they are accountable either to a Community institution or to the authorities of a Member State, or appropriate check and balance procedures exist ensuring control of their activity.

61. Irrespective of the above, the Law requires that credit institutions should, in any case, gather sufficient information to establish if the customer qualifies for an exemption as mentioned above.

62. Sufficient information may include as a minimum:

    (i) confirmation from the competent supervisory/regulatory authority of the country of establishment and/or operation and

    (ii) a copy of the licence or authorisation issued to the customer by the competent supervisory/regulatory authority of the country of establishment and/or operation.

63. Credit institutions should verify that the person(s) who is/are authorised to handle the accounts of the above persons are duly authorised by the customer and are not exempted from the provisions of this directive for purposes of identification and verification of their identity.

64. Furthermore, article 63(2) of the Law states that credit institutions may apply simplified due diligence and identification procedures, provided that the risk of money laundering or terrorist financing is low and there is no suspicion of money laundering or terrorist financing in respect of:

    (1) a pension, or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages at source and the scheme rules do not permit the transfer of members' rights.

(2) electronic money, as defined in article 2 of the Electronic Money Institutions Law of 2012 provided that:

(i) where, if the device cannot be recharged, the maximum amount stored on the device is no more than EUR 250, whereas a limit of EUR 500 is applied for the device used for payment transactions executed only within the Republic or

(ii) where, if the device can be recharged, a limit of EUR 2.500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1.000 or more is redeemed in that same calendar year by the bearer, in accordance with articles 26 and 27 of the Electronic Money Institutions Law of 2012.

(3) The Central Bank of Cyprus may permit persons under its supervision to consider certain products or transactions related to these products as low risk provided that the following criteria are met:

(i) the product has a written contractual basis·

(ii) the related transactions are carried out through an account of the customer with a credit institution governed by the EU Directive or a credit institution situated in a third country which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Financing of Terrorism, imposes requirements equivalent to those laid down in the EU Directive·

(iii) the product or related transaction(s) are not anonymous and their nature is such that it allows for the timely application of section 60 (c) of the Law·

(iv) the product is subject to a predetermined maximum threshold as follows:

(aa) in the cases of life insurance or savings products of similar nature, the annual premium does not exceed EUR 1.000 or the single premium does not exceed EUR 2.500,

(bb) in the cases of products which are related to the financing of tangible assets and where the legal and beneficial title of the assets is not transferred to the customer until termination of the contractual relationship (irrespective of whether the transaction is carried out in a single transaction or in several transactions which appear to be linked), the annual payments do not exceed EUR 15.000 per year,

(cc) In all other cases the maximum threshold shall be EUR 15.000·

(v) the benefits of the product or related transactions cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined advanced age, or similar events·

(vi) in the case of products or related transactions allowing for the investment of funds in financial assets or claims, including insurance or other kind of contingent claims:

(aa) the benefits of the product or related transaction are only realisable in the long term,

(bb) the product or related transaction cannot be used as collateral,

(cc) during the contractual relationship, no prepayments are made, no surrender clauses are used and no early termination takes place.

4.7 Prohibition of anonymous and numbered accounts and accounts in fictitious names

The Law Article 66(2)

65. Article 66(2) of the Law prohibits persons carrying out financial or other business activities to open or maintain anonymous or numbered accounts or accounts in names other than those stated in official identification documents.

4.8 Transaction and products that favour anonymity

The Law Article 66(3)

66. Article 66(3) requires persons carrying out financial or other business activities to pay special attention to any money laundering or terrorist financing threat or risk that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for such purposes and apply reasonably possible measures and procedures to address risks arising from technological developments and new financial products.

67. In the case of customer transactions via the internet, phone, fax, automatic teller machines or other electronic means where the customer is not present so as to verify the authenticity of his signature and that he/she is the real beneficial owner of the account and/or that he/she has been properly authorised to operate the account, the credit institution should apply reliable methods, procedures and control mechanisms over the access to the electronic means so as to ensure that it transacts with the true owner or the authorised signatory to the account. Failure by credit institutions to check and verify that they are dealing with the true owner or the authorised signatory may lead to the execution of transactions from non- authorised persons resulting in financial losses or damage on the reputation of the credit institution either through fraud or acquisition of confidential information by third parties or unintentional involvement

in illegal activities. In this regard and for the purposes of managing the risks emanating from customer transactions effected through electronic means, credit institutions are required to apply the principles prescribed in the paper issued by the Basel Committee on Banking Supervision in July 2003 titled: "Risk Management Principles for Electronic Banking". The said document can be downloaded from the following web-site address: http://www.bis.org.

4.9 Prohibition of correspondent relationships with "shell banks"

The Law Articles 66(1) (a*) and (b)*

68. Article 66(1)(a) prohibits credit institutions from entering into or continuing a correspondent banking relationship with a shell bank. Furthermore, it is required (article 66(1)(b)) that credit institutions take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

The Law Article 2

69. The Law (article 2) defines a "shell bank" as a credit institution or institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, including a real address and management, and which is unaffiliated with a regulated financial group.

4.10 Failure or refusal to provide identification evidence

The Law Article 62(4)

70. Article 62(4) of the Law requires that where the person carrying out financial or other business activities is unable to comply with the customer identification procedures and due diligence measures, laid down in articles 61(1)(a) to (c) of the Law, then it should not carry out a transaction through a bank account, establish a business relationship, or it should terminate the business relationship and consider whether, under the circumstances, it is warranted to file a report with MOKAS.

71. Failure or refusal by a prospective customer that requests the opening of an account or the establishment of a business relationship or the execution of an one-off transaction, to submit the requisite identification information without adequate justification before the establishment of the business relationship, the opening of an account or the execution of an one-off transaction, constitute 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, credit institutions should not proceed with the opening of the account, the establishment of the business relationship or the execution of the one-off transaction while at the same time they should consider whether it is warranted under the circumstances to submit a report to MOKAS, based on the information they have in their possession.

4.11 Construction of a customer's business profile

The Law Article 61(1)

72. Article 61(1) of the Law requires, inter alia, that customer identification procedures and due diligence measures shall comprise the following:

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

(ii) the verification of the beneficial owner's identity and taking risk-based and adequate measures to verify his/her identity on the basis of documents, data or information issued or obtained from a reliable independent source so that the person carrying out financial or other business activities is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer; and

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

73. Credit institutions should establish to their satisfaction that they are dealing with a real person (natural or legal) and obtain sufficient evidence of identity to establish that a prospective customer is who he/she claims to be. The verification procedures necessary to establish the identity of the prospective customer should be based on reliable data, documents and information issued or obtained from independent reliable sources, i.e. those data, documents and information that are the most difficult to amend or obtain illicitly. Certified true copies of the identification evidence should always be retained by the credit institutions and kept in customers' files. However, it must be stressed that no single form of identification can be fully guaranteed as genuine or representing correctly the identity and, consequently, an ongoing identification procedure should generally be implemented.

74. A person's residential address is an integral part of the identity of the person and, thus, there needs to be a separate procedure for the verification of a customer's address. In the case that a customer's address is verified by an on-site visit of an officer of the credit institution, then a relevant note describing the event should be prepared and kept in the customer's file.

75. Credit institutions should verify the identity of the beneficial owners of accounts and one-off transactions and, for legal persons, they should obtain adequate information, data and documentation issued by independent and reliable sources so as to understand the ownership and control structure of the customer. Irrespective of the customer's type (natural or legal person, sole trader or partnership) credit institutions should request and obtain sufficient

information on the customer's business activities and the expected pattern and level of transactions. This information should be collected before the establishment of the business relationship and the execution of any transaction, with the aim of constructing the customer's business/economic profile, which, as a minimum, should include the following :

(i) The purpose and the reason for opening the account or requesting the provision of banking services.

(ii) The anticipated account turnover.

(iii) The nature of the transactions.

(iv) The expected origin of incoming funds (e.g. countries and names of principal counterparties) to be credited to the account and the expected destination (e.g. countries and names of principal counterparties) of outgoing transfers/payments. The source and size of the customer's wealth and annual income.

(v) Clear and detailed description of the main business/ professional activities/operations.

76. The above mentioned information as well as all data and information that form the customer's business/economic profile such as, in the case of legal persons, the name of the company, the country of its incorporation, the business address, the names and the identification information of the beneficial owners, management, and authorised signatories, ownership structure, financial information on 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) should be recorded in a separate form designed for this purpose that should be retained in the customer's file along with all other documents and account opening information/documentation as well as with all internal records of meetings with the respective customer. An identical form should also be designed and used for recording similar information that make up the business/economic profile of a customer who is a natural person. The said form should also be filed in the respective customer's file. The above mentioned forms should be updated regularly or whenever new information emerges that needs to be added to the business/economic profile of the customer or alters existing information that makes up the business/economic profile of the customer.

77. Transactions executed should be compared and evaluated against the anticipated turnover of the account, the usual turnover of the customer and the data and information kept that make up his business/economic profile. Significant deviations should be investigated and the findings recorded on a separate memo which should be kept in the respective customer's file. Any transaction that is not justified by the available information on the customer, should be

thoroughly examined so as to determine whether suspicions over money laundering arise for the purposes of submitting an internal report to the MLCO and then by the latter to MOKAS.

4.12 Reliance on third parties for customer identification and due diligence purposes

The Law Article 67

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

79. The Law (article 67) explicitly provides that the ultimate responsibility for performing the above mentioned measures and procedures remains with the credit institutions or the person who carries out the financial or other business activities which relies on the third person. Consequently, the responsibility to apply customer identification and due diligence procedures cannot be delegated to the third person.

The Law Article 67(2)

80. The Law defines as third person a credit or financial institution or auditors or accountants or tax consultants or independent legal professionals or persons providing to third parties trust and company services, as laid down in paragraphs (e) and (f) of the definition of the term "other business activities" (article 2 of the Law) governed by the European Union Directive and situated in the Republic or other country in the European Economic Area, and who:

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

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

81. Furthermore, the Law provides that the third persons could be any person carrying out financial activities as defined in Article 2 thereof or auditors or independent legal professionals or persons providing to third parties trust and company services as laid down in paragraphs (e) and (f) of the definition of the term "other business activities" (article 2 of the Law) operating in countries outside the European Economic Area which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing, hasdeemed that they apply procedures and measures for the prevention of money laundering and terrorist financing equivalent to those laid down in the European Union Directive. It is understood that the said third persons should meet the requirements mentioned in paragraph 80 above.

The Law Article 67(2)(c)

82. It should be noted that the terms “financial institutions” and “persons engaged in financial activities” do not include dealers in foreign exchange.

The Law
Article 67(3)

83. The Law provides that credit institutions should require from the third person to:

(i) provide them immediately with all available customer identification data, information and documents collected in the course of applying customer identification and due diligence procedures in accordance with the requirements of the Law; and

(ii) immediately forward to them relevant copies of the customer identification documents, data and information on the customer and the beneficial owner which the third person collected while applying the abovementioned procedures and measures.

The Law
Article 67(4)

84. Notwithstanding paragraph 83(ii) above, the relevant copies of identification documentation and other data and information on the identity of the customer and the beneficial owner are forwarded, immediately after a request by persons carrying out financial or other business activities, taking into account the degree of risk resulting from the type of customer, the business relationship, the product or the transaction, from the following third parties:

(a) Credit and financial institutions which fall under the scope of the European Union Directive and operate in the Republic or other country of the European Economic Area,

(b) any third parties carrying out financial activities, as defined in section 2 of the Law and operate in countries outside the European Economic Area, which according to a decision of the Advisory Authority for Combating Money Laundering and the Financing of Terrorism, hasdeemed that they impose equivalent procedures and measures for the prevention of money laundering and terrorist financing to those laid down by the EU Directive.

85. Moreover, the credit institution should obtain data and information so as to verify that the third person is subject to professional registration by law in its country of incorporation and/ or operation as well as subject to supervision for the purposes of compliance with the measures for the prevention of money laundering and terrorist financing. It is noted that credit institutions may rely on third parties only at the outset of establishing a business relationship for the purpose of ascertaining and verifying the identity of their customers. According to the degree of risk, any additional data and information for the purpose of updating the customer's business profile during the operation of the account or for the purpose of examining unusual transactions executed through the account, should be 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 on the management of funds and assets.

86. All copies of identification documents, data and information obtained by a credit institution should be duly certified by the third person as true copies of the original. Paragraphs 186-187 of this Directive as regards the certification of documents is relevant. In the cases where the third person on whom the credit institution relies for performing customer identification and due diligence procedures is an auditor, accountant, tax consultant or an independent legal professional or a trust and company services provider from a country of the European Economic Area or a third country that the Advisory Authority for Combating Money Laundering and Terrorist Financing has deemed to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive, then the credit institution is obliged, before accepting the customer identification data verified by the said third person, to apply the following additional measures/procedures:

    (i). Obtain a copy of the policy and procedures applied by the third person.

    (ii). Ascertain and evaluate the systems, policy and procedures applied by the third person for the prevention of money laundering and terrorist financing. The said assessment should be performed by the credit institution's MLCO.

    (iii). Collect data\information on the person appointed as Compliance Officer in accordance with Article 69(1) of the Law.

    (iv). As a result of the above mentioned assessment, the credit institution is satisfied that the third person implements customer identification, due diligence and record keeping systems and procedures are in line the requirements of the Law and this Directive.

    (v). The MLCO maintains a separate file for every third person where it stores the assessment report and other relevant information (identification details, records of meetings, evidence of professional registration by law etc).

    (vi). The MLCO assesses on an annual basis the business relationship with the third person.

    (vii). The MLCO keeps a register with data/information (e.g. name, business address, professional area of activities, supervisory authority, date of commencement of cooperation, date of last assessment, date of next assessment, assessment rating) on third persons with whom the credit institution has entered into cooperation.

    (viii). The MLCO gives his/her approval for the commencement of the cooperation with the third person and the acceptance of identification data verified by the third person.

4.13 Specific customer identification issues

4.13.1 Natural persons

87. Credit institutions ascertain the true identity of natural persons who reside in Cyprus or abroad by obtaining the following information:

    (i) True name and/or names used based on information from the official valid identity card or passport;

    (ii) Full permanent address, including postal code;

    (iii) Telephone and fax numbers;

    (iv) E-mail address;

    (v) Date and place of birth;

    (vi) Details on the profession and other occupations of the customer including the name of employer/business; and

    (vii) Specimen of signature.

88. According to the Business of Credit Institutions Laws of 1997 to 2013 the identification of a customer's identity should be always based on an official identity card or passport submitted by the beneficial owner of the account.

89. In this connection, credit institutions should maintain certified true copies of the pages containing the relevant information from the abovementioned documents. In addition, credit institutions are advised, if in doubt about the identity of any person (passport, national identity card), to seek its verification by the Ministry of Interior (competent issuing authority in the Republic) or the Embassy or the Consulate of the issuing country in Cyprus or a reputable credit or financial institution situated in the customer's country of origin. It is noted that the above mentioned documents should bear a photograph of the customer.

90. In addition to the name verification, the permanent address of the customer must be verified by using one of the following ways:

    (i) Visit at the place of residence (in such a case, the credit institution's officer who carries out the visit should prepare a memo which must be retained in the customer's file);

    (ii) The submission of a recent (up to 6 months) utility bill, (e.g. electricity, water) or copy of house insurance, municipal tax bill and / or a statement of bank account (for protection

against the submission of fake documents, the prospective customers should be required to submit the original documents).

91. Credit institutions should require and receive information, on public positions which the (prospective) customer holds or has held in the last twelve months, as well as on whether he is a close relative or associate of such individual, in order to determine if the customer is a 'Politically Exposed Person' (see Section 4.14.2.5 of this Directive).

92. In addition to the above, a reference from a reliable staff member or a reliable existing customer or a third person who is personally known to the management of the credit institution may facilitate the customer identification procedure. Details of such references should be recorded in the customer's file.

93. Having been satisfied that the original identification documents have been presented, credit institutions should keep copies of the pages containing all relevant information which must be certified as true copies of the original documents (see paragraphs 186-187 of this Directive).

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

95. Consequently, credit institutions are requested to inform immediately the Central Bank of Cyprus, in case they ascertain, eitherat the commencement or during the business relationship that the name of a prospective or existing customer appears in the lists of persons and entities subject to the restrictive measures, issued in accordance with relevant regulations of the European Union and United Nations Security Council Resolutions.

4.13.2 Joint Accounts

96. In the cases of joint accounts of two or more persons, the identity of all individuals that hold and/or have the right to handle the account, should be verified in line with the procedures set out above for natural persons.

4.13.3 Nominees or agents of third persons

The Law Article 65(1)

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

98. As a result of the above, credit institutions should take all necessary measures for the purpose of verifying and establishing the identity of the persons on whose behalf and for their benefit a nominee or agent is acting, that is, to ascertain the identity of the beneficial owners of the accounts. For this purpose, credit institutions should always obtain a copy of the authorisation agreement that has been concluded between the interested parties.

4.13.4 Accounts of unions, societies, clubs, provident funds and charities

99. In the case of accounts opened in the name of unions, societies, provident funds and charities, credit institutions should ascertain the objectives of their operation and satisfy themselves as to the legitimate purpose of the organisation by requesting the submission of their constitution/articles of association/rules of procedures and registration documents by the competent authorities (in case the law requires such registration). Moreover, credit institutions should obtain a list of the members of the Board of Directors/Management Committee and verify the identity of all individuals that have been authorised to manage the account in line with the identification procedures for natural persons.

4.13.5 Accounts of unincorporated businesses/partnerships

100. In the case of unincorporated businesses, partnerships and other entities without legal personality, the identity of their partners/directors/beneficial owners and of all persons duly authorised to operate the accounts, should be verified in line with the procedures applied for natural persons. Furthermore, in the case of partnerships, credit institutions should also obtain the original or a certified copy of the partnership's registration certificate. Credit institutions should also obtain documentary evidence of the trading address of the business/partnership and ascertain the nature and size of its activities and receive all the information required under Section 4.11 above for the creation of the business profile of the enterprise.

101. In cases where a formal partnership arrangement exists, credit institutions should also obtain a copy of the arrangement as well as a mandate from the partnership authorising the opening of an account and conferring authority on those who will be responsible for its operation.

4.13.6 Accounts of corporate customers (companies)

The Law Article 65(2)

102. Article 65 (2) of the Law provides that for customers that are corporate or legal entities, credit institutions should establish that the natural person appearing to act on behalf of the customer is appropriately authorised to do so and his/her identity has been established and verified.

103. Due to the difficulties in identifying the true shareholders / beneficial owners of the accounts, corporate accounts are one of the most favourable vehicles for money laundering, particularly when fronted by legitimate trading operations. Credit institutions should take all necessary measures for the full ascertainment of the company's control and ownership structure as well as the verification of the identity of the natural persons who are the beneficial owners and who exercise control over the company.

104. The identification of a company comprises the ascertainment of the following:

(i) Registered number;

(ii) Registered corporate name and trading name used;

(iii) Registered office address;

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

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

(vi) The members of the Board of Directors;

(vii) The persons that are duly authorised to operate the accounts of the company and act on behalf of the company.

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

(ix) The registered shareholders acting as nominees of the beneficial owners.

(x) The business profile of the company in accordance with the provisions of Section 4.11 above.

105. For the purpose of verifying the above data/documents, credit institutions must request and obtain, inter-alia, original or certified copies of the following documents:

(i) The company's Certificate of Incorporation;

(ii) Certificate of registered office;

(iii) Certificate of directors and secretary;

(iv) Certificate of registered shareholders in the case of private companies;

(v) Memorandum and Articles of Association;

(vi) A resolution of the Board of Directors, certified by the company's secretary, for opening an account and granting authority to those who will operate it;

(vii) In the cases where the registered shareholders act as nominees of the beneficial owner(s), a copy of the trust deed/agreement concluded between the nominee and the beneficiary of the account, by virtue of which the registration of the shares on the nominee's name on behalf of the beneficiary has been agreed;

(viii) Legal ownership structure certified by the Director of the Company;

(ix) Documents and data for the verification of the identity of the authorised signatories/agents of the company, the registered shareholder(s) and ultimate beneficial owner(s) in accordance with the provisions of this Directive.

106. For companies incorporated abroad, credit institutions should request and obtain equivalent documents and data similar to the above.

107. Where deemed necessary for a better understanding of the activities, sources and uses of funds/assets of a company, credit institutions should obtain a copy of its latest audited financial statements and/or a copy of its latest management accounts.

108. As an additional due diligence measure, and on the basis of the assessed risk emanating from the business relationship with a specific company, credit institutions should carry out a search and obtain information from the records of the Registrar of Companies in Cyprus (for domestic companies) or from a corresponding authority in the company's country of incorporation (for non-Cypriot companies) and/or request information from other sources (e.g. credit information agency) in order to establish that the applicant company is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and that the company continues to be registered by an appropriate authority in Cyprus or abroad as a going concern. It is pointed out that, if at any later stage any changes occur in the structure or the ownership status of the company or any suspicions arise emanating from changes in the nature, financial and economic purpose of the transactions performed by the company via its account, then it is imperative that further enquiries are made for ascertaining the nature and any consequences of these changes on the documentation

and information held by the credit institution for the company and determine as to whether, any supplementary information for updating the business profile of the company needs to be collected.

The Law Article 2

109. The Law (article 2) defines the term beneficial owner as being the natural person or the natural persons who ultimately own or exercise control over a customer. In the case of companies, the beneficial owner is considered to be:

(i) The natural person or natural persons who ultimately own or control a company by holding directly or indirectly, or controlling sufficient percentage of the shares or the voting rights of the company, inter alia, through bearer shares; a percentage of 10% plus one share, shall be deemed sufficient to satisfy this criterion.

(ii) The natural person or natural persons who otherwise exercise control over the management and administration of the company.

110. As a result of the above, in the case of a company requesting the opening of a bank account whose direct/immediate and principal shareholder is another company (parent/holding) registered in Cyprus or abroad, credit institutions are required, before opening the account, to establish the ownership structure and the identity of the natural persons who are the ultimate beneficial owners and/or control the parent/holding company.

The Law Article 2

111. The Law (article 2) requires that credit institutions look for the persons who have the ultimate control over the company's business and assets. Ultimate control will often rest with those persons who have the power to manage funds, accounts or investments without requiring authorisation and who would be in a position to override internal procedures. In such circumstances, credit institutions must also verify the identity of the natural person(s) who exercises ultimate control as described above even if that person has no direct or indirect interest or an interest of less than 10% in a company's share capital or voting rights.

112. In cases where the beneficial owner(s) of a company requesting the opening of an account is a trust set up in Cyprus or abroad, credit institutions are required to implement the procedure provided in Section 4.14.2.3 below.

4.13.7 Investment funds and persons engaged in the provision of financial and investment services

113. In the cases where credit institutions establish and maintain business relationships with persons involved in the provision of financial and investment services 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, has been deemed to be applying requirements equivalent to those laid down in the European Union Directive for the prevention of money laundering and terrorist financing, the requirements of Section 4.6 of this Directive should be applied on a risk sensitive basis.

114. In the case of business relationships established or maintained with persons who carry out the above activities and which are incorporated and/or operating in a third country other than those mentioned above, credit institutions should apply the following enhanced due diligence measures and procedures, in addition to the above mentioned due diligence measures required by the Law and this Directive for the identification and verification of natural and legal persons, including the ultimate beneficial owners:

(i) The approval of the MLCO before the commencement of the business relationship.

(ii) A copy of the licence or authorisation granted to the said person from a competent supervisory/regulatory authority, whose authenticity should be verified either directly by the relevant supervisory/regulatory authority or other independent and reliable sources;

(iii) A confirmation from the relevant supervisory/regulatory authority that the said person is subject to supervision in relation to the prevention of money laundering and terrorist financing.

(iv) Examine whether their licence provides for the provision of advisory and/or portfolio management services.

(v) Adequate documentation and sufficient information is obtained in order to fully understand the control structure and management of the business activities as well as the nature of the investment and financial services provided by the customer.

(vi) Monitoring of the transactions on a regular basis.

It is understood that the said customers cannot maintain "client accounts".

115. In case of establishing a business relationship with a company which is a subsidiary of another company (parent company) that provides financial and investment services, credit institutions should implement the provisions of paragraphs 113 and 114 in relation to the parent companies, depending on the country of incorporation and operation of the parent company.

116. In the case of investment funds, credit institutions, in addition to identifying the beneficial

owners, should obtain full 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.

4.13.8 Safe custody and safety deposit boxes

117. Particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, credit institutions should follow the identification and due diligence procedures prescribed in the Law and this Directive.

4.14 Procedures for high risk customers

4.14.1 Customer identification and due diligence on a risk sensitive basis

The Law Article 64(2)

118. Article 64(2) of the Law requires persons carrying out financial or other business activities to apply enhanced and additional customer due diligence measures in all instances which due to their nature entail a higher risk of money laundering or terrorist financing. It is reminded that the Customer Acceptance Policy of each credit institution should define the categories of high risk customers, as these are defined in the Law, in this Directive (Section 4.14.2), as well as the clients that the credit institution on its own has classified as high risk on the basis of the policy it has established.

119. In order to determine what constitutes sufficient customer identification, one should take into account each customer's perceived risk associated with money laundering and terrorist financing. The extent and the number of checks that must be carried out for customer identification may vary depending on the perceived risk of the customer's country of origin or the type of service, product or account requested by the customer, or the customer's background and professional or business activities as well as the level of the expected turnover and transactions or the complexity of the customer's ownership structure. Information on the source of funds, i.e. how payments will be made, from where and by whom should be recorded so as to facilitate future transaction checks.

120. However, for high risk products, accounts or customers, credit institutions should take additional measures for verifying their customers' identity, creating their business profile and ascertaining the source of assets i.e. how they have been acquired and their origin as well as monitor the movement of their transactions on a regular basis. In the cases where there is an accumulation of high risk customers and particularly when complex structures are combined with introduced business, credit institutions' enhanced due diligence measures should entail a

direct contact with the natural person who ultimately owns or exercise control over the customer. For this purpose, minutes should be prepared following every meeting and kept in the customer's file.

121. The credit institution should be in a position to prove to the Central Bank of Cyprus, if so requested in the context of the latter's supervisory function, that the extent of customer identification and due diligence measures implemented is proportional to the money laundering and terrorist financing risks faced.

4.14.2 High risk customers

122. Credit institutions must determine the categories of customers that are considered as high risk, on the basis of the risk assessment report prepared by the MLCO (see Section 3 of this Directive), as well as the enhanced due diligence measures that should be applied.

123. In addition, sections 4.14.2.1- 4.14.2.9 list the categories of customers designated as high risk either by the Law or the Directive of the Central Bank of Cyprus and, therefore, credit institutions are obliged, apart from normal customer identification and due diligence measures set out in the Law and this Directive, to perform enhanced due diligence as set out here below.

124. The MLCO should become aware of those prospective high risk customers the credit institution intends to accept, and acts as an advisor before the establishment of a business relationship. Therefore, for existing high risk customers the above said process should be implemented during the review process. The approval of the MLCO is required for the reclassification of high risk customers to a lower risk level.

4.14.2.1 Non-face to face customers

The Law Article 64(1)

125. Article 64(1) of the Law requires persons carrying out financial or other business activities to apply, when a customer is not physically present for identification purposes, one or more of the following additional customer due diligence measures:

(i) taking supplementary measures for certifying or verifying the documents submitted or requiring confirmatory certification from a credit institution or financial organization that falls within the scope of application of the European Union Directive;

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

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

127. Credit institutions should apply the below practical procedures for implementing the measure referred to in article 64(1)(a)(i) of the Law for the purpose of mitigating the higher risk involved in non-face to face customers:

(i) Direct confirmation of the prospective customer's true name, address and signature from a bank operating in the European Economic Area or a third country which the Advisory Authority for Combating Money Laundering and Terrorist Financing has deemed to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive or

(ii) Telephone contact with the customer at his residence or office, before the opening of the account, on a telephone number which has been verified from an independent source where the credit institution will verify any supplementary information on customer's identification that has been already obtained and

(iii) Contact with the customer through mail in an address previously verified by independent and reliable sources. Such communication should be in the form of a registered letter.

128. It is pointed out that the same requirements prescribed in article 64(1)(a) of the Law and this Directive are applied for companies or other legal persons requesting the opening of an account through mail, telephone or internet. Credit institutions should take additional measures for ensuring that the company or legal entity truly operates at its business address and carries out legitimate business activities.

4.14.2.2 Accounts in the names of companies whose shares are in the form of bearer

129. Credit institutions may accept as customers companies whose own shares or those of their parent companies (if any) have been issued in the form of bearer by applying, in addition to the procedures prescribed in Section 4.13.6 of this Directive, with regard to corporate customers the following supplementary due diligence measures:

(i) The credit institution obtains a written declaration from a third person, as this is defined in Article 67 of the Law and provided that the prerequisites stipulated in the said Article and Section 4.12 of this Directive are satisfied, or from the company's directors by which the identity of the beneficial owners is disclosed. Moreover, the credit institution obtains, duly certified by the said persons as true copies of the original, the relevant evidential records of the beneficial owners' identity.

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

(iii) If the opening of the account has been recommended by a third person as defined in article 67 of the Law, at least **once a year,** the credit institution must obtain from the third person who has introduced the customer a written confirmation that the capital base and the shareholding structure of the company or that of its holding company, as the case may be, 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 confirmation should be provided by the company's directors.

4.14.2.3 Accounts in the names of trusts and foundations

The Law Article 65(2)

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

The Law Article 2

131. The Law also requires that the identity of beneficial owners of legal entities, such as foundations, and legal arrangements such as trusts, to be verified as follows:

(i) When the future beneficiaries have already been determined, the natural person or natural persons who are the beneficiaries of 10% or more of the property of a legal

arrangement or entity.

(ii) When the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates.

(iii) The natural person or natural persons who exercise control of 10% or more of the property of a legal arrangement or entity.

132. Trusts do not form a separate legal entity and, therefore, a business relationship is established with the trustees who act on behalf of the trust. Consequently, trustees together with the trust should be considered as the credit institution's customers. When credit institutions enter into such relationships, they must ascertain the legal substance of the trust, and its name, country and date of establishment, and verify the identify of the settlors, trustees and beneficial owners as well as of other persons possessing considerable powers in the trust (e.g. protector, any investment advisor, accountant, any tax advisor).

133. Furthermore, credit institutions should ascertain the nature of activities and purpose of establishing the trust as well as the source and origin of funds. The verification procedure of the said information should be based on reliable data, documents or information. Consequently, credit institutions should request and check the trust deed and obtain copies of the relevant extracts of the said agreement, a certified copy of the registration of the said trust as provided in the Regulating Companies Providing Administrative Services and Related Matters Law or in any other equivalent law of another country or jurisdiction, as well as other relevant information provided by the trustees. All relevant details and information should be recorded and kept in the customer's file.

134. According to the FATF ''Report on the misuse of corporate vehicles'' a foundation may be used for similar purposes as a trust. A foundation is a legal entity carrying out activities and its income is derived from the principal assets and is used to fulfil the statutory purpose. A foundation is controlled by a board of directors and has no owners.

135. In this connection, as in the case of trusts, the identity of the founder, the beneficiaries, the Board of Directors and other persons who hold important powers in the foundation (e.g. a protector) should be verified. In addition, information such as the purpose of incorporation, the registered address and other relevant information should also be received by the credit institutions. Therefore, credit institutions should take copies of extracts from the articles of association or statute, where the latter exists, to verify the above information. All relevant data and information should be recorded and kept in the customer's file.

4.14.2.4 "Client accounts" in the name of third persons

136. In the context of the performance of their usual professional activities, third persons acting as intermediaries frequently hold funds on behalf of their clients in "client accounts" opened with credit institutions. Such accounts may be general or pooled accounts holding the funds of many clients or they may be opened specifically for a single client ("specific client account").

137. Credit institutions may open "client accounts" in the name of financial institutions from countries 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 deemed to be applying procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the European Union Directive, by applying, on a risk sensitive basis, the requirements laid down in Section 4.6 of this Directive.

138. "Client accounts" may be opened for Payment Institutions and Electronic Money Institutions which have been licensed by the Central Bank of Cyprus or for the representatives (branches or agents) of Payment Institutions and Electronic Money Institutions exercising the freedom of establishment, provided that the credit institution will apply at the start of the business relationship appropriate due diligence with respect thereto, as required by this Directive. For amounts equal to or exceeding 15.000 Euro, the Payment Institution, the Electronic Money Institution or the representative shall provide the credit institution with a statement of the names of clients and the corresponding amounts of the deposits. The credit institution, on a risk sensitive basis, may request the Payment Institution, the Electronic Money Institution or the representative to provide it with data and documents about the identity of their clients.

139. In the case in which a Class B Licensee, as defined in article 61(1) of the Betting Law 106(I)/2012, requests the opening of a pooled client account, credit institutions may proceed with its opening and maintenance provided that the following conditions are met:

    (i) The Licensee holds a Class B licence granted by the National Betting Authority and the said authority has notified the credit institution of the granting of such licence in accordance with the provisions of article 18 of the Betting Law. Credit institutions should request and obtain, in addition to the data and the information required by this Directive for the identification and verification of the identity of natural and legal persons, as the case may be, a copy of the licence granted to the said Licensee by the National Betting Authority.

(ii) The MLCO has assessed the customer identification and due diligence procedures employed by the Licensee and has found them to be in line with article 56 of the Betting Law and the Directives issued by the National Betting Authority under article 11(c) of the said Law. A record of the assessment should be prepared and kept in a separate file maintained for each Licensee.

(iii) During the operation of the account, the credit institution verifies the identity of the beneficiaries of credit transactions which equal or exceed 15.000 Euro. The credit institutions obtain all relevant customer identification data and other documentation regarding the beneficiaries, duly certified by the Licensee as true copy of the originals before the execution of any credit transaction which is equal to or greater than 15.000 Euro.

140. In the case that the opening of a "client account" is requested by a third person acting as auditor/accountant/tax advisor or independent legal professional or trust and company service provider or real estate agent 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 deemed to be applying procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the European Union Directive, credit institutions may proceed with the opening of the account provided that all requirements laid down in paragraph 86 of this Directive, as well as the following conditions are met:

(i) For general or pooled client accounts, the credit institution verifies the identify of all beneficiaries of credit transactions which equal or exceed 15.000 Euro.

(ii) With regard to specific client accounts, the credit institution verifies the identity of the beneficiary(ies) before opening the account.

(iii) The credit institution obtains all relevant customer identification data and other documentation for the beneficiaries duly certified by the third person as true copy of the originals upon opening the account or before the execution of any credit transaction, as the case may be.

141. Client accounts may be opened to the administrator of buildings or houses in relation to the collection of communal or other expenses by the owners, provided that the credit institution will apply at the start of the business relationship the appropriate due diligence with respect thereto, as required by this Directive. It is noted that the credit institution should receive a copy of the relevant agreement concluded by the two parties.

142. In the cases referred to in paragraphs 139-141 it is pointed out that credit institutions may open general client accounts ("pooled accounts") provided that the credit institution can hold sub-accounts or connected accounts in its system and is in a position to know, and has verified, the identity of the beneficial of credit transactions for amounts equal to or exceeding 15.000 Euro. Otherwise, a specific client account should be opened and the identity of the beneficial owner should be verified before the opening of the account. Supporting documentation related to the specific transactions should also be obtained.

143. For all the above cases, credit institutions should exercise ongoing monitoring of the above mentioned business relationships and transactions. The said business relationships should be reviewed on an annual basis.

4.14.2.5 Accounts for Politically Exposed Persons ("PEPs")

The Law Article 64(1)(c)

144. Article 64(1)(c) of the Law requires that, in respect of transactions or business relationships with PEPs residing in the Republic or in a foreign country, persons carrying out financial or other business activities should apply the following:

(i). have appropriate risk-based procedures to determine whether the customer or the beneficial owner is a PEP;

(ii). have Senior Management approval for establishing business relationships with such customers, or continuing the aforementioned relationships or continuing the relationship with existing customers which in the meantime have become PEPs;

(iii). take adequate measures to establish the source of assets and the origin of funds; and

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

The Law Article 2

145. The Law (article 2) defines that politically exposed persons means natural persons who have or had been entrusted with prominent public functions in the Republic or in a foreign country, as well as immediate family members, or persons known to be close associates, of such persons.

146. Business relationships with individuals holding important public positions and with natural or legal persons closely related to them, may expose a credit institution to enhanced risks, especially, if the potential customer seeking to establish an account is a PEP, a member of his immediate family or a person that is known to be a close associate of a PEP. Credit institutions

should pay more attention when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering statutes and regulations are not equivalent with international standards. In order to manage effectively such risks, credit institutions should assess which countries among those with which they maintain business relationships are more vulnerable to corruption or maintain laws and regulations that do not meet the Recommendations of the Financial Action Task Force (see Section 4.14.2.9 of this Directive). With regard to the issue of corruption a 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 Recommendations of the FATF, credit institutions may retrieve information from the country assessment reports prepared by FATF or other regional bodies operating in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe), the International Monetary Fund and the World Bank.

147. For the purpose of this Directive, PEPs include the following natural persons:

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

1. heads of State, heads of Governments, ministers and deputy or assistant ministers;
2. members of parliaments;
3. members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
4. members of courts of auditors or of the boards of central banks;
5. ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
6. members of the administrative, management or supervisory bodies of State-owned enterprises.

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

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

1. the spouse;
2. any partner considered by national law as equivalent to the spouse;
3. the children and their spouses or partners;

4. the parents.

(iii) Persons known to be "close associates" of a PEP include the following:

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

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

148. 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 paragraph 147 above, for a period of at least one year, credit institutions shall not be obliged to consider such a person as politically exposed.

149. Credit institutions should adopt, further to the above legal requirements, the following additional due diligence measures when they open an account and/or establish a business relationship with a PEP:

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

(ii) The decision for establishing a business relationship with a PEP should be taken by a senior management executive of the credit institution following a brief report on the customer's profile prepared by a competent officer of the credit institution.

(iii) When establishing a business relationship with a customer (natural or legal) and subsequently it is ascertained that the person(s) involved are or have become PEPs, then the approval of the credit institution's Senior Management should be given for continuing

the operation of the business relationship and/or account. In this respect, credit institutions' systems must filter on a regular basis and not less frequently than once a month, their customers (and physical persons related to them) for such cases.

(iv) Before establishing a business relationship with a PEP, the credit institution should obtain adequate documentation to ascertain not only his/her identity but also to assess his/her business reputation and integrity (e.g. references from third parties);

(v) Credit institutions should establish the business profile of the account holder by obtaining the information detailed in Section 4.11 above. The profile of the expected business activity should form the basis for the future monitoring of the account. The profile should be regularly reviewed and updated with new data and information. Credit institutions should be particularly cautious and most vigilant where their customers are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks; and

(vi) The account and the business profile of the customer should be subject to **annual review** in order to determine whether to allow the account to continue operating. A note should be prepared summarising the results of the review by the credit institution's officer in charge of the account. The note should be submitted for consideration and approval to the credit institution's Senior Management and filed in the customer's personal file.

4.14.2.6 Correspondent accounts of banks outside European Union

The Law Article 64(1)(b)

150. Article 64(1)(b) requires for cross-border correspondent banking relationships with credit institutions from third countries outside the European Union, the application of the following enhanced due diligence measures:

(i). Gathering adequate information for the credit institution-customer so as to fully understand the nature of its business and assess, using publicly available information, its reputation and the quality of its supervision.

(ii). Assessing its systems and procedures in place for the prevention of money laundering and terrorist financing.

(iii). Obtaining the approval of the Senior Management before entering into new correspondent bank account relationships.

(iv). Document the respective responsibilities of the person engaged in financial activities and of the credit institution-customer.

(v). With regard to payable-through accounts, it must be ensured that the credit institution-customer has checked the identity and performed on-going due diligence on the customers who have direct access to the correspondent bank accounts and that it is able to provide customer due diligence data upon request of the credit institution-correspondent.

151. In addition to the above measures, credit institutions should ensure that the following conditions are met:

(i) The correspondent bank is either connected to a regulated financial group or maintains a physical presence in the form of a fully-fledged office carrying out true banking business in its country of incorporation i.e. the correspondent bank is not a "shell bank". "Shell bank" is a credit institution which does not have a physical presence, including a real address and management, in the country of its incorporation and which is not connected to a regulated financial group. The physical existence of a bank and its regulated status should be checked by one of the following means:

- Checking with the home country Central Bank or the competent supervisory authority of the country of incorporation, or
- obtaining from the correspondent bank evidence of its group structure as well as licence or authorisation to conduct banking and financial business.

(ii) The correspondent bank employs adequate procedures to prevent money laundering and terrorist financing. In this regard, the MLCO should obtain and evaluate information on the correspondent bank's customer acceptance policy and identification procedures as well as anti-money laundering and terrorist financing measures in general. The MLCO must ensure that the correspondent bank does not provide any services neither allows the use of its correspondent bank accounts by shell banks. In addition, it must be ascertained whether the correspondent bank has been subject to a special investigation for the purpose of preventing money laundering or terrorist financing by the competent supervisory authority of its country of origin or operation and as to whether any administrative sanctions have been imposed by the supervisory/regulatory authority of its country of origin and/or operation for inadequate preventive measures. It is noted that the Law requires the approval of the Senior Management of the credit institution prior to entering into new correspondent banking relationships.

(iii) The credit institution collects sufficient information to establish fully the nature of the correspondent's business activities, ownership structure, management and places of operations and verifies the identity of its beneficial owner(s). In addition, the credit

institution assesses, using publicly available information, the reputation and the quality of supervision of the correspondent bank. Additional information on the correspondent bank can be obtained from "The Bankers' Almanac", "Thomsons' Directories" or other international services providing professional information as well as correspondent banks operating in the country of registration of the bank.

(iv) The correspondent bank account must be operated by duly approved officials of the bank in the name of which the account is maintained.

(v) The relevant agreement for the correspondent banking relationship must adequately document what is mentioned in sub-paragraphs (ii) and (iv) above, as well as the respective responsibilities of the two banks.

(vi) The account of the correspondent bank as well as the information that form the business/economic profile should be examined and reviewed, respectively, on an annual basis or whenever it becomes known that data and information held by the credit institution are not adequate and reliable, or a transaction takes place that appears to be unusual and/or significant compared to the normal pattern of transactions and the business/economic profile of the correspondent bank or there is a significant change in the correspondent's bank legal status and situation. The outcome of the above should be recorded in a separate note/form which should be kept in the respective correspondent bank's file.

4.14.2.7 Services to private banking customers

152. Private banking services offer the personal and discreet delivery of a wide variety of financial services and products to high net worth individuals and institutional investors. A customer's needs will often entail the use of complex products and fiduciary services, sometimes involving more than one jurisdiction, including trusts, private investment vehicles and other company structures. Where such legal vehicles and structures are used, it is important that credit institutions ascertain their legitimacy and their financial/commercial objective, as well as the ownership layers so that they establish who the beneficial owner is.

153. The role of the relationship officers is particularly important to the credit institution in managing, controlling and mitigating the money laundering or terrorist financing risks it faces. Relationship officers develop strong personal relationships with their customers, which can facilitate the collection of the necessary information to know the customer's business, including knowledge of the source(s) of the customer's wealth. Having in mind that there are some practices and products within the private banking operations that pose unique

vulnerability to money laundering, credit institutions are required to establish enhanced due diligence procedures for the acceptance and ongoing maintenance of private banking relationships. In this regard, in addition to the identification requirements of this Directive for natural or legal persons, as the case may be, credit institutions should adopt and apply the following additional due diligence measures whenever they enter into a private banking relationship:

(i). All new private banking customers should be subject to independent review by thecredit institution's officers and Senior Management's approval.

(ii). The credit institution must obtain data and information so as to be satisfied that a customer's use of complex business structures and/or the use of trust and private investment vehicles, have a genuine, legitimate and financial/commercial purpose.

(iii). Credit institutions should establish the business profile of the account holder by obtaining the information prescribed in Section 4.11 above. The anticipated account activity, the source of wealth (description of the economic activity which has generated the net worth), the estimated net worth, the source of funds (description of the origin and the means of transfer of money credited to the account during the opening) will form the basis for the future regular monitoring of the account.

(iv). The credit institution should carry out a search as a normal part of customer due diligence, before entering into a business relationship which will include checks for negative information. Based on the perceived risk, a credit institution may obtain a satisfactory written reference or references from a reliable, independent source or sources before opening an account for a customer. Such references should only be accepted when they are:

- received directly from the referee;
- specifically addressed only to the credit institution; and
- verified as truly issued by the referee.

(v). After a business relationship has been established, customer identification data and information that make up the customer's business profile should be reviewed and updated on a regular basis. In this respect, a credit institution must undertake, on a regular basis, checks and reviews of its business relationship with the customer, examining the movement of account, the nature of transactions, the banking products supplied as well as the adequacy of the identification data and information maintained. The outcome of the above should be recorded in a separate note/form which should be kept in the respective customer's file.

4.14.2.8 Electronic gambling /gaming through the internet

154. Credit institutions may enter into business relationships and open accounts in the names of persons who are involved in the activities of electronic gambling / gaming through the internet provided that these persons are licensed by a competent authority of a country of the European Economic Area or a third country which applies sufficient measures for the licensing and supervision of such businesses. For this purpose, credit institutions must request and obtain, apart from the information required by this Directive for customer identification, as the case may be, a copy of the licence that has been granted to the subject person by the competent supervisory/regulatory authority, the authenticity of which must be verified either directly with the supervisory/regulatory authority or by other independent and reliable sources.

155. Furthermore, credit institutions must collect adequate information so as to understand customers' control structure and ensure 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.

156. In the case that a credit institution's customer is a person who offers services (e.g. payment providers, software houses, card acquirers) to the persons mentioned in paragraph 154, then the credit institution must request and obtain, apart from the information required by this Directive for customer identification of natural or legal persons, as the case may be, adequate information so as to be satisfied that the services are offered only to licensed persons. Moreover, credit institutions should obtain information necessary to fully 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 business profile. Additionally, the credit institution must obtain the signed agreement between its customer and the company duly licensed by the competent authority of a country referred to in paragraph 154 above to be engaged in electronic gambling/gaming through the internet activities.

157. In all the above cases, the decision for opening the account must be taken or approved by a member of the Senior Management of the credit institution. Moreover, the account must be closely monitored and subject to regular review with a view to deciding whether or not to permit the continuance of its operation. The outcome of the above should be recorded in a separate note/form which should be kept in the respective customer's file.

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

158. The Financial Action Task Force ("Financial Action Task Force on Money Laundering-FATF") was established in Paris in 1989 at the Summit of the heads of State or Governments of the G-7 and the President of the European Commission, in response to increased concerns about money laundering. The Task Force's responsibility is to investigate money laundering methods, review the action which has already been taken at national and international level, and put forward new measures to combat money laundering. Furthermore, in 2001 the FATF issued Recommendations for combating the financing of terrorism.

159. Today, the Recommendations of the FATF constitute the foremost internationally recognized standards for the prevention and detection of money laundering. The Government of Cyprus has formally endorsed the FATF's Recommendations and has directly assured the President of the FATF that the competent authorities of Cyprus will take all necessary actions to ensure full compliance and implementation of the Recommendations. In this regard, the Central Bank of Cyprus is committed to the implementation of FATF's Recommendations and all its other related initiatives in an effort to reduce the vulnerability of the banking system to money laundering and terrorist financing activities.

160. In this respect, credit institutions are required to apply the following:

1. Exercise additional monitoring procedures and pay special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or they apply inadequately the aforesaid Recommendations.

2. Transactions with persons from the aforementioned countries with no apparent economic or visible lawful purpose, should be further examined with the aim of ascertaining their financial, commercial or investment motives. If a credit institution does not receive sufficient information and clarifications and thus cannot satisfy itself as to the legitimacy of a transaction, then a suspicious transaction report should be filed through the MLCO with MOKAS.

161. With the aim of implementing the above, the MLCO should obtain and study the announcements and the country assessment reports prepared by FATF (http://www.fatf-gafi.org), the other regional bodies that have been established and work on the principles of FATF (e.g. Moneyval Committee of the Council of Europe www.coe.int/moneyval), the International Monetary Fund and the World Bank. Based on the aforesaid reports, the risk from transactions and business relationships with persons from various countries must be

assessed and, when deemed necessary, enhanced due diligence measures should be applied for identifying and monitoring transactions of persons from countries with significant shortcomings in their legal and administrative systems for the prevention of money laundering and terrorist financing. In this regard, the MLCO should decide on the countries that appear not to adequately apply FATF's Recommendations and for which enhanced due diligence measures should apply for business relationships and transactions originating from those countries.

4.15 On-going monitoring of accounts and transactions

The Law Article 61(1)(d)

162. Article 61(1)(d) of the Law requires persons engaged in financial or other business to conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with data and information maintained by the person who carries out financial or other business in respect of the customer, the business and the risk profile of the customer, including the source of funds as well as ensuring that the documents, data or information held are kept up-to-date.

The Law Article 58(e)

163. Article 58(e) of the Law requires credit institutions, inter alia, to examine in detail any transaction which by its nature may be associated with money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

164. **Appendix 2** of the Directive of the Central Bank of Cyprus "A framework of principles of operation and criteria for assessment of banks' organizational structure, internal governance and internal control systems" which defines the "Principles for a sound and an effective operation of information technology systems in the context of managing a bank's operational risk" requires credit institutions to apply for the systems and services provided through the internet, inter alia, the following:

- automated systems for the monitoring of transactions, whose effective operation will be based on the creation, by the credit institution, of statistical models of customers' transactions. These systems, based on the profile established for each customer, should be in a position to identify any transactions indicating extraordinary behaviour and produce, in real time, alerts for the investigation of potential cases of fraud;
- effective management of the risk of money laundering and terrorist financing. These risks are particularly pronounced in the electronic transactions as these services are available from anywhere, at any time, also because of the impersonal nature of transactions and their

automatic processing. Consequently, credit institutions are expected to install filters and monitoring tools/systems which, as a minimum, will impose limits on specific groups or categories of transactions, thus, providing the possibility of delaying the execution of a transaction until the verification of specified details etc;

- capability of easily accessing and processing the details of old transactions, thus, making it feasible to identify particularities and/or irregularities in transactions, which help to establish evidence and provide sufficient information to the supervisory authorities, especially in the cases of fraud, money laundering, terrorist financing, provision of investment services etc;

165. On-going monitoring of customers' accounts and transactions is an essential aspect of effective money laundering and terrorist financing preventive procedures. Credit institutions should have a full understanding of normal and reasonable account activity of their customers as well as of their business 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, credit institutions will not be able to discharge the duty to report suspicious transactions/activities to MOKAS. It is noted that in accordance with Article 70 of the Law persons carrying out financial or other business activities are required to refrain from executing transactions known or suspected to be associated with money laundering or terrorist financing before informing MOKAS for their knowledge or suspicions, as prescribed in Articles 27 and 69 of Law.

166. The procedures and intensity of monitoring accounts and examining transactions should be risk sensitive and, as a minimum, should achieve the following:

- Identifying from a credit institution's records all high-risk customers as defined by the Law, this Directive and the Customer Acceptance Policy adopted by each credit institution. The management information system of each credit institution should be able to produce detailed lists of each group of high risk customers so as to facilitate enhanced monitoring of accounts and transactions.
- Detecting unusual or suspicious transactions that are inconsistent with the business profile of the customer for the purposes of further investigation.
- The investigation of unusual or suspicious transactions from the competent officers who have been appointed for this purpose. The results of the investigations should be recorded in a separate memo and kept in the file of the customer concerned.

- Based on the investigation findings, all necessary measures and actions must be taken including any internal reporting of suspicious transactions/activities to the MLCO.
- Ascertaining the source and origin of the funds credited to accounts.

167. In order to accomplish the above, credit institutions should introduce and implement adequate automated/ electronic management information systems which will be capable of supplying, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of customer accounts and transactions to the Senrior Management, the MLCO and other competent officials based on the assessed risk of these accounts and transactions in relation to money laundering or terrorist financing purposes. The monitoring of accounts and transactions must be carried out in relation to specific types of transactions, the business profile of the client, by comparing on a regular basis the actual movement of the account with the expected turnover as declared when opening the account, as well as with the movement of accounts and the nature of the transactions conducted by other customers engaged in similar business activities. Significant deviations must be further investigated and the relevant findings recorded in an appropriate memo which should be kept in the customer's file. Furthermore, the procedures should cover customers who do not have a direct contact with the credit institution as well as dormant accounts exhibiting unexpected movements. The automated / electronic management information systems should be used to extract information in connection with data missing from the documents used for account opening, identification data and information needed for the construction of a customer's business profile, as well as any other information pertaining to the business relationship of the customer with the credit institution.

168. For all accounts in general, automated/electronic management information systems should be 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, the incoming and outgoing transfers made over a predetermined limit) taking into account the business profile of the customer, the country of his origin, the source of the funds, the type of transaction or other risk factors. Particular attention should be given to transactions exceeding the threshold limits. Some types of transactions should alert the credit institution that a customer might be involved in unusual or suspicious activity. These may include transactions that do not seem reasonable based on usual business or commercial terms or transactions involving large sums of money in cash or

other financial instruments or fairly large incoming transfers that are not consistent with the normal pattern of a customer's transactions. Significant movement of the account, incompatible with the size of the account balance, may be evidence that money is laundered through that account.

5. CASH DEPOSITS AND WITHDRAWALS

5.1 Cash Deposits

169. Large cash deposits from illicit activities are considered to be one of the most popular methods of money laundering. Therefore, the most effective way to prevent money laundering as well as to recognise money laundering activities, has its origins at the initial placement stage when criminals attempt to deposit cash derived from illegal activities into the financial system.

170. Consequently, credit institutions are required to implement appropriate internal procedures for the acceptance and control of cash deposits for amounts exceeding 15.000 Euro or the equivalent in foreign currencies. In particular, credit institutions are required to implement procedures, on a risk sensitive basis, to ascertain the source and origin of cash and establish as to whether the level and nature of transaction is consistent with the activities and the business profile of the customer effecting the cash deposit. Furthermore, depending on the limits and controls that each credit institution puts in place, supporting documentation and data on the financial, commercial and other purpose of the transaction in cash should be obtained. The cash deposit transaction should be executed after approval by a senior official is granted to that effect. Similar checks should also be made for cash deposits below 15.000 Euro or the equivalent in foreign currencies when suspicions arise that the transaction is likely to be connected with money laundering or terrorist financing activities.

5.2 Deposits of cash imported from abroad

5.2.1 Prohibition of accepting cash deposits in foreign currency notes that have been imported from abroad.

171. Credit institutions are prohibited from accepting cash deposits in foreign currency notes of value of 10.000 Euro or more that have been imported from abroad when:

(i) the said cash deposits are not accompanied by the relevant declaration form of the Department of Customs and Excise "Declaration of Cash" in accordance with the Regulation (EC) 1889/2005 of the European Parliament and of the Council regarding the controls of cash entering or leaving the Community, and the Control of Cash Entering or Leaving the Community and the Exercising of Intra-Community Cash Controls Law (No.53(I) of 2009), or

(ii) the declaration form of imported cash contains incomplete, incorrect or false information.

172. In this regard, it is noted that according to Regulation (EC) 1889/2005 of the European Parliament and of the Council regarding the controls of cash entering or leaving the Community and the Law on the controls of cash entering or leaving the Community and exercise of cash controls within the Community, any natural person entering the Republic, from a third country or another member state of the European Union, carrying cash of value of 10.000 Euro or more, is obliged to declare the said amount to a competent officer of the Customs and Excise Department.

173. In the case of cash deposits in foreign currency that have been imported from abroad and are equal to or exceed the aforementioned limit, credit institutions are required to obtain and file together with the transaction, the original customs declaration form. Credit institutions are obliged to inform directly the Department of Customs and Excise of those cases of customers who request to deposit cash in foreign currency notes which have been imported from abroad that are not accompanied by the relevant declaration form, or the declaration form contains incomplete, incorrect or false information.

5.2.2 Acceptance of cash deposits in foreign currency

174. One-off deposits in foreign currency notes which have been imported in Cyprus from abroad in excess of the equivalent of 100.000 Euro, from any person or a group of connected persons, should be accepted only with the prior written approval of the MLCO of the credit institution concerned.

175. In addition, deposits of foreign currency notes which occur on a continuous and regular basis and which exceed or are expected to exceed the equivalent of 100.000 Euro, in the same calendar year, by any person or a group of connected persons, should be accepted only with the prior written approval of the MLCO of the credit institution concerned. Notwithstanding the above, a single cash deposit below the threshold limit of the equivalent of 100.000 Euro, by a person or a group of connected persons, should be accepted only with the prior written approval of the MLCO, if as a result of accepting it, the aggregate amount of cash deposits effected by a particular person or a group of connected persons, in the same calendar year, will exceed the amount of the equivalent of 100.000 Euro.

5.2.3 Definition of connected persons and connected cash deposits

176. A ''group of connected persons'' is defined to be:

(i) Members of a family (i.e. husband, wife, children);

(ii) A natural person and an enterprise in which the natural person and any member(s) of his/her family is a partner or shareholder or director or beneficial owner or has control in any other way;

(iii) Anatural person and a company in which the natural person is a manager or has a material interest either on his own or together with any member(s) of his/her family or together with any partners;

(iv) A legal person and a parent/holding company, subsidiaries, fellow subsidiaries, associated companies or entities which have a material interest in that person; and,

(v) two or more persons, natural or legal, which are financially inter-dependent or connected in such a manner that may be viewed as representing a single risk.

177. For the purposes of this Directive, "material interest" in a company means an interest in excess of 10% in any class of shares of the company or an interest which enables its holder to effectively appoint and control the majority of the company's directors or exercise important influence.

5.2.4 Internal procedures and responsibilities of the Money Laundering Compliance Officers

178. Applications for the acceptance of deposits in foreign currency notes as reported in the paragraphs above should be submitted in writing to the MLCO by the competent officer of the credit institution's branches/units where the customer concerned maintains his/her account(s) and must be accompanied by complete information on the customer, his/her activities, the nature of the proposed transaction, the source of cash and, for customers who intend to effect cash deposits on a continuous and regular basis, copies of their most recent annual audited accounts and/or management accounts. The MLCO, after examining the application and the information submitted, should communicate in writing his decision for the acceptance or not of the single deposit (if the transaction concerns a customer who intends to effect an one-off cash deposit) or the acceptance of a series of deposits (if the transaction concerns customers who intend to effect cash deposits on a continuous and regular basis). Copies of the application and the decision of the MLCO should be kept in a

separate file by the MLCO as well as in the file of the customer concerned.

179. The MLCO should ensure, in the context of implementing the "know your customer" principle and before giving his written approval for the acceptance of an one-off cash deposit or cash deposits on a continuous and regular basis in excess of the predetermined limits, that the size of the one-off deposit or the series of deposits in foreign currency is consistent with the financial condition, the cash flow outlook of the business and other activities of the customer concerned. Furthermore, the MLCO should ensure that the customer identification and due diligence procedures, set out in Section 4 of this Directive, are duly applied and that the cash involved is not suspected to be associated with any illicit activities.

180. The MLCO should record and maintain full information on the customers or the group of connected customers (name, address, account number(s), branch/unit where the account is maintained) in relation to whom he has given his written approval for the acceptance of an one-off cash deposit or cash deposits on a continuous and regular basis. In this regard, the MLCO should maintain two separate registers of customers who are involved in: (i) one-off foreign currency cash deposits, and (ii) foreign currency cash deposits on a continuous and regular basis.

181. The MLCO should monitor, at least on a monthly basis, the volume of deposits in foreign currency effected by the customers in relation to whom he has given his written approval for the acceptance of such deposits on a regular and continuous basis. In this context, the MLCO should prepare a monthly analytical statement with information on foreign currency cash deposits effected by the said customers during the month under review as well as on the accumulated deposits for the period i.e. from the beginning of the year until the end of the month under review.

5.2.5 Exempted cash deposits in foreign currency.

182. Notwithstanding the above, the following exemptions apply:

(i) Deposits of foreign currency from the Government of the Republic of Cyprus.

(ii) Deposits of foreign currency from semi-governmental organisations in Cyprus.

(iii) Deposits of foreign currency notes from other credit institutions licensed to operate in or from within Cyprus.

5.3 Cash Withdrawals

183. Large sums of cash withdrawals can expose the credit institutions to risk, especially when the money is used by the final recipients for the financing of illicit activities.

184. Consequently, credit institutions are requested to apply appropriate procedures to monitor cash withdrawals for sums that exceed 15.000 Euro or the equivalent in foreign currencies. In particular, credit institutions, depending on the assessed risk, have to implement procedures to ascertain the purpose and the destination of funds as well as to establish as to whether the transaction is consistent with the business activities and the business profile of the customer concerned. Moreover, and depending on the limits and controls that each credit institution puts in place, credit institutions must request and obtain the appropriate supporting documentation and data for the economic, commercial or other purposes of each cash withdrawal which will be performed with the prior approval by a senior official.

6. RECORD KEEPING PROCEDURES

6.1 Introduction

The Law Articles 68(1) and 68(2)

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

(i) Copies of the customer identification evidence;

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

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

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

186. The copies of the customers' identification evidence should be certified by the credit institution's employee who verifies the identity of the customer or the third person on whom the credit institution relies for the purpose of customer identification and due diligence procedure. The aforementioned certification should bear the name of the person certifying the copies, his/her signature and the date of certification.

187. For non-Cypriot natural persons and / or legal persons or entities incorporated outside Cyprus, credit institutions may obtain documents bearing the stamp Apostille, in accordance with the Hague Convention, and which are officially translated into Greek or English. These documents, which bear the Apostille stamp, must be the original and carry the distinctive serial number which has been designated by the Central Authority in the country of issue. The credit institution must communicate with the aforesaid Central Authority in the country of issue to confirm the authenticity of the documents' origin.

The Law Articles 68(3)

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

189. Moreover, credit institutions must apply appropriate systems which will enable them to

promptly identify and inform the Central Bank of Cyprus and MOKAS as to whether they maintain or have maintained, during the previous five years, a business relationship with specific natural or legal persons and on the nature of that business relationship.

190. It is noted that, in accordance with the Directive of the Central Bank of Cyprus on "A Framework of Principles of Operation and Criteria of Assessment of Banks' Organisational Structure, Internal Governance and Internal Control Systems", issued in May 2006, credit institutions must establish appropriate procedures to ensure the maintenance of books and records in a systematic and secure manner for a time period of not less than 10 years and in a manner which facilitates an audit trail and the reconstruction of all transactions in a chronological order, the verification of each recorded transaction against original vouchers and the validation of any changes in the balances of accounts with supporting data covering all transactions leading to the aforementioned changes.

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

(i) the identity of the account holder(s);

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

(iii) the identity of the authorised signatory(ies) to the account;

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

(v) connected accounts;

(vi) for selected transactions:

1. the origin of the funds;

2. the type and amount of the currency involved;

3. the form in which the funds were placed or withdrawn i.e. cash, cheques, funds transfers etc.;

4. the identity of the person undertaking the transaction;

5. the destination of the funds;

6. the form of instructions and authority; and

7. the type and identifying number of any account involved in the transaction.

6.2 Format of records

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

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

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

The Law Article 47

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

6.3 Electronic funds transfers

Regulation (EC) no. 1781/2006

196. In relation to the above subject, credit institutions are required to apply Regulation (EC) no. 1781/2006 on information on the payer accompanying transfers of funds which was published in the Official Journal of the European Union on 8 December, 2006 (OJ L 345 of 8.12.2006, pg.1).

197. Credit institutions should apply procedures so as to promptly identify incoming funds transfers in excess of 1.000 Euro that are not accompanied by full information on the payer,

as that information is detailed in the above Regulation.

198. In case where any of the requisite information is missing from the message or payment form accompanying the incoming funds transfer, then credit institutions should consider, depending on the perceived risk of money laundering associated with the relevant transaction, whether it is advisable to apply one or more of the following measures:

1. Contact the ordering customer's credit institution and request that complete information be made available on the ordering customer. If the aforesaid credit institution refuses or is unable to provide the missing information, then the credit institution may decide not to accept the funds transfer and return it to the ordering customer's credit institution.
2. Consider whether the lack of full information on the ordering customer raises suspicions for money laundering which need to be reported to MOKAS.
3. In the light of past experience with the ordering customer's credit institution and the circumstances of the transaction, consider as to whether the business relationship with the originating financial institution should be restricted or terminated.

The Law
Article 71

199. It is noted that Article 71 of the Law provides that the non-execution or delay in the execution of any transaction for the account of a customer due to the non-provision of sufficient details or information for the nature of the transaction and/or the parties involved, as required by the Directives of the competent supervisory authority or Regulation (EC) no. 1781/2006 of the European Parliament and of the Council of 15th November, 2006 on the information on the payer accompanying transfers of funds, does not constitute breach of any contractual or other obligation by the credit institution to its customers.

7. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES

7.1 Introduction

200. Although it is difficult to comprehensively define a suspicious transaction, as the types of transactions which may be used by criminals who are involved in 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 for that type of account. It is, therefore, imperative that bankers ensure that they maintain adequate information and know enough about their customers' business in order to recognise that a transaction or a series of transactions is unusual or suspicious.

7.2 Examples of suspicious transactions/activities

201. A potential money launderer who attempts to launder illicit funds or to be involved in terrorist financing activities will use any service offered by a credit institution as a means of changing the nature of money from illegal to lawful. This process could possibly range from a simple cash transaction to more sophisticated and complex transactions. A list containing examples of what might constitute suspicious transactions/activities related to money laundering and terrorist financing is attached as **Appendix 5** to this Directive.

202. The abovementioned list is not exhaustive nor includes all types of transactions that may be used. The list must be constantly updated and revised to include new ways and methods that are used for money laundering and terrorist financing. Nevertheless, the list can assist the credit institutions and their staff in recognising the main methods used for money laundering and terrorist financing. The detection by credit institutions of any of the transactions contained in the aforesaid Appendix should prompt further investigation and constitute a valid cause for seeking additional information and / or explanations as to the source and origin of the funds, the nature and the financial / commercial purpose of the underlying transaction, as well as the circumstances surrounding the particular activity.

7.3 Internal reporting suspicious transactions and activities

The Law Article 27

203. Under Article 27 of the Law it is an offence for any person who knows or reasonably suspects that another person is engaged in money laundering or financing of terrorism offences, and does not report to MOKAS this information, as soon as is reasonably practical, after it comes to his/her attention. Failure to report in these circumstances is

punishable with a maximum of five (5) years imprisonment or a fine not exceeding 5.000 Euro or both of these penalties.

The Law
Article 26

204. In the case of credit institutions' employees, article 26 of the Law, recognises that internal reporting to the MLCO will satisfy the reporting requirement imposed by virtue of Article 27. This means that once a credit institution's employee has reported his/her suspicion to the MLCO he or she is considered to have fully satisfied his/her statutory requirements, under Article 27. Consequently, credit institutions shall ensure that their employees are aware of their legal obligations and know the person (i.e. the MLCO) to whom they should report money laundering or terrorist financing knowledge or suspicion.

205. All of the "Internal Money Laundering Suspicion Reports" must be registered and maintained in a separate file by the MLCO.

206. Once an Internal Money Laundering Suspicion Report has been submitted, all subsequent transactions of the customer concerned should be monitored by the MLCO.

7.4 Reports to MOKAS

The Law
Article 70

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

208. All MLCOs' Reports to MOKAS should be sent or delivered at the following address:

Unit for Combating Money Laundering ("MOKAS")
The Law Office of the Republic,
7 Pericleous Street,
2020 Strovolos
Nicosia
Tel.: 22 446018
Fax: 22 317063

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

209. The form attached to this Directive, as **Appendix 4**, should be used and followed at all times when submitting a report to MOKAS. Reports can be submitted to MOKAS by post, facsimile, e-mail or by hand.

210. Having submitted a suspicious transaction/activities report, a credit institution may subsequently wish to terminate its relationship with the customer concerned for risk avoidance reasons. In such an event, however, credit institutions should exercise particular caution, as per Article 48 of the Law, not to alert the customer concerned that a disclosure report has been filed with MOKAS. Close liaison with MOKAS should, therefore, be maintained in an effort to avoid any impediments to the investigations conducted.

211. After submitting the report to MOKAS, credit institutions are expected to adhere to any instructions given by MOKAS and, in particular, as to whether or not to continue the operation of an account or suspend a transaction. It is noted that Article 26(2)(c) of the Law empowers MOKAS to instruct credit institutions to refrain from executing or delaying the execution of a customer's order without such action constituting a violation of any contractual or other obligation of the credit institution and its employees.

212. Furthermore, after the submission of a report to MOKAS in relation to suspicious transactions/activities, the account(s) concerned as well as any other connected account(s) should be placed under the close monitoring of the MLCO.

8. EDUCATION AND TRAINING OF EMPLOYEES

The Law Article 58

213. Article 58 of the Law requires persons carrying out financial or other business activities to establish adequate and appropriate systems and procedures to make their employees aware with regard to:

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

(ii) the Law,

(iii) the Directives issued by the competent Supervisory Authority, and

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

Furthermore, Article 58(g) of the Law requires the regular training of staff to recognise and handle transactions and activities suspected to be related with money laundering or terrorist financing activities.

214. The effectiveness of the procedures and recommendations laid down in this Directive and other relevant circulars of the Central Bank of Cyprus in relation to the prevention of money laundering and terrorist financing depends on the extent to which credit institutions' employees appreciate the seriousness of the background which led to the enactment of the Law and on the level of their education with regard to their duties and statutory obligations for countering this serious problem. It is reminded that an employee can be personally liable for failure to report information regarding money laundering and terrorist financing, in accordance with the internal reporting procedures. Consequently, staff of credit institutions must be encouraged to cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is a slight suspicion that they are related to money laundering or terrorist financing. In this regard, it is crucial that credit institutions establish comprehensive measures to ensure that their staff is fully aware of their responsibilities and duties. In this regard, the MLCO has the responsibility, in cooperation with other competent units of the credit institution (e.g. the Personnel and Training departments etc), to prepare and implement, on an annual basis, an education and training programme for the staff as required by the Law and this Directive. The MLCO is required to evaluate the adequacy of the seminars and the training provided to the staff and maintain detailed data regarding the seminars/programmes carried out, such as:

(i) Name of employee participating in the seminar/training by branch/department and by position (management staff, officers, newcomers etc.),

(ii) the date, title and duration of the seminar and the names of the trainers, and

(iii) whether the lecture/seminar was organised internally or offered by an external agency or consultants.

215. The time and content of staff training of different units should be adapted to the needs of each credit institution. Furthermore, the frequency of education/training may vary depending on the amendments to the legislative or regulatory requirements, the staff duties as well as on any other changes that the financial system is undergoing.

216. The training programme should aim at educating staff on the latest developments in anti-money laundering and terrorist financing including the practical methods and trends used by criminals for this purpose.

217. The training programme should have a different structure for new staff, customer service staff, compliance staff, staff moving from one department to another or staff dealing with the attraction of new customers. Newly recruited staff should be educated in understanding the importance of preventive policies against money laundering and terrorist financing and the procedures, measures and controls that the credit institution has in place for that purpose. Customers service staff who deals directly with the public should be trained on the verification of new customers' identity, the exercise of due diligence on an on-going basis, the monitoring of accounts of existing customers and the detection of patterns of unusual and suspicious activity. On-going training should be given at regular intervals so as to ensure that staff is reminded of its duties and responsibilities and kept informed of any new developments.

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

9. IMPLEMENTATION OF THE DIRECTIVE ON BANKS' BRANCHES AND SUBSIDIARIES OPERATING OUTSIDE THE EUROPEAN UNION

219. This Directive is applicable to branches and subsidiaries established by credit institutions under the approval of the Central Bank of Cyprus, in third countries outside the European Union. Credit institutions should ensure that branches and subsidiaries established in third countries fully comply with the provisions of this Directive with regard to customer identification and due diligence measures and record keeping procedures.

220. In this regard, credit institutions should forward this Directive, as well as the relevant abstracts from their risk management and procedures manual for the prevention of money laundering and terrorist financing, to the Board of Directors and Senior Management of their branches and subsidiaries in countries outside the European Union. The MLCO of the Head Office in Cyprus, who has the main responsibility for the implementation of the Central Bank of Cyprus' Directives, should ensure that the branches and subsidiaries located in third countries have taken all the necessary measures to comply with this Directive in relation to customer identification, due diligence and record keeping procedures. Where the laws or regulatory requirements of the hosting country in which the branches and subsidiaries are situated differ from the requirements of the Law and this Directive, then the branches and subsidiaries shall apply the stricter requirements of the two, to the extent that this is permitted by the legislation/regulations of the hosting country.

221. Where the legislation/regulations of the third country do not permit the implementation of the requirements of this Directive and the said legislation/regulations do not require the implementation of equivalent measures and procedures, then the MLCO of the credit institution concerned should immediately inform of this fact the Central Bank of Cyprus. In addition, the credit institution should take additional measures to effectively manage the increased risk of money laundering and terrorist financing which emanates from the above deficiency.

10. SUBMISSION OF PRUDENTIAL RETURNS TO THE CENTRAL BANK OF CYPRUS

10.1 Submission of Data and Information

The Law Article 59(9)

222. According to Article 59(9) the Central Bank of Cyprus may request and collect from persons subject to its supervision information necessary or useful for the performance of its functions and request within a specified deadline, the provision of information, data and documents. In case of refusal of any person under its supervision to comply with its request for the provision of information within the specified deadline or if the person refuses to give any information or demonstrates or provides incomplete or false or manipulated information, the Central Bank of Cyprus has the power to impose an administrative fine in accordance with the provisions of subsection 6 of the above Article.

10.2 Monthly Statement of Large Cash Deposits and Funds Transfers

223. As from September 1990, all banks in Cyprus are obliged to sumbit a monthly return on their large cash deposits and incoming and outgoing funds transfers. The submission of the above monthly return has proved to be particularly useful as it provides credit institutions with the opportunity to initially evaluate and, subsequently, to reinforce their systems of internal control and monitoring of their operations for the purpose of early identification and detection of transactions and business relationships which may be unusual and/or carry increased risk of being involved in money laundering operations. Attached as **Appendix 6** to this Directive is the form of the "Monthly Statement of Large Cash Deposits and Funds Transfers" which must be submitted to the Central Bank of Cyprus within 15 days after the end of the reporting month, as well as explanations and instructions for its completion.

10.3 Monthly Statement of customers' loans and deposits based on the country of permanent residence of the ultimate beneficial owner

224. According to Section 3 of this Directive, credit institutions are obliged to apply appropriate measures and procedures depending on the degree of risk to prevent the use of their services for money laundering or terrorist financing. It is noted that the risk based approach, includes the identification and assessment of money laundering and terrorist financing risks emanating from specific customers, products and services and geographic locations in relation to the operations of credit institutions and their customers, as well as the management and mitigation of these risks by applying appropriate and effective policies, procedures and safety nets.

225. In that respect, as from March 2013 credit institutions are obliged to submit on a monthly basis data on customers' deposits and loans by country of permanent residence, regardless of the nationality or citizenship, of the ultimate beneficial owner, as defined in Article 2 of the Law. It is noted that in the case of legal persons / entities with more than one beneficiary, then the country of permanent residence of the beneficiary with the highest percentage of ownership should be taken into account. In the case of beneficiaries who reside in different countries and own the same percentage of ownership, the country in which the company or the group has physical presence should be indicated. The monthly statement must be submitted within 15 days at the latest after the end of the month to which it relates. The circulars of the Central Bank of Cyprus dated 5 December 2012 and 3 January 2013 are relevant.

226. The MLCO assesses the data submitted to the Central Bank of Cyprus with the above mentioned monthly statement and, where necessary, investigates any trends which may indicate risks of engagement in transactions or activities of money laundering or terrorist financing and ensures his/her readiness to address questions by the Central Bank of Cyprus.

10.4 Adjustment of credit institutions' computerised accounting systems

227. To that end, the Central Bank of Cyprus requires all credit institutions to adjust their computerised accounting systems so as to be able to report complete and accurate information in the above mentioned returns thereby enhancing the ability of credit institutions to identify and monitor transactions which are considered to involve higher risk of being associated with money laundering activities and terrorist financing.

11. REPEAL/CANCELLATION OF PREVIOUS GUIDANCE NOTES AND SUPPLEMENTS/AMENDMENTS

228. The Directive on the Prevention of Money Laundering and Terrorist Financing of April 2008 and its subsequent amendments, in accordance with Article 59(4) of the Prevention and Suppression of Money Laundering Activities Laws are, hereby, repealed and cancelled.

12. APPENDICES

APPENDIX 1

QUESTIONNAIRE FOR THE ASSESSMENT OF THE FITNESS AND PROBITY OF AN INDIVIDUAL TO BE APPOINTED AS A MONEY LAUNDERING COMPLIANCE OFFICER

NAME:

CREDIT INSTITUTION:

INSTRUCTIONS FOR THE COMPLETION OF THE QUESTIONNAIRE:

- In case you provide false or misleading information or you knowingly avoid to disclose significant information, you raise doubts about your integrity and, as a consequence, your fitness for appointment.
- The space provided after each question in the questionnaire is NOT indicative of the extent of the expected answer. Where you deem necessary, you are requested to use a separate sheet of paper, stating the number of the question on the top left part of the sheet of paper.
- All questions must be answered. If a question is not applicable please indicate by responding "Not Applicable" ("n/a").
- Certified copies of all documents referred to in this questionnaire must be attached (e.g. university degrees, certificates, identity cards etc).

1. Personal details

1.1 Full name and surname

1.1.1 Title:

1.1.2 Name(s):

1.1.3 Surname:

1.2 Maiden name (if different):

1.2.1 Date of change of name (if applicable):

1.3 Date of birth:

1.4 Identification Card Number:

1.5 Social Insurance Number:

1.6 Country and town or community of birth:

1.7 Nationality:

1.8 Passport number, issuing country and expiry date:

1.9 Telephone number and e-mail address for communication purposes:

1.10 Residential address:

I have been a resident at this address for less than 180 days. YES ☐ or NO ☐
In case your address has changed in the last ten years, please give your previous address(es) during the past ten years.

2. Experience

2.1 Employment history

Please attach your recent Curriculum Vitae (CV) which should include full details and information about your employment, starting from the most recent one. Please state in your CV significant information which would be of interest to the Central Bank, such as the reasons for the termination of employment, or information about periods during which you had been unemployed. You should include full history for the last ten years,

which, for every period of employment, should necessarily include the following information:

- date of commencement and termination of employment,
- name, address and nature of employer's business and,
- position held and key areas of responsibility and competence.

2.2 Academic qualifications

Please give details of your academic qualifications (institution, degree/certificate, duration of study (from - to)) and attach the relevant certified copies.

Full name of institution	Degree/Certificate	From - To	Obtained

2.3 Professional qualifications and membership to Professional Bodies (certified copies to be attached):

Full name of Professional Body	Full title of the professional qualification obtained	Date qualification obtained / date membership obtained (month / year):

2.4 Other relevant education / training (certified copies to be attached)

Description	From - To	Name of the educational institution

3. Good reputation and character

The following questions must be answered by responding YES or NO. In case where the response to a question is YES, provide full details on a separate sheet of paper noting thereon the number of the question.

3.1 Have you been convicted of an offence involving fraud or dishonesty in the Republic of Cyprus or elsewhere? YES ☐ or NO ☐

3.2 Have you been convicted of any offences, excluding minor motoring offences, other than those declared in question 3.1 or have you been subject to penalties or charges for tax evasion? (See also declaration to be signed regarding tax compliance). YES ☐ or NO ☐

3.3 Have you been charged before any Court of Law in Cyprus or elsewhere with an offence for which you have not been acquitted and which has not been waived? YES ☐ or NO ☐

If yes, what was the outcome?

3.4 Are you currently involved in, or the subject of, any criminal or civil proceedings, other than as an expert witness or a judge, the examination of which has not yet been concluded?

YES ☐ or NO ☐

3.5 Have you at any time, in Cyprus or elsewhere, been declared bankrupt, or entered into any compromise agreement with your creditors, or are you currently the subject of bankruptcy proceedings? YES ☐ or NO ☐

Are you aware whether bankruptcy proceedings are pending against you? YES ☐ or NO ☐

3.6 Have you at any time, in Cyprus or elsewhere, entered into a compromise agreement with your creditors or have you failed to pay any amount to creditors that was a judgment debt under a Court Order in Cyprus or elsewhere within one year of the Order? YES ☐ or NO ☐

3.7 Have you ever been forbidden from the potential of holding the post of a director or have you been removed from the post of a director of a legal entity by a Court order, in Cyprus or elsewhere?

YES ☐ or NO ☐

3.8 Have you, or as far as you are aware, has your employer been criticised during the last ten years by a

professional body to which you and/or your employer belong or formerly belonged?
YES ☐ or NO ☐

3.9 Have you ever resigned from a professional or supervisory body in order to avoid the pursue of legal action or disciplinary measures against you? YES ☐ or NO ☐

3.10 Have you been a director of a firm, which was, during the period of your directorship, convicted of any offence? YES ☐ or NO ☐

3.11 Have you ever been refused entry to any profession or have you been dismissed or requested to resign from any office or employment, whether or not remunerated? YES ☐ or NO ☐

3.12 Has your right to carry on any trade, business or profession for which a specific license, registration or other authorisation is required, ever been prohibited or suspended, in Cyprus or elsewhere?
YES ☐ or NO ☐

3.13 Are you or have you ever been, to the best of your knowledge, the subject of an investigation for allegations relating to the provision of financial services? YES ☐ or NO ☐

3.14 During the last ten years, have you been the director of a company in Cyprus or elsewhere, which has gone into liquidation, or receivership or entered into any arrangements with its creditors or was voluntarily wound-up? YES ☐ or NO ☐

3.15 Have you ever, during the formation or management of any company, partnership or business, been charged by a Court of Law in Cyprus or elsewhere for fraud, illegal dealings or other similar offences against such entity, its proprietors or its creditors? YES ☐ or NO ☐

3.16 Have you ever been charged for offences relating to tax legislation or tax evasion?
YES ☐ or NO ☐

4. Participation in other organisations

4.1 Have you guaranteed the liabilities of any organisation or individual? YES ☐ or NO ☐
If yes, please give details.

4.2 Please give details of any titles you have in financial entities. (if you don't, please note n/a)

4.3 Please state whether loans or other facilities have been granted by the credit institution to you or your connected persons (see the definition of "connected persons" on the last page). If yes, please provide the following information:

Name of Obligor	Amount	Date of granting	Outstanding Balance	Arrears/Excesses of the facility

4.4 Please provide the following details for companies where you hold more than 10% of their share capital or where you act as a Director and to which credit facilities have been granted by the credit institution:

Name of Obligor	Amount	Date of granting	Outstanding Balance	Arrears/Excesses of the facility

5. Criminal Record

Please attach a recent original Police Report from the police authorities of your country of residence.
Please note that individuals who in the last five years resided outside Cyprus must provide a clearance letter / certificate from the police authorities of those countries of residence.

6. References

6.1 On a separate page please provide the names and contact details of two personal referees who from their personal experience are familiar with your financial activities and may provide information about your character. In case you have not been self-employed during the last ten years, one of the two personal referees must be your most recent employer.

6.2 Have these referees consented to give references? YES ☐ or NO ☐

6.3 Please state whether you give your consent to the Central Bank of Cyprus to ask for these references at this stage. YES ☐ or NO ☐

If NO, please give the reasons below:

7. Other

Please note that all persons appointed as Compliance Officers must submit to the Central Bank of Cyprus on an annual basis, a declaration confirming that there have been no material changes in the information provided in this questionnaire.

APPENDIX 2

INTERNAL MONEY LAUNDERING SUSPICION REPORT

REPORTER

Name: .....Tel .....
Branch/Dept. .....Fax .....
Position.....E-mail.....

CUSTOMER

Name: ....
Address:..... .....
.....Date of birth .....
Contact/Tel/Fax/E-mail .....Occupation/Employer .....
.....Details on employer: .....
Passport No .....Nationality .....
ID Card No .....Other ID .....

INFORMATION/SUSPICION

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

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

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

FOR MONEY LAUNDERING COMPLIANCE OFFICER'S USE

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

APPENDIX 3

MONEY LAUNDERING COMPLIANCE OFFICER'S

INTERNAL EVALUATION REPORT

Reference..... Customer.....

Reporter..... Branch/Dept.....

ENQUIRIES UNDERTAKEN (Brief description)

.....

.....

.....

DOCUMENTS RESEARCHED/ATTACHED

.....

.....

.....

DECISION OF THE MLCO

.....

.....

.....

FILE REFERENCE.....

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

APPENDIX 4

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

INSTITUTION NAME:_____

I. CUSTOMER'S DETAILS

Date when the business relationship commenced, or a one-off transaction was either carried out or attempted to be carried out:_____

Date when the business relationship was terminated:_____

Account Number	Branch	Type of account	Date of opening	Date of closure	Account balance

(a) NATURAL PERSONS

	Name(s)	Residential address(es)	Business address(es)	Occupation/employer details	Date and place of birth	Nationality, passport number(s) and/or ID number
Beneficial owner of the account						
Authorised signatory(ies) of the account						

(b) LEGAL ENTITIES

Company name:	
Country of incorporation:	
Date of incorporation:	
Registered address:	
Business address:	
Other addresses:	
Main activities:	

Introducer (where available):

Name:_____

BusinessActivities:_____

Business address:_____

	Name	Nationality, passport number and/or ID number	Issuing Country	Date of birth	Residential address	Occupation & Employer
Registered shareholder(s)						
Beneficial shareholder(s) (if different from above)						
Directors/Managers						
Authorised signatory(ies) to the account(s)						

II. KNOWLEDGE/SUSPICION OF MONEY LAUNDERING AND/OR FINANCING OF TERRORISM

Please explain the knowledge or suspicion connected with Money Laundering and/or the Financing of Terrorism.

Period during which the account(s) raised suspicions

	Account number	From (dd/mm/yyyy)	Until (dd/mm/yyyy)
1			
2			
3			
4			

CENTRAL BANK OF CYPRUS
EUROSYSTEM

DETAILS OF SUSPICIOUS TRANSACTIONS

DEBIT TRANSACTIONS

	Type *	Amount	Date	Beneficiary	Acc. Number (IBAN)	Beneficiary's Address	Beneficiary's bank	Country of receipt
1.								
2.								
3.								
4.								
5.								

CREDIT TRANSACTIONS

	Type *	Amount	Date	Beneficiary	Acc. Number (IBAN)	Originator's Address	Originator's bank	Country of Origin
1.								
2.								
3.								
4.								
5.								

* Please complete using one of the following: Cash Withdrawal / Deposit, Funds Transfer, Cheques

III. OTHER INFORMATION

- Customer's accounts with other credit institutions in Cyprus or abroad (if known)

	Credit institution's name	Acc. Number	Country where the account is maintained	Other information
1.				
2.				
3.				
4.				
5.				

- Other *natural persons* (beneficiaries, directors, signatories, third persons) who maintain account(s) with the credit institution, that are somehow connected with the suspicious transactions/activities and the reported subjects. Please clarify the relationship maintained with the above.

	Name	Profession	Relation with the reported subject	Other information
1.				
2.				
3.				
4.				
5.				

- Other *legal persons*, (connected companies, third persons) that maintain account(s) with the credit institution, that are somehow connected with the suspicious transactions/activities and the reported subjects. Please clarify the relationship maintained with the above.

	Name	Business Activities	Relation with the reported subject	Other information
1.				
2.				
3.				

4.				
5.				

IV. ATTACHED DOCUMENTS

(Where practicable, please also send the documents in an electronic version)

1. Customer Identification Documents

(i) Natural Persons

- Photocopies of the relevant pages of customers' passports evidencing identity and/or photocopies of the customers' IDs ☐
- Documents evidencing address ☐

(ii) Legal Entities

- Certificates of incorporation ☐
- Certificates of directors and registered shareholders ☐
- Documents evidencing identity of registered shareholders, beneficial owners, and authorised signatories ☐

2.Documents relating to the suspicious transaction(s)

- Bank statements ☐
- Swift messages ☐
- Bank advice slips ☐
- Correspondence ☐
- Other relevant documents ☐

Compliance Officer

Name:_____

Telephone:_____

Facsimile:_____

E-mail Address:_____

Date:_____

Signature:_____

APPENDIX 5

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

A) MONEY LAUNDERING

1. Cash and other banking transactions

(i) Provision of considerable high amount of cash collateral against loans.

(ii) Cash withdrawals of large amounts which are not consistent with the nature and scale of customer's activities.

(iii) Cash withdrawals of large amounts from a dormant account or an account which has recently been credited with a huge inward transfer from abroad.

(iv) Cash withdrawal of a large amount which is re-deposited in another account.

(v) Cash transactions involving large rounded amounts.

(vi) Cash withdrawals of large amounts from accounts which used to be dormant or from accounts which have recently been credited with huge inward transfers.

(vii) Unusually large cash deposits made to the account of an individual or company whose ostensible business activities would normally be generated by cheques and other payment instruments.

(viii) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

(ix) Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

(x) Company accounts whose transactions, both deposits and withdrawals, are denominated in cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Wire Transfers, etc.).

(xi) Customers who constantly pay-in or deposit cash to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments.

(xii) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

(xiii) Frequent exchange of cash into other currencies.

(xiv) Branches that have much more cash transactions than usual. (Head Office statistics should detect abnormal deviations in cash transactions.)

(xv) Customers whose deposits contain counterfeit notes or forged instruments.

(xvi) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

(xvii) Large cash deposits using night safe facilities, thereby avoiding direct contact with the credit institution.

(xviii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the credit institution.

(xix) Numerous deposits of small amounts, through multiple branches of the same credit institution or by groups of individuals who enter a single branch at the same time. The money is then frequently transferred to another account, often in another country.

2. <u>Transactions through bank accounts</u>

(i) The use of accounts in the names of trustees, nominees or client accounts without any apparent reason or without this being in line with the activities of the account holder.

(ii) Demanding the return of funds on grounds that these have been sent by error.

(iii) Multiple transactions carried out on the same day at the same branch of a bank but with an apparent attempt to use different teller.

(iv) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

(v) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

(vi) Customers who appear to have accounts with several credit institutions within the same locality, especially when the credit institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

(vii) Matching of payments out with credits paid in by cash on the same or previous day.

(viii) Paying in large third party cheques inconsistent with the customer's account activity.

(ix) Accounts that receive relevant periodic deposits and are dormant in other periods.

(x) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

(xi) Greater use of safe deposit facilities by individuals. The use of sealed packets deposited and withdrawn.

(xii) Companies' representatives avoiding contact with the branch.

(xiii) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

(xiv) Large number of individuals making payments into the same account without an adequate explanation.

(xv) An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

3. <u>Investment related transactions</u>

(i) Purchasing of securities to be held by the credit institution in safe custody, where this does not appear appropriate given the customer's apparent standing.

(ii) Back to back deposit/loan transactions with subsidiaries of, or affiliates of, overseas financial institutions in countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on money laundering prevention.

(iii) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.

(iv) Large or unusual settlements of securities transactions in cash form.

(v) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. Funds transfer/ international activity

(i) The credit institution acts as an intermediary for the transfer of funds from a credit institution outside Cyprus to another credit institution also outside Cyprus, without any direct knowledge of the originator and/or the beneficiary of the said funds. The transfer is not in favour of a customer of the intermediary credit institution or any other credit institution operating in Cyprus.

(ii) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

(iii) Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs.

(iv) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

(v) Unexplained electronic funds transfers by customers on an in and out basis or without passing through an account.

(vi) Frequent requests for travellers' cheques, foreign currency drafts or other negotiable instruments to be issued.

(vii) Frequent paying in of travellers' cheques, foreign currency drafts particularly if originating from overseas.

(viii) Numerous funds transfers received in an account when each transfer is below the reporting requirement in the remitting country.

(ix) Funds transfer activity to/from a high risk jurisdiction without an apparent business reason, or when it is inconsistent with the customer's business or history.

(x) Funds originating from companies operating in high risk jurisdictions, e.g. jurisdictions which do not apply or apply inadequately FATF's recommendations against money laundering and terrorist financing.

(xi) Funds transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted is not provided with the wire transfer.

(xii) Many small, incoming wire transfers of funds received, which are almost immediately, all or most, wired to a country in a manner inconsistent with the customer's business profile or history.

(xiii) Large incoming wire transfers on behalf of a foreign customer with little or no explicit reason.

(xiv) Wire activity that is unexplained, repetitive, or shows unusual patterns. Payments or receipts with no apparent links to legitimate contracts, goods, or services.

5. Correspondent Accounts

(i) Funds transfers in large amounts, where the correspondent account has not previously been used for similar transfers.

(ii) The routing of transactions involving a Respondent Bank through several jurisdictions and/or financial institutions prior to or following entry into the credit institution without any apparent purpose other than to disguise the nature, source, ownership or control of the funds.

(iii) Frequent or numerous funds transfers either to or from the correspondent account of a Respondent Bank originating from or going to a jurisdiction which does not apply or which applies inadequately FATF's recommendations on money laundering prevention.

6. Secured and unsecured lending

(i) Customers who repay problem loans unexpectedly.

(ii) Requests to borrow against assets (i.e. a security or a guarantee), held by a third person where the origin of the assets is not known or the assets are inconsistent with the customer's standing (back-to-back loans).

(iii) Requests by a customer to a credit institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

7. Customers who provide insufficient or suspicious information

(i) A customer is reluctant to provide complete information when opening an account about the nature and purpose of its business, anticipated account activity, prior banking relationships, names of its officers and directors, or information on its business location. He usually provides minimal or misleading information that is difficult or expensive for the credit institution to verify.

(ii) A customer provides unusual or suspicious identification documents that cannot be readily verified.

(iii) A customer's home/business telephone is disconnected.

(iv) A customer makes frequent or large transactions and has no record of past or present employment experience.

8. Activity inconsistent with the customer's business profile

(i) The transaction seems to be inconsistent with the normal type of transactions for the particular sector.

(ii) Unnecessarily complex transaction having in mind its commercial purpose.

(iii) Customer's activities are inconsistent with the declared ones.

(iv) The types of transactions show an unexpected change which is inconsistent with the normal operations of the customer.

(v) A large volume of cashier's cheques, money orders, and/or wire transfers deposited into, or purchased through, an account when the nature of the account holder's business would not appear to justify such activity.

(vi) A retail business which has dramatically different patterns of cash deposits from similar businesses in the same general location.

(vii) Ship owning and ship management companies engaged in transactions or activities unconnected to shipping business.

9. Characteristics of the customer or his business activity

(i) 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 (for example student, unemployed, self-employed, etc).

(ii) Stated occupation of the customer is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

(iii) Regarding non-profit or charitable organisations, financial transactions 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.

(iv) A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

(v) Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

10. Transactions from employees or agents or trustees

(i) Changes in the lifestyle of employees, e.g. luxurious way of life or avoiding being out of office due to holidays.

(ii) Changes in the performance or behaviour of employees

(iii) Transactions with agents where the identity of the beneficiary or the other party to the transaction remains unknown in contrast to the normal procedure for this type of activity.

(iv) Customers who want to be serviced by the same credit institution employee, even for routine transactions, or who stop transacting with the credit institution when a particular employee is out of office.

(v) Complex trust or nominee network.

(vi) Transactions or company structures established or working with an unneeded commercial way. e.g. companies with bearer shares or bearer derivatives or use of a postal code.

(vii) Trustee's uunwillingness to keep the necessary information or exercise the necessary controls in properly discharging his duties.

(viii) Use of nominee documents in a way that restricts the control exercised by the company's Board of Directors.

(ix) Customers who use client account in the name of a professional intermediary instead of their own bank account.

B) TERRORIST FINANCING

1. Sources and methods

The funding of terrorist organisations is conducted through 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:

- Collection of membership dues and/or subscriptions
- Sale of books and other publications
- Cultural and social events
- Donations
- 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 monetary instruments (traveller's cheques, bank cheques, money orders), use of credit and debit cards, 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:

- Establishing a non-profit organisation with a stated charitable purpose but which actually exists only to channel funds to a terrorist organisation.
- 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.
- The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.
- The non-profit organisation provides support functions to the terrorist movement.

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

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

APPENDIX 6

Statement of Large Cash Deposits and Funds Transfers

Month: ..... , 20...
Reporting Credit Institution: .....

1. Cash Deposits

1(a) Cash Deposits in excess of €10.000

(i)Total number of transactions ……

(ii)Total number of customer accounts affected ……

€'000

(iii) Total amount of individual cash deposits

in excess of €10.000 ……

1(b) Cash deposits in foreign currency notes
in excess of the equivalent of €10.000

(i) Total number of transactions ……

(ii) Total number of customer accounts affected ……

€'000

(iii) Total amount of cash deposits in foreign currencies

in excess of the equivalent of €10.000 ……

2. Inward funds transfers in favour of customers in excess of €500.000 or equivalent in foreign currencies

(i) Total number of transactions ……

(ii) Total number of customer accounts affected ……

€'000

(iii) Total amount of inward funds transfers in excess of €500.000 or equivalent in foreign currencies ……

3. Outward Funds Transfers in favour of customers in excess of €500.000 or equivalent in foreign currencies

(i) Total number of transactions ……

(ii) Total number of customer accounts affected ……

€'000

(iii) Total amount of outward funds transfers in excess of €500.000 or equivalent in foreign currencies ……..

4. Reporting of knowledge or suspicions connected with money laundering

(a) Total number of Internal Money Laundering Suspicion Reports submitted by credit institution employees to the Money Laundering Compliance Officer ……..

(b) Total number of Money Laundering Compliance Officers' Reports submitted to the Unit for Combating Money Laundering ("MOKAS") ……..

I confirm that the above figures extracted from the credit institution's books and records are true and accurate and this statement has been completed in accordance with the explanations and instructions of the Central Bank of Cyprus.

Date: …….. Signature:…….…. …….

(Money Laundering Compliance Officer)

EXPLANATIONS AND INSTRUCTIONS FOR COMPLETING THE MONTHLY STATEMENT OF LARGE CASH DEPOSITS AND FUNDS TRANSFERS

Introduction

The monthly Statement of Large Cash Deposits and Funds Transfers must provide a brief picture of the total amount of cash deposits in Euro and foreign currency notes that credit institutions have accepted during the month under review, as well as the total amount of funds transfers - as defined below – in Euro as well as in foreign currencies.

1. Cash deposits

(a) Cash Deposits in Euro

This item includes cash deposits in Euro from customers in excess of €10.000 per transaction.

Sub-category (i) refers to the total number of cash deposit transactions, and sub-category (ii) refers to the total number of customers' accounts affected by the above mentioned cash deposits.

For example if a customer deposits the amount of €15.000 in cash through the credit of 5 different accounts by €3.000 then:

(i) total number of transactions (1),

(ii) total number of accounts which are affected from the above transaction (5).

Sub-category (iii) refers to the total amount of cash deposits in excess of €10.000 that credit institutions have accepted from customers during the month under review.

(b) Cash Deposits in foreign currency notes in excess of the equivalent of €10.000

This item includes cash deposits in foreign currencies in excess of the equivalent of €10.000 per transaction.

Sub-category (i) refers to the total number of cash deposit transactions, and sub-category (ii) refers to the total number of customers' accounts affected by the above mentioned cash deposits.

Sub-category (iii) must include the total number of cash deposits in foreign currencies in excess of the equivalent of €10.000 that the credit institution has accepted during the month under review. This amount must be converted into Euro, according to the Euro / foreign currency closing exchange rate on the day each transaction was carried out.

Exemptions:

Cash deposits in Euro and foreign currency notes from the following categories are exempted and should not be reported in the monthly statement submitted to the Central Bank of Cyprus:

a) Cash deposits in Euro and foreign currency notes by the Government of the Republic.

b) Cash deposits in Euro and foreign currency notes by public entities

c) Cash deposits in Euro and foreign currency notes by other credit institutions operating in Cyprus

2. Inward funds transfers in favour of customers in excess of €500.000 or equivalent in foreign currencies

This item includes inward funds transfers originating from a customer's account kept in a bank outside Cyprus in favour of a customer maintaining an account with the credit institution which are in excess of €500.000 or equivalent in foreign currencies per transaction.

Exemptions:

The following funds transfers are exempted and should not be included in the monthly statement submitted to the Central Bank:

a) Transfers from another customer's account maintained with the same credit institution; and

b) Inward funds transfers received by order of customers maintaining accounts with other credit institution in Cyprus.

3. Outward funds transfers by order of customers in excess of €500.000 or equivalent

This item includes outward funds transfers by order of a customer maintaining an account with the credit institution in favour of a customer maintaining an account with a bank outside Cyprus.

Exemptions:

The following funds transfers are exempted and should not be included in the monthly statement submitted to the Central Bank:

a) Transfers to another customer's account maintained with the same credit institution; and

b) Outward funds transfers made in favour of customers maintaining accounts with other credit institution in Cyprus.

4. Reporting of knowledge or suspicions connected with money laundering

Sub-category 4(a) must include the number of Internal Money Laundering Suspicion Reports submitted by the credit institution's employees to the Money Laundering Compliance Officer during the month under review.

Sub-category 4(b) must include the number of reports submitted by the Money Laundering Compliance Officer to MOKAS during the month under review.