



CENTRAL BANK OF CYPRUS

EUROSYSTEM

**BANK SUPERVISION AND REGULATION
DEPARTMENT**

***PREVENTION OF MONEY LAUNDERING
AND TERRORIST FINANCING***

***DIRECTIVE TO BANKS
IN ACCORDANCE WITH ARTICLE 59(4) OF THE
PREVENTION AND SUPPRESSION OF MONEY
LAUNDERING ACTIVITIES LAW OF 2007***

(THIRD ISSUE)

APRIL 2008

CONTENTS

	<u>PAGE</u>
PREFACE	1
1. INTERNAL CONTROL PROCEDURES AND RISK MANAGEMENT	
1.1 Obligation to establish procedures	3
1.2 Customer Acceptance Policy	6
2. THE ROLE OF THE MONEY LAUNDERING COMPLIANCE OFFICER	
2.1 Appointment of a Money Laundering Compliance Officer (“MLCO”)	7
2.2 Duties of the Money Laundering Compliance Officer	7
2.3 Annual Report of the Money Laundering Compliance Officer	11
3. THE APPLICATION OF APPROPRIATE MEASURES AND PROCEDURES ON A RISK SENSITIVE BASIS	
3.1 Introduction	14
3.2 Identifying and Assessing Risks	15
3.3 Design and implementation of controls to manage and mitigate risks	16
3.4 Monitoring and improving the effective operation of banks’ internal procedures	18
3.5 Risk management is dynamic	19
4. CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES	
4.1 Introduction	20
4.2 When customer identification and due diligence procedures should be applied.	20
4.3 Customer identification and due diligence procedures	21
4.4 Timing of identification	22

4.5	Exercise of due diligence and updating of identification data of existing customers	23
4.6	Simplified customer identification and due diligence procedures	24
4.7	Prohibition of anonymous and numbered accounts and accounts in fictitious names	26
4.8	Transaction and products that favour anonymity	26
4.9	Prohibition of correspondent relationships with “shell banks”	27
4.10	Failure or refusal to provide identification evidence	27
4.11	Construction of a customer’s business profile	27
4.12	Reliance on third parties for customer identification and due diligence purposes	29
4.13	Specific customer identification issues	32
4.13.1	Natural persons residing in Cyprus	32
4.13.2	Natural persons not residing in Cyprus	33
4.13.3	Joint-Accounts	33
4.13.4	Nominees or agents of third persons	34
4.13.5	Accounts of unions, societies, clubs, provident funds and charities	34
4.13.6	Accounts of unincorporated businesses/partnerships	34
4.13.7	Accounts of corporate customers (companies)	35
4.13.8	Investment funds and persons engaged in the provision of financial and investment services	37
4.13.9	Safe custody and safety deposit boxes	38
4.14	Procedures for high risk customers	39

4.14.1	Customer identification and due diligence on a risk sensitive basis	39
4.14.2	High risk customers	39
4.14.2.1	Non-face to face customers	40
4.14.2.2	Accounts in the names of companies whose shares are in the form of bearer	41
4.14.2.3	Accounts in the names of trusts	42
4.14.2.4	“Client accounts” in the name of third persons	42
4.14.2.5	Accounts for Politically Exposed Persons (“PEPs”)	43
4.14.2.6	Correspondent accounts of banks outside European Union	46
4.14.2.7	Services to private banking customers	48
4.14.2.8	Electronic gambling /gaming through the internet	49
4.14.2.9	Customers from countries which do not adequately apply FATF’s recommendations	50
4.15	On-going monitoring of accounts and transactions	51
5.	CASH DEPOSITS AND WITHDRAWALS	
5.1	Cash Deposits	55
5.2	Deposits of cash imported from abroad	55
5.2.1	Prohibition of accepting cash deposits in foreign currency notes that have been imported from abroad	55
5.2.2	Acceptance of cash deposits in foreign currency	56
5.2.3	Definition of connected persons	57
5.2.4	Internal procedures and responsibilities of the Money Laundering Compliance Officers	57
5.2.5	Submission of Returns to the Central Bank of Cyprus	58

5.2.6 Exempted cash deposits in foreign currency	59
5.3 Cash Withdrawals	59
6. RECORD KEEPING PROCEDURES	
6.1 Introduction	61
6.2 Format of records	62
6.3 Electronic funds transfers	63
7. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES	
7.1 Introduction	65
7.2 Examples of suspicious transactions/activities	65
7.3 Internal reporting suspicious transactions and activities	65
7.4 Reports to MOKAS	66
8. EDUCATION AND TRAINING OF EMPLOYEES	68
9. IMPLEMENTATION OF THE DIRECTIVE ON BANKS' BRANCHES AND SUBSIDIARIES OPERATING OUTSIDE THE EUROPEAN UNION	70
10. SUBMISSION OF PRUDENTIAL RETURNS TO THE CENTRAL BANK OF CYPRUS	
10.1 Monthly Statement of Large Cash Deposits and Funds Transfers	71
10.2 Monthly Statement of one-off deposits in foreign currency in excess of the equivalent of 100.000 Euro which have been imported in Cyprus from abroad	71
10.3 Annual Statement of aggregate deposits in foreign currency notes in excess of the equivalent of 100.000 Euro in a calendar year	71

10.4	Adjustment of banks' computerised accounting systems	72
11.	REPEAL/CANCELLATION OF PREVIOUS GUIDANCE NOTES AND SUPPLEMENTS/AMENDMENTS	73
12.	APPENDICES:	
	Appendix 1: The main provisions of the Prevention and Suppression of Money Laundering Activities Law of 2007.	74
	Appendix 2: Internal Money Laundering Suspicion Report.	86
	Appendix 3: Money Laundering Compliance Officer's Internal Evaluation Report.	87
	Appendix 4: Money laundering Compliance Officer's Report to the Unit for Combating Money Laundering ("MOKAS").	88
	Appendix 5: Examples of suspicious transactions / activities related to money laundering and terrorist financing operations.	94
	Appendix 6: Statement of large cash deposits and funds transfers.	103
	Appendix 7: Monthly statement of one-off deposits in foreign currency notes in excess of the equivalent of 100.000 Euro which have been imported in Cyprus from abroad.	109
	Appendix 8: Annual statement of aggregate deposits in foreign currency notes in excess of the equivalent of 100.000 Euro in a calendar year.	110

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 apply 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 for the purpose 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 has been 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”.
- (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 (Third Edition) (hereinafter to be referred to as "the Directive") is issued to all banks in accordance with Article 59(4) of the Prevention and Suppression of Money Laundering Activities Law of 2007, and aims at laying down the specific policy, procedures and internal controls that all banks 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 supervisory authorities, including the Central Bank of Cyprus, the duty of monitoring, evaluating and supervising the implementation of the Law and the Directives issued to supervised entities. The main provisions of the Law, which are of direct interest to banks and their employees, are presented in Appendix 1 to this Directive.

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 visibly lawful purpose.
2. The Board of Directors, the bank's Senior Management and, in the cases of branches of foreign banks operating in Cyprus, the local management, are responsible for ensuring the implementation of the requirements of the Law and this Directives 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 "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, requires the Compliance Unit of a bank or its Risk management Unit (where no Compliance Unit has been set up) to establish and apply suitable procedures for the purpose of achieving a timely and on-going compliance of the bank with the existing 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 organically belong to the Compliance Unit or, where such unit has not been established, to the Risk Management Unit.
5. The Money Laundering Compliance Officers 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.

6. The Central Bank of Cyprus requires banks to apply the following measures and procedures:
- The Board of Directors determines, records and approves the general policy principles of the bank for the prevention of money laundering and terrorist financing which are subsequently communicated to the Senior Management and the Money Laundering Compliance Officer.
 - The Money Laundering Compliance Officer has the responsibility in cooperation with other departments of the bank (e.g. the Department of Organisation and Methods) 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 bank'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 bank'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 Money Laundering Compliance Officer.
 - Explicit responsibilities and duties are allocated to the bank'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.
 - The Money Laundering Compliance Officer, the Assistant Money Laundering Compliance Officers and other members of staff who have been assigned with the duty of implementing the adopted procedures for the prevention of money laundering and terrorist financing, have complete and timely access to all information concerning customers' identity, transactions' records and other relevant files and information maintained by the bank so as to be fully facilitated in the effective discharge of their duties.
 - All employees are made aware of the person (Money Laundering Compliance Officer) to

whom they should report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing activities.

- There is a clear reporting chain, explicitly prescribed in the risk management and procedures manual by which information regarding suspicious transactions is passed without delay to the Money Laundering Compliance Officer, either directly or through his Assistants;
- 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).
- 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 bank with regard to the development of new products and possible changes in the bank'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, 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.
- The Senior Management of banks ensures that the Money Laundering Compliance Officer has sufficient resources, including competent staff and technological equipment, for the effective discharge of his/her duties.
- The Internal Audit Department reviews and evaluates, **on an annual basis**, the effectiveness and adequacy of the policy, procedures and controls applied by the bank 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 as well as to the Senior Management and the Money Laundering Compliance Officer of the bank who will decide the necessary measures that need to be taken to ensure the rectification of any weaknesses and omissions which have been detected by the internal

auditor.

- Explicit procedures and standards of recruitment and evaluation of new employees' integrity, are applied.

1.2 Customer Acceptance Policy

7. Banks should develop and establish a clear policy and procedures for accepting new customers, completely 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 bank from its customers and/or their transactions and/or their countries of origin or operations. (See Chapter 3 of this Directive).
8. The Money Laundering Compliance Officer prepares the customer acceptance policy and submits it through the bank's Senior Management to the Board of Directors for consideration and approval.
9. 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. 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 bank 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 10. Article 69(1) of the Law requires persons carrying on financial and other business to apply
Article 69(1) the following internal reporting procedures:

- (i) Appointing a person 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) requiring 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 contained in the report proves this fact or creates such suspicion;
- (iii) allowing the MLCO to have access to other information, records and details which may be of assistance to him/her and which is available to the person responsible for maintaining the said internal reporting procedures; and
- (iv) securing 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.

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

2.2 Duties of the Money Laundering Compliance Officer

12. The role and responsibilities of the MLCO, including those of his Assistants, should be clearly

specified by banks and documented in the risk management and procedures manual for the prevention of money laundering and terrorist financing.

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

- (i) The MLCO has the primary responsibility, together with the bank's Senior Management, for establishing appropriate measures, systems and procedures for the due implementation of the Law and the Directive of the Central Bank of Cyprus as well as for adherence to all other circulars/recommendations which are issued by the Central Bank of Cyprus, from time to time, for the prevention of the use of the banking system for money laundering and terrorist financing. In this regard, the MLCO has the primary responsibility for the preparation of the bank's risk management and procedures manual for the prevention of money laundering and terrorist financing.
- (ii) The MLCO monitors and assesses whether the policy, procedures and controls that have been introduced for the prevention of money laundering and terrorist financing are correctly and effectively applied. In this regard, the MLCO should apply appropriate monitoring mechanisms (e.g. on-site visits to units/branches) which will provide him/her with all necessary information for assessing the level of compliance of the units /branches of the bank with the procedures and controls which are in force. In the event that the MLCO identifies shortcomings and/or weaknesses in the application of the requisite procedures and controls, he/she should give appropriate guidance for the assumption of corrective measures.
- (iii) The MLCO prepares the Customer Acceptance Policy which is submitted through the Senior Management of the bank to the Board of Directors for consideration and approval.
- (iv) The MLCO receives information from the bank's employees which is considered by the latter to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. A specimen of such an internal report (hereinafter to be referred to as "Internal Money Laundering Suspicion Report") is attached, as "Appendix 2", to this Directive. All such reports should be registered and kept on a separate file.
- (v) The MLCO validates and considers the information received as per paragraph (iv) above by reference to any other relevant information and discusses the circumstances of the case with the reporting employee concerned and, where appropriate, with the employee's superior(s). The evaluation of the information reported to the MLCO should be made on a separate form which should be registered and retained on file. A specimen of such a report (hereinafter to be referred to as "Money Laundering Compliance Officer's Internal Evaluation Report") is attached, as "Appendix 3", to this Directive.

- (vi) If following the evaluation described in paragraph (v) above, the MLCO decides to notify MOKAS, then he/she should complete a written report and submit it to MOKAS the soonest possible. A specimen of such a report (hereinafter to be referred to as "Money Laundering Compliance Officer's Report to 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.
- (vii) After the submission of the MLCO's report to the Unit for Combating Money Laundering ("MOKAS"), the transactions of the customer(s) involved are monitored by the MLCO.
- (viii) If following the evaluation described in paragraph (v) 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.
- (ix) 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.
- (x) The MLCO acts as a first point of contact with MOKAS, upon commencement of and during an investigation as a result of filing a report to MOKAS under (vi) above.
- (xi) The MLCO responds to requests from MOKAS and provides all the supplementary information requested and fully co-operates with MOKAS.
- (xii) The MLCO ensures that all branches and subsidiaries of the bank 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.
- (xiii) The MLCO is responsible for the evaluation, on an **annual basis**, of all risks arising from existing and new customers, new products and services and updating and amending systems and procedures applied by the bank for the effective management the aforesaid risks.
- (xiv) The MLCO is generally responsible for the timely and correct submission to the Central Bank of Cyprus of the prudential reports referred to in Chapter 10 of this Directive and providing the necessary explanations to the employees responsible for the preparation of the aforesaid returns. The MLCO responds on a timely manner to any queries or clarifications requested by the Central Bank of Cyprus in relation to information contained

in the aforesaid returns.

- (xv) 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 bank 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.
- (xvi) The MLCO keeps records with the full details of customers or group of connected customers (name, address, account number(s), branch 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.
- (xvii) 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.
- (xviii) The 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.
- (xix) The MLCO provides advice and guidance to other employees of the bank on the correct implementation of procedures and controls against money laundering and terrorist financing.
- (xx) The MLCO determines which of the bank'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 bank, an annual staff training program.
- (xxi) The MLCO maintains full records of the seminars and other training offered to the bank's employees and assesses the adequacy of the education/training provided.
- (xxii) The MLCO assesses the systems and procedures applied by a third person on whom the bank relies for customer identification and due diligence purposes (see Section 4.12) or who applies for the opening of "client accounts" (see paragraph 125 of this Directive).
- (xxiii) The MLCO assesses the adequacy of the policy measures and procedures against money

laundering and terrorist financing applied by non-EU banks which apply for the opening of correspondent accounts (see paragraph 133 of this Directive).

(xxiv) The MLCO ensures that the bank 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 bank 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 updating of the said lists with new or existing customers which the bank has decided, in the light of additional information obtained, to classify as high or low risk customers.

(xxv) The MLCO informs, through regular periodic reports (apart from the Annual Report prepared in accordance with Section 2.3 of this Directive), the Senior Management of the bank regarding the management of risks associated with money laundering and terrorist financing.

(xxvi) 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.

2.3 Annual Report of the Money Laundering Compliance Officer

14. The MLCO has also the additional duty of preparing an Annual Report which is a significant tool for assessing a bank'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.
15. 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 bank's Senior Management. In the case of a bank operating in Cyprus in the form of a branch, the Annual Report should be submitted to the bank's Board of Directors through the Senior Management of its country of origin.
16. The Board of Directors assesses and approves the Annual Report. The Senior Management of the bank will then take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report.

17. A copy of the Annual Report shall also be forwarded within the same time limit specified above, to the Bank Supervision and Regulation Department of the Central Bank of Cyprus.
18. 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 changes in the Law and the Central Bank of Cyprus' Directives which took place during the year and measures taken and/or procedures introduced for securing compliance with the above changes.
 - (ii) Information on the inspections and reviews performed by the MLCO and the bank's Internal Audit Unit and the material deficiencies and weaknesses identified in the bank's anti-money laundering and terrorist financing policies, procedures and controls. In this regard, the report should outline the seriousness of the issue, its risk implications and the recommendations made as well as the action taken for rectifying the situation.
 - (iii) The number of internal money laundering suspicious reports submitted by bank employees to the MLCO, broken down by district, address and branch and possible comments/observations thereon.
 - (iv) The number of suspicious reports submitted by the MLCO to MOKAS with information on the main reasons for suspicion and highlights of any particular trends.
 - (v) Information on circulars and other communication with staff on money laundering and terrorist financing preventive issues.
 - (vi) 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 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.
 - (vii) Information on the policy, procedures and controls applied by the bank in relation to high risk customers as well as the number and countries of origin of high risk customers with whom the bank has a business relationship such as companies with bearer shares, trusts, client accounts, politically exposed persons, correspondent accounts for non-EU banks and persons engaged in electronic gambling/gaming through the internet.
 - (viii) Information on the systems and procedures applied by the bank for the on-going

monitoring of accounts and transactions.

- (ix) 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.
- (x) Information on the training courses/seminars attended by the MLCO, Assistant MLCOs and any other educational material received.
- (xi) Information on training provided to staff during the year, including:
 - the courses/ seminars organised
 - their duration,
 - the number of employees attending,
 - names and qualifications of the instructor(s), and
 - specifying whether the courses/seminars were developed in-house or by an external organisation /consultant.
- (xii) Information on the next year's training program.
- (xiii) Results of the assessment of the adequacy and effectiveness of staff training.
- (xiv) 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.

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

3.1 Introduction

The Law Article 61(2) 19. The Law requires all persons carrying on financial or other business 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 must be able to demonstrate to the competent supervisory authorities that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

20. It is recognised that no system of checks will detect and prevent all cases of money laundering or terrorist financing. A system of procedures and controls on a risk sensitive basis aims at balancing the cost burden placed on banks and their customers with a realistic assessment of the threat of the banks being used for money laundering or terrorist financing. Consequently, applying measures and procedures on a risk sensitive basis enables banks to focus their efforts in those areas where the risk of money laundering and terrorist financing appears to be higher.

21. 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 threat to banks 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 in response to a bank's particular circumstances;
- helps to produce a more cost-effective system; and
- promotes the prioritisation of effort and activities of banks in response to the likelihood of money laundering or terrorist financing occurring;

22. 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 a bank. These are:

- identifying and assessing the money laundering and terrorist financing risks emanating from the particular customers, products, services, and geographical areas of operation of banks;
- 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 application across the bank by persons specifically appointed for that purpose by the Board and Senior Management.

3.2 Identifying and Assessing Risks

23. The MLCO has the responsibility to identify, record and evaluate all potential risks. Irrespective of the ways that this may be performed, 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 bank. There also needs to be a clear communication of policies and procedures across the bank, along with robust mechanisms to ensure that these are implemented effectively, weaknesses are promptly identified and improvements are made wherever necessary.

24. A risk-based approach starts with the identification, recording and assessment of the risk that has to be managed. Banks need to assess and evaluate the risk of how they might be involved through the use of their services by criminals for the purpose of money laundering or terrorist financing. The particular circumstances of each bank 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 bank is relatively simple, involving relatively few products and customers, or customers with similar characteristics, then the bank should focus on those customers who fall outside the 'norm'. The identification and assessment of risk that each bank faces presupposes the finding of answers to the following questions:

- What risk is posed by the bank's customers? (i.e. complexity of their legal 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? (i.e. customer transactions where there is no apparent legal financial/commercial rationale; situations where the origin of wealth and/or source of funds 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 bank affect risk? (i.e. non-face-to-face customers, customer introduced by a third person etc).
- What risk is posed by the products/services the customer is using? (i.e. making payments via electronic funds transfers , large cash deposits or withdrawals, investment products etc).

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

- The scale and complexity of a bank's activities.
- Geographical spread of its operations and its customers' activities.
- The nature and profile of customers as well as of products and services offered.
- The bank's distribution channels and practices.
- The volume and size of transactions.
- The degree of risk associated with each area of operations.
- 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

26. Once a bank 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 will involve 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.
27. 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 bank 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:
- Varying the customer due diligence procedures in respect of customers 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 (i.e. documents from independent and reliable sources, third person information, documentary evidence etc)
 - Obtaining additional customer or business relationship 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.
28. 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 which should be accompanied with the relevant due diligence procedures, regular monitoring and controls.
29. Low risk customers are those business relationships prescribed in Article 63 of the Law (see Section 4.6 of this Directive).
30. 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 determined by the bank itself to be classified 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 their nature present a higher risk of money laundering or terrorist financing.
31. In this connection, banks 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 bank itself) containing the customers' names, account number(s), branch where the account is maintained and date of commencement of business relationship. The said lists should be promptly updated with all new customers or existing customers that the bank has determined, in the light of additional information received, to classify under the low or high risk categories.

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

33. In view of this, documenting the measures set out in paragraphs 27-31 above in the risk management and procedures manual will assist banks 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 banks' internal procedures

34. Banks 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 bank will need to consider are the following:

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

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

3.5 Risk management is dynamic

35. 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 are managed and countered effectively.
36. Customers' activities change (without always the bank becoming aware) and the bank's products and services – and the way these are offered or sold to customers – change. The products/transactions attacked by prospective money launderers or terrorist financiers will also vary as perceptions of their relative vulnerability change.
37. In view of the above, a bank should keep its risk assessment report fully updated. It is, therefore, required that a bank revisits its assessment at least annually, even if it decides that there is no case for revision.

4. CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES

4.1 Introduction

38. Collecting and maintaining sufficient information about a customer and making use of that information for the purposes of customer identification 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 banks are used for the above mentioned illegal purposes. In addition to minimising the risk of a bank'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 banks from possible fraud and the underlying risks on their financial robustness and reputation.

4.2 When customer identification and due diligence procedures should be applied

*The Law
Articles 58
and 60* 39. Articles 58 and 60 of the Law require persons carrying on financial and other business 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;
- (i) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- (ii) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transactions;
- (iii) when there are doubts about the veracity or adequacy of previously obtained customer identification data, documents or information.

*The Law
Article 2* 40. 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 on financial or other business 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 41. In addition, banks 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) 42. 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 on financial or other business 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;

The Law Article 61(3) 43. 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 claims to be.

The Law Article 2 44. The Law (article 2) provides the following definitions in relation to the above
‘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:

(a) 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 a percentage of 10 % plus one share shall be deemed sufficient to meet this criterion;

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

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

(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;

(iii) 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 45. Article 62(1) of the Law requires that the verification of the identity of the customer and the
Articles 62(1), beneficial owner should be made before the establishment of a business relationship or the
62(2) and carrying out of the transaction.
62(4)

46. 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 little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact and before the execution of any transactions.

47. However, article 62(4) explicitly requires that in situations where the person carrying on financial or other business is unable to comply with the customer identification and due diligence procedures 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)*

48. Article 60(d) of the Law requires persons carrying on financial or other business 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.
49. Banks must ensure that their customer identification records remain completely updated with all relevant identification elements and information throughout the business relationship. In this respect, banks 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.
50. Despite the above and taking into account the level of risk, if at any time during the business relationship with an existing customer, a bank becomes aware that reliable or adequate data and information are missing from the identity and the business/economic profile of the customer, then the bank 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.
51. 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, banks should check the adequacy of the data and information held with regard to the customer's identity and business/economic profile, whenever one of the following events or incidents occurs:

- (1) An individual transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the business/economic profile of the customer.
- (2) There is a material change in the customer's legal status and situation, such as :
- (i) Change of director(s)/ secretary;
 - (ii) Change of registered shareholder(s) and/or beneficial owner(s);
 - (iii) Change of registered office;
 - (iv) Change of trustee(s);
 - (v) Change of corporate name and/or trading name(s) used; and
 - (vi) Change of the principal trading partners and/or assumption of new major business activities.
- (3) There is a material change in the way the account operates, such as :
- Change in the person(s) that are authorised to operate the account(s); and
 - Application for the opening of new account(s) or the provision of new banking service(s) and/or product(s).

52. 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 bank is unable to comply with the customer identification requirements set out in the Law and this Directive, then the bank 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)

53. Article 63(1) of the Law states that persons carrying on financial or other business may not apply customer identification and due diligence procedures in respect of the following business relationships:

1. Credit or financial institutions situated in the European Economic Area¹.
 2. Credit or financial institution carrying out one or more of the financial activities as these are defined in article 2 of the Law that are situated in a country outside the European Economic Area which:
 - a. in accordance with a decision taken by the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it applies requirements equivalent to those laid down in the European Union Directive, and
 - b. 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.
54. For the purpose of subparagraph 51(4) above, domestic public authorities of countries of the European Economic Area should fulfill the following criteria:
- (i) 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) the activities, as well as their accounting practices, are transparent;
 - (i) 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.
55. Irrespective of the above, the Law requires that banks should, in any case, gather sufficient information to establish if the customer qualifies for an exemption as mentioned above.
56. Furthermore, article 63(2) of the Law states that customer identification and due diligence procedures may not be applied 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 and the scheme rules do not permit the assignment of a member's interest under the scheme.
 - (2) electronic money, as defined in article 2 of the Electronic Money Institutions Law. (Law

The Law
Article 63(2)

¹ European Economic Area includes the member states of the European Union and three members of the European Free Trade Association (EFTA) i.e. Iceland, Liechtenstein and Norway,

86(I)/2004) provided that:

- (i) where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150, 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 1000 or more is redeemed in that same calendar year by the bearer.

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

The Law 57. Article 66(2) of the Law prohibits persons carrying on financial or other business to open or
Article 66(2) 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 58. Article 66(3) requires persons carrying on financial or other business to pay special attention
Article 66(3) to any money laundering or terrorist financing threat that may arise from products or
transactions that might favour anonymity, and take measures, if needed, to prevent their use
for such purposes.

59. 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 owner of the account and/or that he/she has been properly authorised to operate the account, the bank should apply reliable methods, procedures and control mechanisms over the access to the electronic means so as to ensure that it deals with the true owner or the authorised signatory to the account. Failure by banks 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 into financial losses or damage on the reputation of the bank either through fraud or acquisition of confidential information by third parties or non intentional involvement in illegal activities. In this regard and for the purposes of managing the risks emanating from customer transactions effected through electronic means, banks 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 60. Article 66(1)(a) prohibits banks from entering into or continuing a correspondent banking
Articles 66(1) relationship with a shell bank. Furthermore, it is required (article 66(1)(b)) that banks take
(a) and (b) 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 61. The Law (article 2) defines a “shell bank” as a credit institution or institution engaged in
Article 2 equivalent activities, incorporated in a jurisdiction in which it has no physical presence,
involving meaningful mind and management and which is unaffiliated with a regulated
financial group.

4.10 Failure or refusal to provide identification evidence

The Law 62. Article 62(4) of the Law requires that where the person carrying on financial or other business
Article 62(4) is unable to comply with articles 61(1)(a) to (c) of the Law, then it is not able to 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, it is warranted to file a report with MOKAS.

63. 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,
constitutes elements that may lead to the creation of a suspicion that the customer is involved in
money laundering or terrorist financing activities. In such an event, banks should not proceed
with the opening of the account, 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 64. Article 61(1) of the Law requires, inter-alia, that customer identification procedures and due
Article 61(1) diligence measures shall comprise the following:

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

(b) 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 on financial or other business 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

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

65. Banks 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 banks and kept in customers' files. However, it must be appreciated that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative.

66. A person's residential address is an integral part of the identity of 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 bank, then a relevant note describing the event should be prepared and kept in the customer's file.

67. Banks 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) banks 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 and, as a minimum, it 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 in the account and the expected destination (e.g. countries and names of principal counterparties) of outgoing transfers/payments.
- (v) The customer's sources and size of wealth and annual income.
- (vi) Clear description of the main business/ professional activities/operations.

68. The above mentioned information as well as all the 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 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.

69. 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 makes 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 70. Article 67 of the Law permits persons carrying on financial or other business to rely on third
Article 67 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.

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

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

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

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

73. Furthermore, the Law provides that the third persons could be any person carrying on financial activities or auditors or independent legal professional or trust and company service provides operating in countries outside the European Economic Area which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it applies procedures and measures for the prevention of money laundering and terrorist financing equivalent to those laid down in the European Union Directive. It is understood that the said third persons should meet the requirements mentioned in paragraph 72 above.

74. It should be noted that the terms “financial institutions” and “persons engaged in financial activities” do not include money transfer businesses or dealers in foreign exchange.

75. The Law provides that, in the case that a bank chooses to rely on a third person, it must require from the third person to:

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

(ii) immediately forward to the bank 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.

76. All copies of identification documents, data and information obtained by a bank should be

duly certified by the third person as true copy of the original. It is noted that banks 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 as regards management of funds and assets.

77. Moreover, the bank should obtain data and information so as to verify that the third person is subject to professional registration in accordance with the competent law of its country of incorporation and/ or operation as well as supervision for the purposes of compliance with the measures for the prevention of money laundering and terrorist financing.
78. Moreover, in the case where the third person on whom the bank relies for performing customer identification and due diligence procedures is an accountant or an independent legal professional or a trust and company services provider from a country which is a member of the European Economic Area or a third country that the Advisory Authority for Combating Money Laundering and Terrorist Financing has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive, then the bank is obliged, before accepting the customer identification data verified by the said third person, to apply the following additional measures/procedures :
- (i). Ascertain and evaluate the systems and procedures applied by the third person for the prevention of money laundering and terrorist financing. The said assessment should be performed by the bank's MLCO.
 - (ii). As a result of the above mentioned assessment, the bank is satisfied that the third person implements customer identification, due diligence and record keeping systems and procedures which are in line the requirements of the Law and this Directive.
 - (iii). The bank 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 in accordance with the appropriate law etc).
 - (iv). 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

at the establishment of a business relationship with customers.

4.13 Specific customer identification issues

4.13.1 Natural persons residing in Cyprus

79. Banks ascertain the true identity of natural persons who are residents of Cyprus by obtaining the following information:
- (i) True name and/or names used as these are stated on the official identity card or passport;
 - (ii) Full permanent address in Cyprus, including postal code;
 - (iii) Telephone and fax numbers;
 - (iv) E-mail address;
 - (v) Date and place of birth; and
 - (vi) The profession and other occupations of the customer including the name of employer/business organisation.
80. It is pointed out that according to the Banking (Amendment) (No 3) Law of 2004 (Law 231 (I) of 2004) the identification of a customer's identity should be based on an official identity card or passport submitted by the real owner of the account.
81. In addition to the name verification, it is important that the permanent address of the customer is also verified by using one of the following ways:
- (i) Visit at the place of residence (in such a case, the bank officer who carries out the visit should prepare a memo which must be retained in the customer's file);
 - (ii) The production of a recent (up to 6 months) utility bill, local authority tax bill and/or a bank statement (to protect against forged or counterfeit documents, the prospective customers should be required to produce original documents).
82. In addition to the above, an introduction from a reliable staff member or from another existing reliable customer who is personally known to the management, may assist the verification procedure. Details of such introductions should be recorded in the customer's file.
83. After banks are satisfied that the original identification documents have been presented, they should keep copies of the pages containing all relevant information which must be certified as true copies of the original documents by the bank's employee who verifies the customer's identity or the third person on whom the bank relies for the performance of the customer

identification and due diligence procedure (see Section 4.12. above).

4.13.2 Natural persons not residing in Cyprus

84. For prospective customers who are not normally residing in Cyprus, in addition to the information collected for the verification of the identity of residents of Cyprus (see paragraph 79 above), banks should require and receive information on public positions which the prospective customer holds or held in the last twelve months as well as whether he is a close relative or associate of such individual, in order to verify if the customer is a ‘Politically Exposed Person’ (see Section 4.14.2.5 of this Directive).
85. For those prospective customers not residing in Cyprus, passports and, where they exist, official national identity cards issued by competent authorities of their country of origin should be obtained. Certified true copies of the pages containing the relevant information from the said documents should be obtained and kept in the customers’ files. In addition, banks are advised, if in doubt for the genuineness of any document (passport, national identity card or documentary evidence of address), to seek to verify identity with an Embassy or the Consulate of the issuing country or a reputable credit or financial institution situated in the customer’s country of residence.
86. In addition to the aim of preventing money laundering and terrorist financing, the above information is also essential for implementing the financial sanctions imposed against various persons by the United Nations and the European Union. In this regard, passport’s number, issuing date and country as well as the customer’s date of birth should always appear on the copies of documents obtained, so that the bank 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.

4.13.3 Joint-Accounts

87. 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 above for natural persons.

4.13.4 Nominees or agents of third persons

The Law 88. Article 65(1) of the Law provides that persons carrying on financial or other business, shall
Article 65(1) 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.

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

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

90. In the case of accounts opened in the name of unions, societies, provident funds and charities, a bank should ascertain their object(s) of operation and satisfy itself as to the legitimate purpose of the organisation by requesting the production of the constitution/rules of procedures and registration documents with the competent governmental authorities (in case the law requires such registration). Moreover, banks should obtain a list of the members of 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.

4.13.6 Accounts of unincorporated businesses/partnerships

91. In the case of partnerships and other unincorporated businesses whose partners/directors/beneficial owners are not existing customers of the bank, the identity of the beneficial owners/controllers/partners and authorised signatories should be verified in line with the procedures applied for natural persons. Furthermore, in the case of partnerships, banks should also obtain the original or a certified copy of the partnership's registration certificate. Banks 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.

92. In cases where a formal partnership arrangement exists, a bank should also obtain mandate from the partnership authorising the opening of an account and conferring authority to those who will be responsible for its operations.

4.13.7 Accounts of corporate customers (companies)

The Law 93. Article 65 (2) of the Law provides that for customers that are corporate or legal entities, banks
Article 65(2) 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.

94. Due to the difficulties in identifying the true beneficial owners, corporate accounts are one of the most favourable vehicles for money laundering, particularly when fronted by a legitimate trading company. Banks 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 real beneficial owners and who exercise control over the company.

95. 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 in a recognised Stock Exchange of the European Union or a third country with equivalent disclosure and transparency requirements.
- (ix) The registered shareholders where they act as nominees of the beneficial owners.
- (x) The business profile of the company in accordance with the provisions of Section 4.11 as above.

96. For the purpose of verifying the above data/documents, banks 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 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 true 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) 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.
97. Where deemed necessary for a better understanding of the activities, sources and uses of funds/assets of a company, banks should obtain a copy of its latest audited financial statements (whenever available) , and/or a copy of its latest management accounts.
98. For companies incorporated outside Cyprus, banks should request and obtain documents similar to the above.
99. As an additional due diligence measure, and on the basis of the assessed risk emanating from the business relationship with a specific company, banks 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 normal operating company. 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 should be made for ascertaining the nature and any consequences of these changes on the documentation and information held by the bank for the company and determine as to whether, any supplementary information for updating the business profile of the company needs to be collected.

100. 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:

*The Law
Article 2*

- (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 directions of the company.

101. 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, banks 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*

102. Apart from verifying the identity of the beneficial owners, the Law (article 2) requires that banks 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, banks 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.

103. 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, banks are required to implement the procedure provided in Section 4.14.2.3 below.

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

104. Banks 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 it has been determined that applies requirements equivalent to those laid down in the European Union Directive for the prevention of money laundering and terrorist financing, and provided that

(i) they ascertain that the said persons possess the necessary license or authorisation from a competent supervisory/regulatory authority to provide the said services, and

(ii) are subject to supervision for anti-money laundering and terrorist financing purposes.

105. 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, banks should request and obtain, **in addition** to the above mentioned documentation and the information required by this Directive for the identification and verification of natural and legal persons, including the ultimate beneficial owners, the following:

(i) 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 with the relevant supervisory/regulatory authority or other independent and reliable sources;

(ii) 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.

106. 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, banks should implement the provisions of paragraphs 104 and 105 in relation to the parent companies, depending on the country of incorporation and operation of the parent company.

107. In the case of investment funds, banks, apart from identifying 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.

4.13.9 Safe custody and safety deposit boxes

108. 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, banks should follow the identification procedures 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* 109. Article 61(2) requires persons carrying on financial or other business to apply the customer
Article 61(2) identification and due diligence procedures set out in the Law but permits persons carrying on financial or other business to determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship, product or transaction. It is pointed out that according to the Law, persons carrying on financial or other business must be able to demonstrate to the competent authorities that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.
110. 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. 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.
111. However, for high risk products, accounts or customers, banks 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.
112. It is reiterated that a bank 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

113. The following categories of customers are designated either by the Law or the Directive of the Central Bank of Cyprus as high risk and, therefore, banks 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 hereinbelow:

4.14.2.1 Non-face to face customers

- The Law* 114. Article 64(1) of the Law requires persons carrying on financial or other business to apply, when a customer is not physically present for identification purposes, one or more of the following additional customer due diligence measures:
- Article 64(1)*
- (i) obtaining additional documents, data or information for verifying the customer's identity;
 - (ii) 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;
 - (iii) 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.
115. Whenever a customer requests the opening of an account, the bank should preferably hold a personal interview during which all information for customer identification should be requested and obtained. It is possible, however, that a customer, especially a non-resident, may request the opening of an account through mail, telephone, or the internet without presenting himself for a personal interview. In such a case, banks 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, banks 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.
116. Practical procedures that can be applied for the purpose of implementing measures (i) and (ii), referred to in article 64(1) of the Law for the purpose of mitigating the higher risk involved in non-face to face customers, are the following:
- (i) Direct confirmation of the prospective customer's true name, address and signature from a bank operating in his country of origin;
 - (ii) Obtaining a reference letter from a third person (as the latter is defined in article 67 of the Law);
 - (iii) The customer supplies the bank with the original customer identification documents e.g. passport, identity card, which are subsequently returned by registered and secured mail;

- (iii) Telephone contact with the customer at his residence or office, before the opening the account, on a telephone number which has been verified from an independent source;
- (iv) Contact with the customer through mail in an address previously verified from independent and reliable sources.

117. 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. Banks should take additional measures for ensuring that the company or legal entity operates at the address of its trading office and carries out legitimate business activities.

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

118. Banks 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 4.13.7 of this Directive, with regard to corporate customers the following supplementary due diligence measures:

- (i) The bank concerned takes physical custody of the bearer share certificates while the account relationship is maintained or obtains a confirmation from another bank operating in Cyprus or another country of the European Economic Area that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform it accordingly.
- (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 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 every year**, the third person who has introduced the customer must confirm that the capital base and the shareholding structure of the company or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones. If the account has been opened directly by the company, then the confirmation should be provided by the company's directors.

4.14.2.3 Accounts in the names of trusts

The Law
Article 65(2) 119. The Law requires that banks 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 2 120. 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 over 10% or more of the property of a legal arrangement or entity.

121. 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 banks' customers. When banks enter into such relationships, they must ascertain the legal substance of the trust, and its name and date of establishment, and verify the identify of the settlors, trustees and true beneficiaries.

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

4.14.2.4 "Client accounts" in the name of third persons

123. Third persons frequently hold funds on behalf of their clients in "client accounts" opened with banks. 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").

124. Banks 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 it has been

determined that it applies procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the European Union Directive.

125. In the case that the opening of a “client account” is requested by a third person acting as auditor/accountant 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 determined that it applies procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the European Union Directive, banks may proceed with the opening of the account provided that the following conditions are met:

- (i) The third person is subject to mandatory professional registration in accordance with the relevant laws of the country of operation.
- (ii) The third person is subject to regulation and supervision by an appropriate competent authority in the country of operation for anti money laundering and terrorist financing purposes.
- (iii) The MLCO has assessed the customer identification and due diligence procedures employed by the third person and has found them to be in line with the Law and this Directive. A record of the assessment should be prepared and kept in a separate file maintained for each third person.
- (iv) For general or pooled client accounts, the bank verifies the identify of all beneficiaries of credit transactions which equal or exceed 15.000 Euro. With regard to specific client accounts, the bank verifies the identity of the real beneficiary(ies) before opening the account.
- (v) The bank 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.

4.14.2.5 Accounts for Politically Exposed Persons (“PEPs”)

*The Law
Article
64(1)(c)*

126. Article 64(1)(c) of the Law requires that, in respect of transactions or business relationships with PEPs residing in a country of the European Economic Area or a third country, persons carrying on financial or other business should apply the following:

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

- (ii). have Senior Management approval for establishing business relationships with such customers;
- (iii). take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;
- (iv). conduct enhanced ongoing monitoring of the business relationship.

The Law
Article 2

127. The Law (article 2) defines that politically exposed persons means natural persons who are residing in another Member State of the European Union or a third country and who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.

128. Business relationships with individuals holding important public positions in a foreign country and with natural or legal persons closely related to them, may expose a bank to enhanced risks, especially, if the potential customer seeking to establish an account is a PEP, a member of his immediate family or a close associate that is known to be associated with a PEP. Banks 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, banks should assess which countries with which they maintain business relationships are more vulnerable to corruption or maintain laws and regulations that do not meet the 40+9 requirements of the Financial Action Task Force (see Section 4.14.2.9 of this Directive). With regard to the issue of corruption one useful source of information is the Transparency International Corruption Perceptions Index which can be found on the web-site of Transparency International at www.transparency.org. With regard to the issue of adequacy of application of the 40+9 recommendations of the FATF, banks 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.

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

- (i) natural persons who have, or had a prominent public function in a foreign country:
 - 1. heads of State, heads of government, ministers and deputy or assistant ministers;
 - 2. members of parliaments;

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

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

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

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

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

1. any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations with a person referred to in subparagraph (i) above.
2. any natural person who has sole beneficial ownership of a legal entity (company) or legal arrangement (trust) which is known to have been set up for the benefit de facto of the person referred to in subparagraph (i) above.

130. 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 129 above, for a period of at least one year, banks shall not be obliged to consider such a person as politically exposed.

131. Banks 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 bank faces, the acquisition and installation of a reliable commercial electronic database for PEPs which is available on the market, seeking and obtaining information from the customer himself or from publicly available information which, inter-alia, can be retrieved from the internet. In the case of companies, legal entities and arrangements, the procedures should aim at verifying whether the beneficial owners, authorised signatories and persons authorised to act on behalf of the company constitute PEPs. In case of identifying one of the above as a "Politically Exposed Person", then automatically the account of the company, legal entity or arrangement should be subject to the procedures stipulated in the Law and this Directive.

- (ii) The decision for establishing a business relationship with a PEP should be taken by the bank's Management. When establishing a business relationship with a customer (natural or legal) and subsequently it is ascertained that the person(s) involved are or have become PEPs, then the approval of the bank's Management should be given for continuing the operation of the business relationship and/or account.
- (iii) Before establishing a business relationship with a PEP, the bank should obtain adequate documentation to ascertain not only his/her identity but also to assess his/her business reputation (e.g. references from third parties);
- (iv) Banks should establish the business profile of the account holder by obtaining the information prescribed 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. Banks should be particularly cautious and most vigilant where their customers are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks; and
- (v) The account 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 bank officer in charge of the account. The note should be submitted for consideration and approval to the bank's Management and filed in the customer's personal file.

4.14.2.6 Correspondent accounts of banks outside European Union

The Law 132. Article 64(1)(b) requires for cross-frontier correspondent banking relationships with credit
Article institutions from third countries outside the European Union, the application of the following
64(1)(b) 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 Management before entering into new correspondent bank account relationship.
- (iv). Document the respective responsibilities of the bank 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 bank concerned.

133. In addition to the above measures, banks should ensure that the following conditions are met:

- (i) The respondent bank is either connected to a regulated financial group or maintains a physical presence in the form of a fully-fledged office carrying on real banking business in its country of incorporation i.e. the respondent 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 relevant supervisory body, or
 - obtaining from the respondent bank evidence of its group structure as well as licence or authorisation to conduct banking and financial business.
- (ii) The respondent bank employs adequate procedures to prevent money laundering and terrorist financing. In this regard, the MLCO banks should obtain and evaluate information on the respondent 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 respondent bank does not provide any services neither allows the use of its correspondent bank accounts by shell banks. Also, it must be ascertained whether the respondent 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 Management of the bank prior to entering into new correspondent banking relationships.

- (iii) The bank collects sufficient information to establish fully the nature of the respondent's business activities, ownership structure, management and places of operations and verifies the identity of its beneficial owner(s). In addition, the bank assesses, using publicly available information, its reputation and the quality of its supervision. Additional information for the respondent 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 respondent bank account must be operated by duly approved officials of the bank in the name of which the account is maintained. Customers of the bank or any other third parties should not be allowed to have direct or indirect access and make transactions through the account on behalf of the bank holding the account.
- (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.

4.14.2.7 Services to private banking customers

134. Private banking services offer the personal and discrete delivery of a wide variety of financial services and products to the 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 to establish that their use is genuine and be able to follow any chain of title to know who the beneficial owner is.

135. The role of the relationship officers is particularly important to the bank 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, banks 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, banks 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 from bank's officers and Management approval.
- (ii). The bank 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). Banks 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 for monies that are accepted for the account opening) will form the basis for the future regular monitoring of the account.
- (iv). The bank 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 bank may obtain a satisfactory written reference or references from a reputable, independent source or sources before opening an account for a customer. Such references should only be accepted when they are:
 - received direct from the referee;
 - specifically addressed only to the bank; and
 - verified as 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 periodic basis. In this respect, a bank 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.

4.14.2.8 Electronic gambling /gaming through the internet

136. Banks may enter into business relationships and open accounts in the names of persons who

are involved in the subject activities 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, banks must request and obtain, apart from the information required by this Directive for customer identification, depending on the circumstances of each case, 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 from other independent and reliable sources.

137. Furthermore, banks 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.
138. In the case that a bank's customer is a person who offers services (e.g. payment providers, software houses, card acquirers) to the persons mentioned in paragraph 136, then the bank 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. Also, banks should obtain information necessary to understand completely 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 bank must obtain the signed agreement between its customer and the company duly licensed by the competent authority of a country prescribed in paragraph 136 above to be engaged in electronic gambling/gaming activities.
139. For all the above cases, the decision for opening the account must be taken or approved by the Management of the bank. Moreover, the account must be closely monitored and subject to regular review with a view of deciding whether or not to permit the continuance of its operation.

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

140. The Financial Action Task Force's ("FATF") 40+9 Recommendations constitute today's primary internationally recognised standards for the prevention and detection of money laundering. The Government of Cyprus has formally endorsed FATF's Forty Recommendations and has directly assured the President of the FATF that the competent authorities of Cyprus will take all necessary actions to ensure full compliance and

implementation of the Recommendations. In this regard, the Central Bank of Cyprus is committed for the implementation of FATF's 40+9 Recommendations and all its other related initiatives in an effort to reduce the vulnerability of the banking system to money laundering and terrorist financing activities.

141. In this respect, banks are required to apply the following:

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

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

4.15 On-going monitoring of accounts and transactions

*The Law
Article
61(1)(d)*

143. 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 on 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)

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

145. 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 banks 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 bank, 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 enhanced 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, banks 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;

146. On-going monitoring of customers' accounts and transactions is an essential aspect of effective money laundering and terrorist financing preventive procedures. Banks 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, they would 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 financial or other business are required to refrain from performing 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.

147. 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 bank's records all high-risk customers as defined by the Law, this Directive and the Customer Acceptance Policy adopted by each bank. The management information system of each bank should be able to produce detailed lists of high risk customers so as to facilitate enhanced monitoring of accounts and transactions.
- Detecting of 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 responsible officials who have been appointed for that 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 must be ascertained.

148. In order to accomplish the above, banks 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 Management, the MLCO and other responsible officials based on the assessed risk of these accounts and transactions being used for with 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 periodically 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 bank 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 bank.

149. 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 prescribed 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 a bank 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 with no economic substance) or transactions where large sums of money in cash are involved 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

150. 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, is originated at the initial placement stage when criminals attempt to deposit cash derived from illegal activities into the financial system.

151. Consequently, banks 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, banks 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 bank puts in place, supporting data and information for the financial, commercial and other purpose of each transaction in cash should be obtained. The cash deposit transaction should be executed after a Management approval is granted to that effect. Banks should also request and obtain, on a risk sensitive basis, where deemed necessary, documentary evidence and data justifying the commercial/economic purpose of the large cash deposit. 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.

152. Banks are prohibited to accept cash deposits in foreign exchange 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 in accordance with the Capital Movement Law (“Declaration of Imported/Exported Currency/Bank Notes and/or Gold”) or the Regulation (EC) 1889/2005 of the European Parliament and of the Council

regarding the controls of cash entering or leaving the Community (“Declaration of Cash”), or

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

153. In this regard, the following are noted:

- (i) Under the Capital Movement Law (115(I) of 2003) any natural person who enters the Republic is obliged to declare to a competent officer of the Customs and Excise Department, any amount of banknotes, either in Euro or in foreign currency, the value of which is equal to or exceeds 12.500 Euro. The said Law applies for cash imported from other member states of the European Union.
- (ii) According to the Regulation (EC) 1889/2005 of the European Parliament and of the Council regarding the controls of cash entering or leaving the Community, any natural person entering or leaving the Republic, originating from a third country outside 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.

154. Cash deposits in foreign currency that have been imported from abroad and are equal to or exceed the aforementioned limits (depending on the country of origin), banks are required to obtain and file together with the transaction, a copy of the customs declaration form. Banks 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

155. 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 bank concerned.

156. 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 bank 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

157. A ‘group of connected persons’ is defined to be:

- (i) Members of family (i.e. husband, wife, children)
- (ii) the depositor and an enterprise in which the individual 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) the depositor and a company in which the individual 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) if the depositor is a legal entity, its holding company, subsidiaries, fellow subsidiaries, associated companies or entities which have a material interest in that person; and,
- (v) two or more depositors, natural or legal, which are financially inter-dependent or connected in such a manner that may be viewed as a single risk.

158. 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 which enables the holder of this interest to effectively appoint and control the majority of the company’s directors or exercising important influence.

5.2.4 Internal procedures and responsibilities of the Money Laundering Compliance Officers

159. 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 bank’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.

160. The MLCO should ensure, within the framework 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 notes is consistent with the financial condition, the cash flow outlook of the business and the activities of the customer concerned. Furthermore, the MLCO should ensure that the customer identification and due diligence procedures, prescribed in Section 4 of this Directive, are duly applied and that the funds involved are not suspected to be associated with any illicit activities.
161. 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.
162. The MLCO should monitor, at least on a monthly basis, the volume of deposits in foreign currency notes 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 Submission of Returns to the Central Bank of Cyprus

163. The MLCO should prepare and submit to the Central Bank of Cyprus the following

prudential returns:

- (i) A **“Monthly statement of one-off deposits in foreign currency notes in excess of the equivalent of 100.000 Euro which have been imported in Cyprus from abroad”** in which information shall be provided on the customers who effected one-off deposits of foreign currency notes which have been imported in Cyprus from abroad during the reporting month and which are accompanied by a duly completed ‘‘Declaration of Imported/Exported Currency/Bank Notes and/or Gold’’ form, as per the provisions of the Capital Movement Law (Law 115 (I)/2003) in respect of cash imported from other member states of the European Union or the ‘‘Declaration of Cash’’ form as per the provisions of the Regulation (EC) 1889/2005 in respect of cash imported from third countries outside the European Union. A specimen of the said return is enclosed as ‘‘Appendix 7’’ to this Directive.
- (ii) An **“Annual Statement of aggregate deposits in foreign currency notes in excess of the equivalent of 100.000 Euro in a calendar year”** in which information shall be provided on the customers whose aggregate cash deposits in the same calendar year (**excluding** those customers reported in the Monthly Statement described in paragraph (i) above) and for whom a written approval has been given for carrying out cash deposits over the determined limits on a continuous and regular basis. A specimen of the said annual return is attached as ‘‘Appendix 8’’ to this Directive.

5.2.6 Exempted cash deposits in foreign currency.

164. Notwithstanding the above, the following exemptions apply:

- (i) Deposits of foreign currency notes from the Government of the Republic of Cyprus.
- (ii) Deposits of foreign currency notes from semi-governmental organisations in Cyprus.
- (iii) Deposits of foreign currency notes from other banks licensed to operate in or from within Cyprus.

5.3 Cash Withdrawals

165. Large sums of cash withdrawals can expose the banks at risk, especially when the money is used by the final recipients for the financing of illicit activities.

166. Consequently, banks are requested to apply appropriate procedures to monitor cash

withdrawals for sums that exceed the 15.000 Euro or the equivalent in foreign currencies. In particular, banks, 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 bank puts in place, banks must request and obtain appropriate data and information for the economic, commercial or other purposes of each cash withdrawal which will be performed with the prior approval of the bank's Management. Banks should request and obtain, on a risk sensitive basis, where deemed necessary, documents and information that justify the economic/business purposes of large cash withdrawals.

6. RECORD KEEPING PROCEDURES

6.1 Introduction

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

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

- (i) Copies of the customer identification evidence;
- (ii) the relevant evidence and details of all business relationships and transactions, including documents for the recording of transactions in the accounting books; and
- (iii) the relevant documents and correspondence with customers and other persons with whom a business relationship is maintained.

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

168. Copies of the customers' identification evidence should be certified by the bank's employee who verifies the identity of the customer or the third person on whom the bank relies for the purpose of customer identification and due diligence procedure.

The Law
Article 68(3)

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

170. Moreover, banks 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 specified natural or legal persons and on the nature of that business relationship.

171. 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, banks must establish appropriate procedures to ensure the maintenance of books and records in a systematic and secured 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 above changes.

172. 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, banks 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:
 - (a) the origin of the funds;
 - (b) the type and amount of the currency involved;
 - (c) the form in which the funds were placed or withdrawn i.e. cash, cheques, wire transfers etc.;
 - (d) the identity of the person undertaking the transaction;
 - (e) the destination of the funds;
 - (f) the form of instructions and authority;
 - (g) the type and identifying number of any account involved in the transaction.

6.2 Format of records

173. 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.

174. 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 banks to be able to retrieve the relevant information without undue delay.

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

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

The Law
Article 47

6.3 Electronic funds transfers

Regulation
(EC) no.
1781/2006

177. In relation to the above subject, banks 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).

178. Banks should institute 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 prescribed in the said Regulation.

179. In cases where any of the requisite information is missing from the message or payment form accompanying the incoming wire transfer, then banks should consider, depending on the perceived risk of money laundering attached to the relevant transaction, whether it is advisable to apply one or more of the following measures:

1. Contact the originator's bank and request that complete information be made available on the ordering customer. If the missing information is not forthcoming, then the bank may decide not to accept the wire transfer and return it to the ordering customer's bank.
2. Consider whether the lack of full information on the ordering customer raises

suspicious for money laundering which need to be reported to MOKAS.

3. In the light of past experience and the circumstances of the case, consider as to whether the business relationship with the originating financial institution should be restricted or terminated.

The Law
Article 71

180. 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 the European 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 bank to its customers.

7. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES

7.1 Introduction

181. Although it is difficult to 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

182. 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 bank 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.

183. 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 banks and their staff in recognising the main methods used for money laundering and terrorist financing. The detection by banks of any of the transactions contained in the said 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 business / commercial purpose of the underlying transaction, and the circumstances surrounding the particular activity.

7.3 Internal reporting suspicious transactions and activities

*The Law
Article 27*

184. Under Article 27 of the Law it is an offence for any person who, in the course of his trade, profession, business or employment acquires knowledge or reasonable suspicion that another person is engaged in money laundering or terrorist financing, not to report to MOKAS the said information, as soon as is reasonably practical, after it comes to his

attention. Failure to report in these circumstances is punishable on conviction by a maximum of five (5) years imprisonment or a fine not exceeding 5.000 Euro or both of these penalties.

The Law
Article 26

185. In case of bank 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 bank 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, banks shall ensure that their employees are aware of their legal obligations and know the person (i.e. the MLCO) to whom they should be reporting money laundering or terrorist financing knowledge or suspicion.

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

187. 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

188. Article 70 of the Law requires persons engaged in financial or other business to refrain carrying out transactions which they know or suspect to be related 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 the attempt to carry out suspicious transactions. Where refraining from performing a suspicious transaction is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, persons carrying on financial or other business shall inform MOKAS immediately afterwards.

189. 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,
27 Katsoni Street, 2nd & 3rd Floors,
CY-1082 Nicosia.
Tel.: 22 446018
Fax: 22 317063

190. 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 or facsimile or by hand.
191. Having made a suspicious transaction/activities report, a bank may subsequently wish to terminate its relationship with the customer concerned for risk avoidance reasons. In such an event, however, banks 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 the MOKAS should, therefore, be maintained in an effort to avoid any frustration to the investigations conducted.
192. After submitting the report to MOKAS, banks are expected to adhere to any instructions given by MOKAS and, in particular, as to whether or not to continue or suspend a transaction. It is noted that Article 26(2) (c) of the Law empowers MOKAS to instruct banks to refrain from executing or delay the execution of a customer's order without such action constituting a violation of any contractual or other obligation of the bank and its employees.
193. 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

194. Article 58 of the Law requires persons carrying on financial or other business 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,
- (iv) the European Union's Directives with regard the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and

Furthermore, Article 58(e) 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.

195. The effectiveness of the procedures and recommendations contained 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 bank employees appreciate the seriousness of the background which led to the enactment of the Law and the level of their education with regard to their duties and statutory obligations for countering this serious problem. It is reminded that an employee 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 banks 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 banks establish complete measures to ensure that their staff is fully aware of their responsibilities and duties. In this regard, the MLCO has the responsibility, in cooperation with other competent units of the bank (i.e. the Personnel and Training departments etc), to prepare and implement, on an annual basis, an education and training programme for the staff as required by the Law and this Directive. 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:

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

196. The timing and content of the training provided to staff of the various departments of the bank should be adjusted according to the needs of each bank. Furthermore, the frequency of training can vary depending on to the amendments of legal and/or regulatory requirements, staff duties as well as any other changes in the country's financial system.
197. 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.
198. 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 bank has in place for that purpose. Customers service staff who deals directly with the public should be trained on the verification of new customers' identity, the exercise of due diligence on an on-going basis, the monitoring of accounts of existing customer and the detection of patterns of unusual and suspicious activity. On-going training should be given at regular intervals so as to ensure that staff is reminded of its duties and responsibilities and kept informed of any new developments.
199. 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, banks 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

200. This Directive is applicable to branches and subsidiaries established by banks under the approval of the Central Bank of Cyprus, in third countries outside the European Union. Banks 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.

201. In this regard, banks should forward this Directive, as well as the relevant sections from their risk management and procedures manual for the prevention of money laundering and terrorist financing, to the Board of Directors and Senior Management of their branches and subsidiaries in countries outside the European Union. The MLCO of the Head Office/parent bank 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 where 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 the legislation/regulations of the hosting country permit.

202. 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 bank concerned should immediately inform of this fact the Banking Supervision and Regulation Division of the Central Bank of Cyprus. In addition, the bank should take additional measures to effectively manage the enhanced 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 Monthly Statement of Large Cash Deposits and Funds Transfers

203. As from September, 1990, all banks in Cyprus have been submitting a monthly return on their large cash deposits and incoming and outgoing wire funds transfers. The submission of the above monthly return has proved to be particularly useful as it provides the opportunity to banks initially to 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 enhanced 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 is submitted to the Banking Supervision and Regulation Division within 15 days after the end of the reporting month as well as explanations and instructions for its completion.

10.2 Monthly Statement of one-off deposits in foreign currency in excess of the equivalent of 100.000 Euro which have been imported in Cyprus from abroad

204. In the abovementioned statement, information shall be provided on the customers who effected one-off deposits of foreign currency notes which have been imported in Cyprus from abroad which were accepted on the strength of a written approval by the MLCO and were accompanied by a duly completed “Declaration of Imported/Exported Currency/Bank Notes and/or Gold” form, as per the provisions of the Capital Movement Law (Law 115(I)/2003) or the “Declaration of Cash” form as per the provisions of the Regulation (EC) 1889/2005 of the European Parliament and of the Council regarding the controls of cash entering or leaving the Community (see Section 5.2 of this Directive). A specimen of the said return is attached as “Appendix 7” to this Directive and should be submitted to the Banking Supervision and Regulation Division within 15 days after the end of the reporting month.

10.3 Annual Statement of aggregate deposits in foreign currency notes in excess of the equivalent of 100.000 Euro in a calendar year

205. In the above mentioned statement, information shall be provided on the customers whose aggregate cash deposits in the same calendar year (excluding those customers reported in the Monthly Statement described in Section 5.2 of this Directive) exceeded 100.000 Euro

in a calendar year and which have been accepted on the strength of a written approval given by the MLCO for accepting cash deposits over the prescribed limit on a continuous and regular basis. A specimen of the said annual return is attached as “Appendix 8” to this Directive and should be submitted to the Banking Supervision and Regulation Division within one month from the end of the reporting year.

10.4 Adjustment of banks’ computerised accounting systems

206. To the above end, the Central Bank of Cyprus requires from all banks to adjust their computerised accounting systems so as to be able to identify promptly all cash deposits and funds transfers in excess of the limits specified for reporting in the monthly and annual returns. The early detection of cash and wire funds transactions will enable the reporting of complete and accurate information in the monthly and annual returns and will also enhance the ability of banks 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

207. The following Guidance Notes and their Supplements/Amendments issued under Article 60(3) of the Prevention and Suppression of Money Laundering Activities Laws of 1996-2004 are, hereby, repealed and cancelled:

<u>Edition</u>	<u>Title</u>	<u>Date of Issue</u>
Guidance Note	Prevention of Money Laundering	29 November 2004
Amendment No.1 to the Central Banks of Cyprus' Guidance Note issued in November 2004	Non-Cooperative_Countries_and_Territories ("NCCTS")	18 February 2005
Amendment No.2 to the Central Bank of Cyprus' Guidance Note issued in November 2004	Incoming Funds Transfers	18 May 2005
Amendment No.3 to the Central Bank of Cyprus' Guidance Note issued in November 2004	1. Issue of Non-Cooperative Countries and Territories ("NCCTS") 2. Non-EU Correspondent Bank accounts	14 November 2005
Amendment No.4 to the Central Bank of Cyprus' Guidance Note issued in November 2004	Deposits in Foreign Currency Notes	1 December 2005
Amendment No.5 to the Central Bank of Cyprus' Guidance Note issued in November 2004	Non-Cooperative Countries and Territories ("NCCTS").	11 July 2006
Amendment No.6 to the Central Bank of Cyprus' Guidance Note issued in November 2004	Non-Cooperative Countries and Territories ("NCCTS").	8 November 2006
Amendment No.7 to the Central Bank of Cyprus' Guidance Note issued in November 2004	Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds	21 December 2006
Amendment No.1 to Amendment No. 4 to the Central Bank of Cyprus' Guidance Note issued in November 2004	Regulation (EC) No 1889/2005 of the European Parliament and of the Council on controls of cash entering or leaving the Community	3 September 2007
Amendment No.8 to the Central Bank of Cyprus' Guidance Note issued in November 2004	Submission of returns to the Central bank of Cyprus	25 October 2007
Amendment No.9 to the Central Bank of Cyprus' Guidance Note issued in November 2004	Investment Funds and persons engaged in the provision of financial and investment services	7 November 2007

12. APPENDICES

APPENDIX 1

1. THE MAIN PROVISIONS OF THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES LAW OF 2007

1.1. Purpose

The main purpose of the above Law (hereinafter to be referred to as "the Law") is to define and criminalise the laundering of proceeds generated from all serious criminal offences including terrorist financing offences and provide for the confiscation of such proceeds aiming at depriving criminals from the profits of their crimes. It also places special responsibilities upon banks, financial institutions and professionals which are required to take preventive measures against money laundering and terrorist financing by adhering to prescribed procedures for customer identification, record keeping, education and training of their employees and reporting of suspicious transactions. The main provisions of the Law, which are of direct interest to banks and their employees, are as follows:

1.2. Prescribed offences (Article 3 of the Law)

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

- (i) money laundering offences; and
- (ii) predicate offences.

1.3. Money Laundering offences (Article 4 of the Law)

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

- (i) converts or transfers or removes such property, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of a predicate offence to evade the legal consequences of his actions;
- (ii) conceals or disguises the true nature, source, location, disposition, movement, rights with respect to property or ownership of this property;
- (iii) acquires, possesses or uses such property;
- (iv) participates in, associates, co-operates or conspires to commit, or attempts to commit and aids and abets and provides counselling or advice for the commission of any of the

offences referred to above;

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

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

1.4. Predicate offences (Article 5 of the Law)

Predicate offences are:

- a) all criminal offences punishable with imprisonment exceeding one year from which proceeds were generated that may become the subject of a money laundering offence as defined in Article 4.
- b) Terrorist financing offences as defined in Article 4 of the Ratification Laws of the United Nations Convention for Suppression of the Financing of Terrorism of 2001 and 2005, as well as the collection of funds for the financing of persons or organisations associated with terrorism.
- c) Offences for drug trafficking as defined in article 2 of the Law.

With regard to the terrorist financing offences it should be noted that on 22 November 2001, the House of Representatives enacted the Ratification Laws of the United Nations Convention for Suppression of the Financing of Terrorism. As a result of the above, terrorist financing is considered to be a criminal offence punishable with 15 years imprisonment or a fine of C€1 mn or both of these penalties. Furthermore, the above Law contains a specific Article which provides that terrorist financing and other linked activities are considered to be predicate offences for the purposes of Article 5 of the Prevention and Suppression of Money Laundering Activities Law of 2007. Consequently, suspicions of possible terrorist financing activities or collection of funds for terrorism financing should be immediately disclosed to MOKAS under Articles 27 and 69 of the Law.

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

1.5. Defences for persons assisting money laundering and duty to report (Article 26 of the Law)

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

In the case of employees of persons whose activities are supervised by one of the authorities established under Article 59, the Law recognises that the disclosure may be made to the MLCO in accordance with established internal procedures and such a disclosure shall have the same effect as a disclosure made to MOKAS.

1.6 Reports to MOKAS (Article 27 of the Law)

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

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

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

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

It is an offence to make a disclosure to the person who is the subject of a suspicion of money laundering or to a third person that information or other relevant material has been submitted to

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

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

Without prejudice to the provisions of article 48, persons carrying financial activities in accordance with article 2 of the Law, may disclose to other persons belonging to the same group operating in countries of the European Economic Area or a third country which according to a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it imposes procedures and measures for the prevention of money laundering and terrorist financing equivalent to those laid down in the European Union Directive, that information has been disclosed to the Unit in accordance with article 27 or that a money laundering or terrorist financing investigation is being or may be carried out by the Unit .

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

Furthermore, Article 49 provides that banks may exchange information among them in cases related to the same customer and the same transaction involving two or more banks provided that they are situated in countries of the European Economic Area or a third country which according to a decision of the Advisory Authority for Combating Money Laundering Offences and Terrorist Financing it has been determined that it imposes procedures and measures for the prevention of money laundering and terrorist financing equivalent to those laid down in the European Union Directive. The Law explicitly provides that information exchanged shall be used exclusively for the purposes of preventing money laundering or terrorist financing.

The disclosure and exchange of information made according to the above paragraphs is not considered to be a breach of any contractual or other legal restriction relating to the disclosure of information.

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

1.10 Special provisions for financial and other business activities (Part VIII of the Law)

The Law recognises the important role of the financial sector, accountants and lawyers and other professionals (real estates agents, dealer in precious metals and stones) for the forestalling and effective prevention of money laundering activities and terrorist financing and places additional administrative requirements on all institutions, including banks, for that purpose.

1.11 Procedures to prevent money laundering (Article 58 of the Law)

The Law requires all persons carrying on financial or other business, as defined in Section 2 of the Law, to establish and maintain specific policies and procedures to guard against their business and the financial system in general being used for the purposes of money laundering. In essence these procedures are designed to achieve two purposes: firstly, to facilitate the recognition and reporting of suspicious transactions and, secondly, to ensure through the strict implementation of the "know-your-customer" principle and the maintenance of adequate record keeping procedures, should a customer come under investigation, that the bank is able to provide its part of the audit trail. The Law requires that all persons engaged in financial or other business to establish appropriate systems and procedures in relation to the following:

- a) Customer identification and due diligence.
- b) Record keeping.
- c) Internal reporting and reporting to MOKAS.
- d) Internal control, assessment and management of risk with the purpose of preventing money laundering and terrorist financing.
- e) The detailed examination of any transaction which by its nature may be considered to be particularly vulnerable to be associated with money laundering or the financing of terrorism, and particularly of the sophisticated, complex and unusually large transactions and all unusual types of transactions that are realised without obvious economic or explicit legal reason.
- f) Employees awareness with regard to the
 - 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 purposes of money laundering and terrorist financing.
- g) The regular training of staff to recognise and handle suspicious transactions and activities which may be related to money laundering or terrorist financing offences.

It should be noted that the purpose of the Directives issued by the Central Bank of Cyprus, as the competent supervisory authority of banks in Cyprus, is to prescribe and indicate the practice which banks should adopt so as to achieve compliance with the requirements of the Law for the implementation of procedures for the prevention of money laundering and terrorist financing.

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

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

- (a) when establishing a business relationship;
- (b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- (c) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of transaction;
- (d) when there are doubts about the veracity or adequacy of previously obtained customer identification documents, data or information previously collected for the customer identification.

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

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

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

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

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

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

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

By derogation to the above, article 62(2) allows the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact.

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

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

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

Article 64 of the Law requires persons carrying on financial or other business to apply enhanced

customer identification and due diligence measures in the following situations:

1.15.1 Non-face to –face customers

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

- (i) obtain from the customer additional documentary evidence, data or information; or
- (ii) take supplementary measures to verify or certify the documents supplied or requiring confirmatory certification by a credit or financial institution covered by the European Union Directive; or
- (iii) ensure that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution operating in a country of the European Economic Area.

1.15.2 Correspondent banking relationships

For cross-frontier correspondent banking relationships with respondent institutions from third countries, the Law requires:

- (i) the collection of 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) the assessment of systems and procedures applied by the credit institution –customer for the prevention of money laundering and terrorist financing;
- (iii) obtaining approval from Senior Management before entering into new correspondent bank account relationship;
- (iv) documenting the respective responsibilities of the bank and of the credit institution-customer; and
- (v) as far as payable-through accounts are concerned, it must be ensured that the credit institution-customer has checked the identity of its customers and has performed on-going due diligence on the customers who have direct access to the correspondent bank accounts and that it can provide relevant customers' due diligence data upon request of the correspondent institutions.

1.15.3 Politically Exposed Persons

In respect of transactions or business relationships with politically exposed persons residing in a country member of the European Economic Area or in a third country, persons carrying on

financial or other business are required to:

- (i). have appropriate risk-based procedures to determine whether the customer is a politically exposed person;
- (ii). have Senior Management approval for establishing business relationships with such customers;
- (iii). take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;
- (iv). conduct enhanced ongoing monitoring of the business relationship.

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

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

Article 63(1) of the Law allows persons carrying on financial or other business not to apply customer identification and due diligence procedures in the following situations:

- (i). Credit or financial institutions situated in the European Economic Area.
- (ii). Credit or financial institutions carrying out one or more of the financial activities as these are defined in article 2 of the Law which is incorporated in a country outside the European Economic Area and which:
 - c. according to a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it imposes requirements equivalent to those laid down in the European Union Directive, and
 - d. is under supervision for compliance with the said requirements.
- (iii). Listed companies whose securities are admitted to trading on a regulated market in a country of the European Economic Area or a third country which is subject to disclosure requirements consistent with Community legislation;
- (iv). Domestic Public authorities of the countries of the European Economic Area.

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

1.17 Supervisory authorities (Article 59 of the Law)

The Law designates the Central Bank of Cyprus as the supervisory authority for all persons licensed to

carry on banking business in or from within Cyprus, the electronic banking institutions and the money transfer businesses. Furthermore, the Law designates the supervisory authorities of the remaining financial sector (Authority for the Supervision and Development of Cooperative Societies, Securities and Exchange Commission, Insurance Companies Control Service) as well as the supervisory authorities of lawyers (Cyprus Bar Association) accountants and auditors (Institute of Certified Public Accountants of Cyprus) real estate agents and traders of services and goods such as precious metals and stones (MOKAS). According to the Law, supervisory authorities are responsible for monitoring, supervising and evaluating the implementation of the Law and the Directives issued to persons under their supervision.

According to Article 59(4) of the Law, the supervisory authorities are empowered to issue directives to the persons under their supervision for the purposes of preventing money laundering and terrorist financing. The Law provides that the directives issued by the supervisory authorities are binding and compulsory with regard to their application.

Furthermore, supervisory authorities are empowered by virtue of Article 59(6) of the Law to take measures and impose sanctions on any person under their supervision who fails to comply with the Law or the Directives of the supervisory authorities or the European Union Regulation 1781/2006. The measures and sanctions provided in the Law are the following:

- (i). Require the supervised person to take such measures within a specified time limit set by the supervisory authority for remedying the situation.
- (ii). Impose an administrative fine up to 200.000 euro after first giving the right to the supervised person be heard, and in case the infringement continues, to impose an administrative fine up to 1 000 euro for every day the infringement continues.
- (iii). To amend or suspend or revoke the licence of operation of the supervised person.

1.18 Prohibition of cooperation with shell banks and anonymous accounts (Article 66 of the Law)

It is prohibited to persons possessing a banking business licence in accordance with the Banking Law of 1997 or the Cooperative Societies Law of 1985 to enter into or continue a correspondent banking relationship with a shell bank. The said persons are required to 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.

Persons carrying on financial or other business activities are prohibited to open or maintain anonymous or numbered accounts or accounts in fictitious names other than the ones stated in official identity documents.

1.19 Non-execution or delay in the execution of a customer's transaction (Article 71 of the Law)

Article 71 of the Law protects banks from a possible claim for damages from a customer in the event of refusal to execute or delay in executing any transaction for the account of that customer due to failure by the customer or any other party involved to provide sufficient details or information for the nature of the transaction and/or the parties involved as required by the Directives issued by the Central Bank of Cyprus in accordance with Article 59 of the Law or the European Union Regulation 1781/2006.

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

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

1.21 Orders for the disclosure of information (Article 45 of the Law)

Courts in Cyprus may, on application by the investigator, make an order for the disclosure of information by a person who appears to the Court to be in possession of the information to which the application relates. Such an order applies irrespective of any legal or other provision which creates an obligation for the maintenance of secrecy or imposes any constraints on the disclosure of information. As already stated above in relation to "tipping off", a person who makes any disclosure which is likely to obstruct or prejudice an investigation into the commission of a predicate offence, knowing or suspecting that the investigation is taking place, is guilty of an offence.

1.22 Service of orders to a supervisory authority (Article 75 of the Law)

Service of an order made under this Law to a supervisory authority shall be deemed as service to all persons who are subject to the control of the supervisory authority. Provided that the supervisory authority concerned shall be obliged to notify forthwith all the persons subject to its control about the order made under the Law.

1.23 Confiscation orders (Article 8 of the Law)

Courts in Cyprus are empowered to make a confiscation order on the assets of a person, including funds held on deposit with banks, if they determine that a person has benefited from committing a predicate offence. A confiscation order can be made before a person is sentenced or otherwise dealt

with in respect of any predicate offence.

1.24 Restraint and charging orders (Articles 14 and 15 of the Law)

Courts in Cyprus may also, by a restraint order, prohibit any person from dealing with any realisable property. In addition, they may also make a charging order, under Article 15 of the Law, on realisable property (immovable property and securities).

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 DateRef

MONEY LAUNDERING COMPLIANCE OFFICER'S
INTERNAL EVALUATION REPORT

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

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

ENQUIRIES UNDERTAKEN (Brief description)

.....
.....
.....

DOCUMENTS RESEARCHED/ATTACHED

.....
.....
.....

DETERMINATION/DECISION

.....
.....
.....

FILE REFERENCE.....

MONEY LAUNDERING

COMPLIANCE OFFICER'S Signature Date.....

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

I. GENERAL INFORMATION

Name of bank _____

Branch's address where account is kept _____

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

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

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

(A) NATURAL PERSONS

	<u>Beneficial owner(s) of the account(s)</u>	<u>Authorised signatory(ies) to the account(s)</u>
Name(s)	_____	_____
	_____	_____
Residential address(es)	_____	_____
	_____	_____
	_____	_____
	_____	_____

CENTRAL BANK OF CYPRUS
EUROSYSTEM

Business address(es)

_____	_____
_____	_____
_____	_____
_____	_____

Occupation(s) and Employer(s)

_____	_____
_____	_____
_____	_____
_____	_____

Date and place of birth

_____	_____
_____	_____
_____	_____
_____	_____

Nationality and passport number(s)

_____	_____
_____	_____
_____	_____
_____	_____

(B) LEGAL ENTITIES

Company's name, country
and date of incorporation _____

Business address _____

Main activities _____

CENTRAL BANK OF CYPRUS

EUROSYSTEM

	<u>Name</u>	<u>Nationality and passport number</u>	<u>Date of birth</u>	<u>Residential address</u>	<u>Occupation and employer</u>
<u>Registered shareholder(s)</u>	1. _____	_____	_____	_____	_____
	2. _____	_____	_____	_____	_____
	3. _____	_____	_____	_____	_____
<u>Beneficial owner(s)</u> (if different from above)	1. _____	_____	_____	_____	_____
	2. _____	_____	_____	_____	_____
	3. _____	_____	_____	_____	_____
<u>Directors</u>	1. _____	_____	_____	_____	_____
	2. _____	_____	_____	_____	_____
	3. _____	_____	_____	_____	_____
<u>Authorised signatory(ies) to the account(s)</u>	1. _____	_____	_____	_____	_____
	2. _____	_____	_____	_____	_____
	3. _____	_____	_____	_____	_____

III. DETAILS OF SUSPICIOUS ACTIVITY

DEBIT TRANSACTIONS	<u>Type</u>	<u>Amount</u>	<u>Date</u>	<u>Beneficiary</u>	<u>Beneficiary's bank</u>

CREDIT TRANSACTIONS	<u>Type</u>	<u>Amount</u>	<u>Date</u>	<u>Originator</u>	<u>Originator's bank</u>

(3) OTHER TRANSACTIONS
(please explain)

(4) KNOWLEDGE/SUSPICION OF
MONEY LAUNDERING
(please explain, as fully as possible,
the knowledge or suspicion
connected with money laundering)

IV OTHER INFORMATION

– Other accounts and banking services
used (deposit and loan accounts,
credit cards, off-the-Balance Sheet
commitments)

– Accounts with other banks in Cyprus or
abroad, (if known)

– Other customers' accounts kept with the bank
connected with the suspicious transactions

MONEY LAUNDERING

COMPLIANCE OFFICER'S Signature

Date

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

1. For natural persons, the relevant pages of customers' passports or ID card evidencing identity.
2. For legal entities, certificates of incorporation, directors and shareholders.
3. All documents relating to the suspicious transaction(s) (i.e. Swift messages, bank advice slips, correspondence etc.).

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 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 bank.
- (xviii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank.
- (xix) Numerous deposits of small amounts, through multiple branches of the same bank 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. Transactions through bank accounts

- (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 banks within the same locality, especially when the bank 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. Investment related transactions

- (i) Purchasing of securities to be held by the bank 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. Wire transfer/ international activity

- (i) The bank acts as an intermediary for the transfer of funds from a bank outside Cyprus to another bank 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 bank or any other bank 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 wire transfers received in an account when each transfer is below the reporting requirement in the remitting country.
- (ix) Wire 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) Wire 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 are 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) Wire 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 bank without any apparent purpose other than to disguise the nature, source, ownership or control of the funds.
- (iii) Frequent or numerous wire 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 for a bank 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 bank 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 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) Customers who want to be serviced by the same bank employee, even for routine transactions, or who stop transacting with the bank when a particular employee is out of office.
- (iv) Complex trust or nominee network.
- (v) 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.

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

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

(viii) Customers who use client account in the name of trustees instead of their own bank account.

B) TERRORIST FINANCING

1. Sources and methods

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

- 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 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.

Statement of Large Cash Deposits and Funds Transfers

Month: , 200...
Reporting Bank:

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 bank 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 bank'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 banks 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 banks 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 bank 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) Deposits from banks licensed by the Central Bank of Cyprus to carry on banking business in Cyprus.
- b) Deposits from government and semi-governmental organisations

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 bank 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 bank; and
- b) Inward funds transfers received by order of customers maintaining accounts with other banks 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 bank 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 bank; and

b) Outward funds transfers made in favour of customers maintaining accounts with other banks 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 bank 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.

APPENDIX 7

Monthly statement of one-off deposits in foreign currency notes in excess of the equivalent of €100.000 which have been imported in Cyprus from abroad

MONTH: _____

REPORTING BANK: _____

Customer's Name	Date of approval by the MLCO	Depositor's main activities and country of origin of cash	Amount of cash deposited in foreign currency €'000

I confirm that the above deposits of foreign currency notes are consistent with the financial condition, the cash flow outlook and the business activities of the abovementioned customers and that the provisions of the Central Bank of Cyprus's Directive for the prevention of money laundering and terrorist financing have been fully implemented.

(Date)

Signature: _____

(Money Laundering Compliance Officer)

Annual statement of aggregate deposits in foreign currency notes in excess of the equivalent of €100.000 in a calendar year

YEAR: _____

REPORTING BANK: _____

Customer's Name	Date of approval by the MLCO	Depositor's main activities and country of origin of cash	Amount of cash deposited in foreign currency €'000

I confirm that the above deposits of foreign currency notes are consistent with the financial condition, the cash flow outlook and the business activities of the abovementioned customers and that the provisions of the Central Bank of Cyprus's Directive for the prevention of money laundering and terrorist financing have been fully implemented.

(DATE)

Signature:

(Money Laundering Compliance Officer)