CENTRAL BANK OF CYPRUS

EUROSYSTEM

PREVENTION OF MONEY LAUNDERING

AND

TERRORIST FINANCING

DIRECTIVE TO CREDIT INSITUTIONS
IN ACCORDANCE WITH ARTICLE 59(4) OF THE PREVENTION
AND SUPPRESION OF MONEY LAUNDERING LAWS
OF 2007 TO 2018

FEBRUARY 2019

CONTENTS

		Page
INTRODUCTION		1
1. INTERNAL CONTROL PROCEDURES AND RISK MANAGEMENT		3
1.1	Obligation to establish procedures	3
1.2	Customer Acceptance Policy	9
2. THE ROLE OF THE ANTI-MONEY LAUNDERING COMPLIANCE OFFICER (AMLCO)		10
2.1	AMLCO Appointment	10
2.2	AMLCO Duties	11
2.3	AMLCO Annual Report	16
3. RISK BASED APPROACH		20
3.1	Introduction	20
3.2	Risk identification and assessment	22
3.3	Design and implementation of controls for risk management and mitigation	25
3.4	Monitoring and improving the operation of the internal procedures	27
3.5	Dynamic Risk Management	28
3.6	Risk Management Report	29
4. CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES		31
4.1	Introduction	31
4.2	When to apply customer identification and due diligence procedures	31
4.3	Identification and due diligence procedures	32

4.4 Timing of customer identification 34

4.5 Exercise of due diligence and updating of identification data of existing customers 35

4.6 Simplified identification and due diligence procedures 37

4.7 Prohibition of anonymous and numbered accounts and accounts in fictitious names 40

4.8 Transactions and products that favour anonymity 41

4.9 Prohibition of correspondent relationships with shell banks 41

4.10 Failure or refusal to provide identification evidence 42

4.11 Economic profile construction 42

4.12 Reliance on third parties for customer identification and due diligence purposes 44

4.13 Specific customer identification issues 49

4.13.1 Natural Persons 49

4.13.2 Customers within the scope of Law 64(I)2017 51

4.13.2.1 Identification documents for specific categories of natural persons within the scope of Law 64(I)/2017 54

4.13.3 Joint Accounts 55

4.13.4 Proxies or representatives of third persons 55

4.13.5 Accounts of unions, associations, clubs, provident funds, and charities 55

4.13.6 Accounts of unincorporated businesses/partnerships 55

4.13.7 Accounts of legal persons (companies) 56

4.13.8 Investment funds and businesses engaged in the provision of financial and investment services 60

4.13.9 Safe custody and rental of safety deposit boxes 62

4.14 Enhanced due diligence measures 62

4.14.1 Customer identification and due diligence on a risk based approach 62

4.14.2 High Risk Customers 64

4.14.2.1 Complex and unusually large transactions or unusual types of transactions 64

4.14.2.2 Accounts in the name of Trusts and Foundations 65

4.14.2.3 "Client accounts" in the names of third persons 66

4.14.2.4 Accounts of Politically Exposed Persons 68

4.14.2.5 Cross-border correspondence relationships with an institution-customer from a third country 73

4.14.2.6 Transactions with a natural person or legal entity established in a third country of high risk 76

4.15 On-going monitoring of the business relationship, accounts and transactions 79

5. CASH DEPOSITS AND WITHDRAWALS 86

5.1 Cash deposits 86

5.2 Deposits of cash imported from abroad 86

5.2.1 Prohibition to accept deposits of cash in foreign currencies imported from abroad 86

5.2.2 Acceptance of cash deposits in foreign currency 87

5.2.3 Definitions of group of connected persons and connected cash deposits 88

5.2.4 Internal procedures and responsibilities of the AMLCO 88

5.2.5 Exempted cash deposits 89

5.3 Cash withdrawals 89

6. RECORD KEEPING PROCEDURES 91

6.1 Introduction 91

6.2 Form of data 93

6.3 Electronic transfers of funds 94

7. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES 96

7.1 Introduction 96

7.2 Examples of suspicious transactions/activities 96

7.3 Internal Report of suspicious transactions/activities 97

7.4 Reports to MOKAS 98

8. STAFF TRAINING AND EDUCATION 100

9. APPLICATION OF THE DIRECTIVE TO BRANCHES AND SUBSIDIARIES OF CREDIT INSTITUTIONS 103

10. SUBMISSION OF DATA, INFORMATION AND PRUDENTIAL STATEMENTS TO THE CENTRAL BANK OF CYPRUS 107

10.1 Submission of data and information 107

10.2 Monthly statement of large cash transactions and funds transfers 107

10.3 Monthly statement of customer loans and deposits based on the country of permanent residence of the beneficial owner 107

10.4 Bi-annual report (RBA) 108

10.5 General Requirements 108

11. REPEAL AND CANCELLATION OF PREVIOUS CIRCULAR, DIRECTIVE AND AMENDMENTS 109

12. APPENDICES 110

Appendix 1: Internal Money Laundering or Terrorist Financing Suspicion Report 111

Appendix 2: Anti - Money Laundering Compliance Officer's Internal Evaluation Report 112

Appendix 3: Documents for the identification of specific categories of natural persons falling within the scope of Law 64(I)/2017 113

Appendix 4: Examples of suspicious transactions/activities related to money laundering and terrorist financing 114

INTRODUCTION

(i). In 1992, the Republic of Cyprus enacted the first Law by which money laundering deriving from drug trafficking was criminalised. Few years later, in 1996 the Republic of Cyprus enacted "The Prevention and Suppression of Money Laundering Activities Law" defining and criminalising money laundering deriving from all serious criminal offences. The said 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).

(ii). 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")[1] by which the former Laws on the prevention and suppression of money laundering activities of 1996-2004 were consolidated, revised and repealed. Under the Law, which came into force on 1 January 2008, the Cyprus legislation was harmonised with the Third European Union Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Directive 2005/60/EC). The Law was amended in the following years in order to adopt international standards and best practices enhancing the mechanisms to prevent money laundering and terrorist financing.

(iii). On the 3 April 2018 the amending Law came into force for harmonization with 'Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing, amending Regulation 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC'[2] hereinafter to be referred to as 'EU Directive'. The Law in this Directive is considered to be the basic Law and all its subsequent amendments.

(iv). 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 procedures that banks should adopt so as to comply with the requirements of the relevant legislation in force.

[1] https://www.centralbank.cy/en/licensing-supervision/prevention-and-suppression-of-money-laundering-activities-and-financing-of-terrorism-1
[2] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015L0849&from=EN

(v). The present Central Bank of Cyprus' Directive (Fifth Edition) (hereinafter to be referred to as "the Directive") is issued to all credit institutions in accordance with Article 59(4) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2018 ("The Law"), and aims to provide guidance to credit institutions for defining policy, procedures and control systems for compliance with the Law and with ultimate aim the effective prevention of money laundering and terrorist financing. It is emphasized that the Law explicitly states that Directives are directly binding and compulsory as regards their implementations by all persons to whom they are addressed. Furthermore, the Law assigns to the supervisory authorities, including the Central Bank of Cyprus, the duty of monitoring, evaluating and supervising the implementation of the requirements of the Law and of the Directives issued to the supervised entities.

(vi). The Central Bank of Cyprus may issue circulars and guidelines for the implementation of the Legal and Regulatory framework aiming to the compliance of the credit institutions which should be taken into account by the credit institutions.

1. INTERNAL CONTROL PROCEDURES AND RISK MANAGEMENT

1.1 Obligation to establish procedures

The Law Article 58

1. Article 58 of the Law requires from obliged entities to implement adequate and appropriate policies, controls and procedures, according to their nature and size in order to mitigate and manage effectively the risks related to money laundering and terrorist financing, for the following:

   (i) Customer identification and due diligence;

   (ii) record keeping;

   (iii) internal report and report to the Unit for Combating Money Laundering (MOKAS);

   (iv) internal control, assessment and management of risk in order to prevent money laundering and terrorist financing;

   (v) the thorough investigation of every transaction which is deemed to be, based on its nature, particularly susceptible to be connected with offences related to money laundering and terrorist financing, and especially of complicated or unusually large transactions and all unusual kinds of transactions that are executed without an obvious financial or explicit legitimate purpose;

   (vi) briefing and regular training of staff;

   (vii) risk management practices;

   (viii) compliance management; and

   (ix) recruitment and assessment of employees' integrity.

2. The Board of Directors, the Senior Management and, in the cases of branches of credit institutions from third countries operating in Cyprus, the Manager of the Cyprus branch, bear the final responsibility for ensuring that the credit institution applies an effective system to prevent money laundering and terrorist financing. Therefore, they have the ultimate responsibility to ensure that appropriate and effective systems and procedures for internal control have been introduced and applied, which reduce the risk of the products and services of the institution to be used for money laundering and terrorist financing. The commitment of Senior Management for the implementation of the above measures is a key element for the design and implementation of a risk based approach.

The Law Article 58C

3. According to Article 58C of the Law, the Senior Management approves the policies, procedures and controls implemented in relation to money laundering and terrorist financing, while monitoring and where appropriate enhancing the measures already taken.

The Law Article 2

4. According to Article 2 of the Law 'senior management' is an officer or employee of the obliged entity with sufficient knowledge of the obliged entity's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure and need not, in all cases, be a member of the Board of Directors.

5. The policies and procedures of credit institutions should clarify how the Senior Management intends to fulfil its responsibility for the reassurance and maintenance of an appropriate system of internal control for the prevention of money laundering and terrorist financing. This entails the definition of a guidance framework to the credit institution and its staff, that will define the persons, their duties and responsibilities for the implementation of specific aspects of the policy. Additionally, effective procedures should include appropriate management supervision, systems and controls, segregation of duties, training and other relevant practices.

The Law Article 58D

6. Article 58D of the Law requires that credit institutions appoint a member of the Board of Directors who will be responsible for the implementation of the Law and Directives, circulars and/or regulations issued by the Central Bank of Cyprus pursuant to the Law, and any other relevant acts of the European Union.

7. The credit institution, where there is a Board of Directors Audit Committee, appoints the Chairman of the Audit Committee, who will be responsible for the implementation of the Law and Directives, circulars and/or regulations issued by the Central Bank of Cyprus pursuant to the Law, and of any other relevant acts of the European Union and communicates immediately to the Central Bank of Cyprus the name of this person and any other subsequent changes as provided for by Article 58D of the Law. Otherwise, the credit institution appoints a non-executive member of the Board of Directors. The role and responsibilities of the said person should be recorded in the Board of Directors operating manual and should be approved by the Board of Directors.

The Law Article 58B

8. Article 58B of the Law requires the establishment of an independent internal audit function which will be responsible to verify that credit institutions have established the internal policies, controls and procedures referred to in Article 58.

9. The Directive of the Central Bank of Cyprus on Governance and Management Arrangements in Credit Institutions issued in July 2014, requires that credit institutions, as these are defined in

paragraph 3 of the said Directive, to set up a Compliance Function which will be independent from the business departments, as well as organisationally independent from the other control functions. It is noted that less complex or smaller institutions may, with the consent of the Central Bank of Cyprus, combine the duties of the units of compliance and/or information security with the duties of the risk management function.

10. The said Directive, among other, provides that the Compliance Function of credit institutions or the Risk Management Function (in cases where there is no Compliance Function) establishes and implements appropriate procedures with the aim of the prompt and continuous compliance of the credit institution with the current supervisory and regulatory framework, including the Law and the Directives for the prevention of the use of the financial system for money laundering and terrorist financing. Hence, the Anti-Money Laundering Compliance Officer ('AMLCO'), who is appointed in accordance with article 69 of the Law, should organisationally report to the Compliance Function or, in cases where there is no Compliance Function, to the Risk Management Function.

11. The AMLCO is appointed by the Board of Directors of the credit institution and may be the same person as the Head of the Compliance Function. The AMLCO of a branch of a credit institution from a third country that is operating in Cyprus, is appointed by the Board of Directors of the credit institution and reports directly to the Manager of the Branch and the Head AMLCO of the Group.

The Law Articles 59(6)(a)(iv) and (v)

12. According to Article 59(6)(a)(iv) and (v) the Central Bank of Cyprus may, among others, forbid temporarily to persons that exercise managerial duties in a credit institution or any other natural person is considered responsible for any breach of the Law or Directive, the exercise of managerial duties in a credit institution. Also, it may impose an administrative fine, as defined in Article 59(6)(a)(ii), to persons that exercise managerial duties in a credit institution, or to any other person, in case where it is determined that the breach was a result of their fault, deliberate omission or negligence. The Central Bank of Cyprus may, upon its judgement, publish the name of the natural person who committed the breach and the type of the breach.

13. The Central Bank of Cyprus requires from credit institutions to establish the following measures and procedures:

    (i) The Board of Directors defines, records and approves the general principles of the credit institution's policy for the prevention of money laundering and terrorist financing, which it communicates to Senior Management and the AMLCO. An effective program for the prevention of money laundering and terrorist financing requires a clear message from the

institution's management in relation to the risk appetite, which will determine the expectations, parameters and limits of operation of the organisation and also the commitment against money laundering and terrorist financing.

(ii) The Board of Directors gives an example of leadership by expressing with consistency the underlying values of corporate compliance culture ensuring that its behavior reflects the values that it embraces.

(iii) In case a credit institution maintains branches or subsidiaries outside Cyprus, it should implement policies and procedures at Group level (refer to Chapter 9 of this Directive)

(iv) The Board of Directives and Senior Management should have knowledge of the level of risk for money laundering and terrorist financing that the credit institution is exposed to, so as to decide whether all necessary measures are taken for its management and minimisation, according to the risk appetite of the credit institution. Therefore, the AMLCO is responsible to prepare and submit for approval to the Board of Directors through the Senior Management, a report recording and assessing the risks for money laundering and terrorist financing, considering the areas where the credit institution is operating, the provision of new products and services, acceptance of new customers, the expansion to new markets/countries, the complex shareholding structure of legal persons, the method of attracting customers, the measures taken for their management and minimisation and also the mechanisms for monitoring the right and effective operation of internal regulations, procedures and controls (refer to Chapter 3 of this Directive).

(v) The AMLCO is responsible in cooperation with other departments of the credit institutions (e.g. Organisation & Methods) for designing policies, procedures and controls and also the description and clear definition of responsibilities and limits of responsibility of each department that is dealing with matters related to the prevention of money laundering and terrorist financing. Therefore, an appropriate manual of procedures and risk management is prepared, which after approved by the Senior Management of the credit institution, it is communicated to the officials and to all staff that is responsible to implement the policy, procedures and controls adopted by the credit institution. The procedures manual covers, among other things, the customer acceptance policy of the credit institution, the procedures for establishing a business relationship, execution of occasional transactions, accounts opening and performing of customer due diligence, including the documents and information required for the establishment of a business relationship and for the execution of transactions, the information and documents record keeping and the procedures for on-going monitoring of accounts and transactions, the procedures and controls for the detection of unusual and suspicious transactions and their reporting to the AMLCO. Also,

it should include the policies and procedures of compliance with Regulation (EU) 2015/847)[3] of the European Parliament and Council of 20th May 2015 regarding the information that accompany the fund transfers and the repealing of the EU Regulation 1781/2006 (hereafter referred as the 'Regulation (EU) 2015/847), the processing of personal data, and also the exchange of information within the Group.

(vi) The manual is periodically assessed and is updated when deficiencies are found or when the need arises to adapt the credit institution's procedures for a more effective management of the risks from money laundering and terrorist financing. It should be noted that any updates of the manual should be approved by Senior Management.

(vii) Explicit duties and responsibilities are assigned through the policies and procedures so as to ensure the effective management of the policy, procedures and controls for the prevention of money laundering and terrorist financing and achieving compliance with the Law, the Directives, the Circulars and the Guidelines of the Central Bank of Cyprus and the provisions of Regulation (EU) 2015/847.

(viii) The AMLCO, the Alternate AMLCO, the Assistant AMLCOs and other members of staff who have been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, have full and prompt access to all data and information concerning customers' identity, transactions' documents and other relevant files and information maintained by the credit institution so as to be fully facilitated in the effective discharge of their duties.

(ix) The staff of the credit institution is informed about the person appointed as AMLCO to whom they should report any information concerning transactions and activities for which they believe or suspect that they might be related to money laundering and terrorist financing.

(x) There is a clear and concise reporting chain, explicitly prescribed in the manual of procedures and risk management by which information regarding suspicious transactions is reported without delay and directly to the AMLCO.

(xi) Policies, procedures and measures are applied so as the risk of money laundering and terrorist financing is identified, assessed and managed during the day-to-day operations of the credit institution in relation to (a) the development of new products, services, new business practices, including new delivery channels (b) the use of new or developing technologies for both new and existing products and (c) possible changes in the business profile of the credit institution (e.g. penetration to new markets by opening

[3] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015R0847&from=EN

branches/subsidiaries in new countries/areas). This risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies.

(xii) The ability to make proper decisions might be weakened by insufficient data quality. Hence, credit institutions must ensure an adequate level of data quality maintained in the customers' files and the information systems. In this respect the credit institution ensures that its policies, controls and procedures ensure the data quality management in terms of accuracy, validity and integrity. The roles and responsibilities regarding data quality should be clearly defined and well organised.

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

(xiv) The Board of Directors and the Senior Management receive regular, adequate and objective information so as to obtain an accurate picture of the risks of money laundering and terrorist financing to which the credit institution is exposed through its operations/activities and/or its business relationships.

(xv) The Board of Directors and the Senior Management receive regular, adequate and objective information from the AMLCO and the Internal Auditor regarding the effectiveness of the measures and controls against money laundering and terrorist financing.

(xvi) The Internal Audit inspects and evaluates, at least on an annual basis, the effectiveness and adequacy of the policy, procedures and controls applied by the credit institution for preventing money laundering and terrorist financing and periodically and according to the risk through regular or special audits, verifies the level of compliance of the institution with the Law, the Central Bank of Cyprus' Directive and the Regulation (EU) 2015/847. The audit program should be appropriate to the size, nature of operations and risk profile of the credit institution. The findings and observations of the Internal Audit are submitted to the Board of Directors' Audit Committee and are notified to the Senior Management and the AMLCO of the credit institution who take the necessary measures to ensure the rectification of any weaknesses and omissions which have been recorded. The Internal Auditor monitors, on a regular basis, through progress reports or other means the implementation of his/her recommendations.

(xvii) The credit institutions apply explicit procedures and standards of recruitment and evaluation of the employees' integrity (existing and new recruits).

1.2 Customer Acceptance Policy

14. Credit institutions should develop and establish a clear policy as well as procedures for accepting new customers, fully in line with the provisions of the Law and the requirements of this Directive. The relevant policy should be prepared after detailed assessment of the risks encountered by each credit institution from its customers and/or their transactions and/or their countries of origin or operations (See Section 3 of this Directive). The AMLCO prepares the customer acceptance policy and submits it through the credit institution's Senior Management to the Board of Directors for consideration and approval. Once approved, the said policy is communicated to the competent staff of the credit institution.

15. The said policy should set in an explicit manner the criteria for accepting new customers, the types of customers that will not be acceptable for a business relationship and should prescribe the categories of customers regarded as high risk. In determining the risk appetite of the credit institution and the customer acceptance policy, due consideration should be given to shell companies, complex business structures, and the risks that such entities may accumulate and the implementation of enhanced due diligence measures for the effective monitoring and mitigation of such risks, provided that the credit institution is capable to undertake and monitor this risk. The knowledge and understanding of staff for the operations of the customer should also be considered. The said policy should also determine the conditions and relevant procedures under which a customer relationship should be terminated. The description of the types of customers that are not acceptable for a business relationship and the categories of high risk customers should take into account factors such as the content and nature of their business activities, their country of origin and/or residence, the anticipated level and nature of business transactions of the customer, as well as the expected source and origin of funds. The customer acceptance policy and related procedures should provide for enhanced due diligence for high risk customers as they are prescribed in the Law, this Directive and also those customers that the credit institution itself has classified as high risk on the basis of its developed policy.

2. THE ROLE OF THE ANTI-MONEY LAUNDERING COMPLIANCE OFFICER ("AMLCO")

2.1 AMLCO Appointment

The Law Article 69

16. Article 69 of the Law requires from obliged entities to apply the following internal reporting procedures and reporting to MOKAS:

    (i) Appoint a senior staff member who has the skills, knowledge and expertise as the AMLCO to whom a report will be submitted for any information or other matter which comes to the attention of a member of the staff and which, in the opinion of that person, proves or creates suspicions that another person is engaged in money laundering or terrorist financing,

    (ii) require that any such report be considered in the light of all other relevant information by the AMLCO to determine whether the information or other matter set out in the report indeed proves this fact or creates such suspicion,

    (iii) allow the AMLCO to have direct and prompt access to other information, data and documents which may be of assistance to him/her and which are available at the obliged entity, and

    (iv) ensure that MOKAS is immediately informed, on their own initiative, by submitting a relevant report and providing additional information at the request of MOKAS, when they know or have reasonable suspicion that funds, irrespective of the amount, constitute revenue from money laundering and terrorist financing.

    Further, the Law explicitly states that the obligation to report to MOKAS includes the attempt to conduct such suspicious transactions.

17. The AMLCO is appointed by the Board of Directors of the credit institution. The Central Bank of Cyprus reserves the right to request his/her substitution if, in its opinion, he/she is no longer "fit and proper", as laid down in Article 69(a) of the Law, to discharge his/her duties. The credit institutions should inform immediately the Central Bank of Cyprus for the appointment of the AMLCO, submitting his/her position/hierarchy and reporting lines within the organisational structure of the credit institution and communication details. Credit institutions should inform staff of the AMLCO's contact details.

18. In case of termination/resignation of the AMLCO the credit institution should immediately inform the Central Bank of Cyprus.

19. The AMLCO should be established in Cyprus, act independently and autonomously in order to fulfil his/her obligations and must hold the appropriate rank so as to have the desired status

under the circumstances. Therefore, in order to safeguard his/hers impartial judgement and to facilitate impartial consultancy to the management, the AMLCO should not, for example, have business responsibilities or undertake responsibilities for the data protection framework or the operation of the internal audit. Also, he/she should not have any other duty within or outside the institution which may create a conflict of interest or jeopardize his/her impartiality with respect to his/her role and duties as AMLCO.

20. Additionally, the credit institution should appoint an Alternate AMLCO who substitutes the AMLCO in case of his/her absence. Where it is deemed necessary, due to the volume and/or the geographic spread of the credit institution's operations, credit institutions may appoint "Assistant AMLCOs" by division, geographical district or otherwise for the purpose of assisting the AMLCO and the immediate forwarding of internal suspicion reports to the AMLCO. Credit institutions should inform staff of the Alternate AMLCO's contact details.. The credit institutions should immediately communicate the appointment of the Alternate AMLCO to the Central Bank of Cyprus, providing his/her name, position and contact details.

21. Credit institutions that keep branches or subsidiaries in another member state or a third country appoint the AMLCO as a coordinator, for ensuring the implementation by all the companies of the group, which are engaged in financial activities, of the group policy and the adequate and appropriate systems and procedures for the effective prevention of money laundering and terrorist financing. Hence, the AMLCO should monitor on a continuous basis the compliance with the obligations through on-site or off-site audits.

2.2 AMLCO Duties

22. The Compliance Function or, where it does not exist, the AMLCO should maintain a procedures manual for all his/her tasks/responsibilities.

23. The role and responsibilities of the AMLCO, the Alternate AMLCO and also the Assistants AMLCOs should be clearly defined and recorded in the said manual.

24. As a minimum, the duties of the AMLCO should include the following:

    (i) The AMLCO has the responsibility, to record and assess on an annual basis all risks arising from existing and new customers, new products and services and the adoption of measures with additions or changes to the systems and procedures implemented by the credit institution for the effective management of the aforesaid risks. The relevant report should be submitted to the Board of Directors of the credit institution through the Senior Management for approval. A copy of the approved report should be submitted to the Central

Bank of Cyprus together with the AMLCO's annual report. Furthermore, in addition to the aforementioned annual briefing of the Board of Directors and the Senior Management on the risks encountered by the credit institution, the AMLCO should notify of any differentiation of those risks.

(ii) The AMLCO prepares the Customer Acceptance Policy which he/she submits, through Senior Management of the credit institution, to the Board of Directors for consideration and approval, based on the risk assessment that every credit institution encounters from its customers and/or their transactions and/or the counties of origin or of business operation. It is understood that the AMLCO holds the responsibility to submit suggestions for the amendment of the said policy considering the risks that should be addressed.

(iii) The AMLCO has the primary responsibility for the preparation of the manual of procedures and risk management in relation to money laundering and terrorist financing. The manual is assessed periodically and updated when deficiencies are detected or when the need arises to adapt the credit institution's procedures for the effective management of the risks emanating from money laundering and terrorist financing.

(iv) Without prejudice to the obligations of the Compliance Function, the AMLCO monitors and assesses the correct and effective implementation of the policy, procedures and controls that have been introduced by the credit institution for the prevention of money laundering and terrorist financing, and at group level, where applicable. In this regard, the AMLCO should apply appropriate monitoring mechanisms (including off-site and on-site visits to units/branches/departments) which will provide him/her with the necessary information for the level of compliance of the credit institution with what is currently in force. In case the AMLCO identifies shortcomings and/or weaknesses in the application of the required procedures and controls, he/she should give appropriate guidance for corrective measures and implement mechanisms to monitor these measures. The AMLCO should occasionally inform the Board of Directors and the Senior Management of the findings of these audits and the level of compliance of the credit institution. The AMLCO of branches should inform the manager of the branch and the Group AMLCO.

(v) The AMLCO receives information from the credit institution's staff which create a suspicion of money laundering or terrorist financing activities or might be related with such activities. The submission of an internal suspicion report should be done in a special form which is easily accessible to the staff of the credit institution. A specimen of such an internal suspicion report (to be referred to as "Internal Suspicion Report for money laundering and terrorist financing") is attached, as Appendix 1, to this Directive. All the above reports should be archived and kept in a separate file.

(vi) The AMLCO evaluates and examines the information received as per paragraph (v) above, citing other available sources of information and discusses the events in relation to the specific case with the reporting employee and, where deemed necessary, with the senior officers of the reporting employee. The evaluation of the information included in the suspicion report submitted to the AMLCO should be made on a separate form which should also be archived in the relevant file. The said report which is referred as "Evaluation of Internal Suspicion Report for money laundering and terrorist financing" is attached, as Appendix 2, to this Directive.

(vii) If, as a result of the evaluation described in paragraph (vi) above, the AMLCO decides to reveal the information to MOKAS then his/her report should be submitted to MOKAS via the secure communication channels as defined by MOKAS, the sooner possible. The obliged entities are required to implement a system that will allow them to produce the said reports in a printed form for audit purposes.

(viii) After the submission of suspicion report to MOKAS the transactions of all customers included in the report should be duly monitored by the AMLCO.

(ix) If, as a result of the evaluation described in paragraph (vi) above, the AMLCO decides not to reveal the relevant information to MOKAS then he/she should fully explain the reasons for such a decision on the "Evaluation of Internal Suspicion Report for money laundering and terrorist financing" which should, as already stated, be archived in the relevant file.

(x) The AMLCO maintains a registry with statistical information (e.g. district and branch where the involved customer accounts are maintained, date of submission of the internal report, date of evaluation, date of reporting to MOKAS) in relation to the internal suspicions reports and the AMLCO's suspicions reports to MOKAS.

(xi) The AMLCO acts as a first point of contact with MOKAS, upon commencement of, and during the investigation of the case examined after the submission of the suspicion report to MOKAS in accordance to paragraph (vii) above.

(xii) The AMLCO responds to all requests and requested clarifications from MOKAS and provides all the information, documents requested and fully co-operates with MOKAS.

(xiii) The AMLCO should ensure that all branches and subsidiaries, where the credit institution holds the majority of the share capital and operate in third countries have taken all necessary measures for achieving full compliance with the provisions of this Directive in relation to customer identification and customer due diligence measures and record keeping procedures. In the cases where the credit institutions operate business in another Member

State, the AMLCO ensures that these entities comply with the corresponding legislation of the other member state.

(xiv) The AMLCO must prepare policies and procedures at Group level, including policies for exchange of information and in relation to data protection.

(xv) The AMLCO has the general responsibility for the timely and correct submission to the Central Bank of Cyprus of the prudential reports referred to in Section 10 of this Directive. Additionally, he/she evaluates the above information and where required, investigates trends which may indicate risks of getting involved in transactions or activities related to money laundering or terrorist financing and proceeds promptly to take additional measures, where necessary. The AMLCO responds promptly to any queries or clarifications requested by the Central Bank of Cyprus in relation to information contained in the aforesaid reports.

(xvi) The AMLCO is responsible for examining and deciding on the applications for accepting cash deposits in foreign currency, referred to in Section 5.2 of this Directive, submitted in writing by the responsible officers of the branches/units of the credit institution where the affected customers' accounts are maintained. Copies of the applications and his/her related decision should be kept, by the AMLCO, in a separate file as well as in the file of the customer.

(xvii) The AMLCO 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 an occasional cash deposit or a series of cash deposits on a continuous and regular basis. In this respect, the AMLCO must keep separate records for customers who are involved in: (i) occasional cash deposits, and (ii) cash deposits on a continuous and regular basis

(xviii) The AMLCO maintains a register for a period of five years of all cases of persons (prospective customers) with whom the establishment of a business relationship was not allowed.

(xix) The AMLCO responds to all questions and requests for clarifications from the Central Bank of Cyprus, provides all requested information and data and co-operates fully with the Central Bank of Cyprus.

(xx) The AMLCO ensures that he/she, the Alternate AMLCO and the Assistant AMLCOs acquire, the requisite by their duties, knowledge and skills for the improvement of the procedures for prompt recognition, prevention and obstruction of any transactions and activities aimed at money laundering and terrorist financing.

(xxi) The AMLCO provides advice and guidance to the management and staff of the credit institution on matters relating to prevention of money laundering and terrorist financing.

(xxii) The AMLCO decides for the services/branches and employees of the credit institution who need further training and/or education in order to prevent money laundering and terrorist financing and organises appropriate training workshops/seminars. In relation to this he/she prepares and implements, in cooperation with other competent departments of the credit institution, an annual plan of training and education of staff.

(xxiii) The AMLCO ensures that the credit institution maintains the following information in relation to the training seminars and other education provided to the staff of the credit institution on the prevention of money laundering and terrorist financing and assesses the adequacy of the training and education provided. The following information shall be kept, as a minimum:

(a) Employee name by service/department and by position (managerial staff, officers, newcomers, etc.). The list should include all the staff of the institution even though they did not attend any seminar.

(b) Date of attendance of the seminar, title and duration of the seminar and the names of the trainers.

(c) Whether the lecture/seminar was prepared within the credit institution or offered by an external organisation or consultants.

(d) Summary information for the programme/content of the lectures/seminars

(xxiv) The AMLCO verifies that the third party with whom the credit institution intends to cooperate on identification issues is an obliged entity as set out in the Law and gives his/her written consent for the cooperation which should be duly justified and kept in the personal file of the third party. Also the AMLCO evaluates the quality of the customers recommended by third parties.

(xxv) The AMLCO maintains records with the data/information of the third parties with whom the credit institution has concluded a cooperation as referred to in paragraph 121(vi).

(xxvi) The AMLCO maintains records, for five years, with the data/information referred to in paragraph 121(vii) for third parties rejected for the conclusion of cooperation.

(xxvii) The AMLCO establishes policies, procedures and controls as referred to in article 64(1)(b) of the Law as well as in this Directive (see part 4.14.2.5) in cases of cross-border correspondence with institutions from third countries.

(xxviii) The AMLCO ensures that the credit institution prepares and maintains lists with the customer categories according to the calculated risk, (as defined in the Law, this Directive and the credit institution itself) which refer the customers names, account number, the branch that keeps the account and the date of the commencement of the business relationship. Additionally, the AMLCO ensures that these lists are regularly updated with all new and old customers for whom additional information is available.

(xxix) The AMLCO shall take or suggest, where appropriate, corrective measures, in matters of prevention of money laundering and terrorist financing in accordance with the findings of the audit conclusions of the Central Bank of Cyprus.

(xxx) The AMLCO evaluates the findings of the Internal Audit to take corrective action for issues of prevention of money laundering and terrorist financing.

(xxxi) The AMLCO takes or recommends, where appropriate, measures to prevent money laundering and terrorist financing taking into account the National and Supranational Risk Assessment reports.

(xxxii) The AMLCO ensures that the credit institution takes into account the public statements of the Financial Action Task Force ("FATF") in respect of countries which do not implement or apply inadequately the FATF recommendations, and ensures that enhanced due diligence measures and monitoring of business relations/transactions are applied. Additionally, he/she ensures that enhanced due diligence measures are applied to high-risk third countries identified by the European Commission and by the credit institution itself.

2.3 AMLCO Annual Report

25. The AMLCO has also the task of preparing an Annual Report which constitutes an important tool for assessing the degree of compliance of the credit institution with the obligations imposed by the Law and the Directive of the Central Bank of Cyprus for the prevention of money laundering and terrorist financing.

26. The Annual Report should be prepared within two months after the end of each calendar year (i.e. by the end of February, at the latest) and submitted to the Board of Directors of the credit institution through the Senior Management. In the case of a credit institution operating in Cyprus in the form of a branch, the Annual Report should be submitted to the Manager of the branch, the Board of Directors of the credit institution through the Senior Management and the Group AMLCO at the headquarters of their country of origin.

27. The Board of Directors evaluates and adopts the Annual Report. The Senior Management of the credit institution ensures the prompt and effective application of all appropriate measures to correct any shortcomings and/or omissions identified in the Report.

28. A copy of the Annual Report submitted to the Board of Directors is simultaneously forwarded to the Central Bank of Cyprus. Copies of the minutes of approval of the Board of Directors must be submitted to the Central Bank of Cyprus immediately after approval.

29. The Annual Report will cover issues of prevention of money laundering and terrorist financing during the year under review and, as a minimum, should contain the following:

    (i) General description of the business operations/model of the credit institution during the last year, mentioning the products/services offered, countries where it operates, possible changes to the operations and/or structure or the introduction of new products, services, technological developments that affected the procedures and controls for money laundering.

    (ii) Information on the measures taken and/or procedures introduced to comply with any amendments and/or new provisions of the Law and the Central Bank of Cyprus' Directives during the year under review.

    (iii) Information on the audits and inspections carried out by the AMLCO and Internal Audit stating the number of audits carried out, at which departments/lines of business and the significant deficiencies and weaknesses identified in the policy and procedures applied by the credit institution to prevent money laundering and terrorist financing. In this respect, the seriousness of the omissions or weaknesses, the risks involved and the actions and/or suggestions made for corrective measures to improve the situation should be highlighted.

    (iv) Information on audits carried out by the Central Bank of Cyprus, indicating any deficiencies and weaknesses identified, the risks involved as well as the corrective measures and actions taken or undertaken to improve the situation.

    (v) Information on the procedures and the automated/electronic information systems applied by the credit institution for the ongoing monitoring of the accounts and transactions of their customers by describing their main functions, the time of their operation (e.g. in real time or after the completion of the transaction), the weaknesses that occurred, and the results of their operation during the year under review, such as the total number of alerts generated by the system, number of internal reports submitted to MOKAS as a consequence of these alerts, number of false-positives alerts, increases/decreases in comparison with the previous year, any identified trends etc.

(vi) The number of internal suspicion reports of money laundering and terrorist financing submitted by the credit institution's staff to the AMLCO, citing summary data by region, address and branch as well as any comments and observations.

(vii) The number of suspicion reports submitted by the AMLCO to MOKAS and summary data/information of the main reasons for the suspicions and any trends observed.

(viii) The number of suspected transaction cases investigated by the AMLCO, but no suspicion report has been submitted to MOKAS.

(ix) Information regarding circulars and other communication with staff on issues for the prevention of money laundering and terrorist financing.

(x) Summary data on an annual basis of the customers total cash deposits and withdrawals, both in euro and foreign currencies in excess of 10,000 euro as well as incoming and outgoing fund transfers for amounts in excess of 500,000 euro (together with comparative data for the previous year) as reported in the "Monthly Statement of Large Cash Transactions and Funds Transfers" submitted monthly to the Central Bank of Cyprus and any comments and observations on significant variations observed in relation to the previous year.

(xi) Summary data, on an annual basis, of the customers' total deposits and loans on the basis of the permanent residence of the beneficial owner of the account, analysing any trends that may increase the risk for money laundering and terrorist financing.

(xii) Summary data for the type (natural or legal persons) and size of the customer base during the last year, the number of customers per risk category, the number of new customers, the number of persons (prospective customers) with whom the establishment of business relationship was not allowed for compliance reasons, the number of customers with whom the business relationship was terminated for compliance reasons, the number of frozen accounts following a court order/MOKAS and the increase/decrease percentage of the above compared to the previous year.

(xiii) Information on the policy, procedures and controls applied by the credit institution in relation to high risk customers with whom a business relationship is maintained. Additionally, the number of high risk customers with whom the credit institution has a business relationship, per category and country of **origin** of the customer and the beneficial owner should be submitted.

(xiv) Data for branches/subsidiaries of the credit institution that operate in third countries and also the information on the measures taken for the compliance of branches/subsidiaries of the credit institution with the provisions of this Directive in relation to customer

identification, due diligence measures and record keeping procedures, as well as comments and information on the level of their compliance with these requirements.

(xv) Information on the training seminars attended by the AMLCO, the Alternate AMLCO and the Assistant AMLCOs and on any other educational material received.

(xvi) Information on training/education provided to staff during the year, reporting:

- The number of courses/ seminars organized,
- their duration,
- the number of staff attending, specifying their seniority i.e. management staff, officers, clerical staff or newcomers etc,
- name(s) and qualifications of the instructor(s),
- whether the courses/seminar was developed internally by the credit institution or by an external organisation/consultant, and
- summary information for the program/content of the courses/seminars.

(xvii) Information for next year's training plan.

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

(xix) Information on the structure and staffing of the AMLCO's Unit 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.

(xx) Copy of the register with the data and information (e.g. name, business address, business area, supervisory authority, date of commencement of cooperation, review date and results of the assessment of customers recommended, number of customers that he/she introduces to the credit institution, number of customers that were reported to MOKAS) on third parties with whom the credit institution has established cooperation and also information for third parties that the AMLCO has rejected.

(xxi) Information on the policy, procedures and controls applied by the credit institution for its compliance with sanctions and restrictive measures, as well as summary data on frozen accounts (e.g. number of frozen accounts, reasons for freezing and total amount).

(xxii) An overall assessment of the effectiveness of the systems and controls, adequacy of resources and also areas likely to be equivalent to breaches of the legal and regulatory framework, describing in order of priority the actions for correction/prevention considered necessary and the expected deadline for completion.

3. RISK BASED APPROACH

3.1 Introduction

The Law Articles 58(A)(1)and (2)

30. For the purposes of article 58(d), article 58A(1) and (2) of the Law requires obliged entities to take appropriate measures to identify, and assess the risks of money laundering and financing of terrorist they are subject to, considering risk factors, including those related to their customers, countries or geographic regions, products, services, transactions or channels for the provision of banking services. These measures should be proportionate to the size and nature of their operations. The risk assessments are documented, updated and made available to the Central Bank of Cyprus through the report referred to in paragraph 3.6 of this chapter.

31. As required by the European Directive, the European Commission on 26 June 2017 published its first Supranational Risk Assessment report with the aim to help member states to identify, analyse and address the risks related to money laundering activities and terrorist financing. Credit institutions should take into account the findings of this Report, including its updates, to the extent that they may affect their own risk assessment.

32. The National Risk Assessment of Cyprus published in November 2018 provides information on the risks of money laundering and terrorist financing that Cyprus faces. Credit institutions should take into account the findings of this Report, including its updates, to the extent that they may affect their own risk assessment.

33. The approach of a credit institution in assessing and managing the risk of money laundering and terrorist financing should include risk assessment at the level of business activity and the risk assessment to which it is exposed as a result of the conclusion of a business relationship or of an occasional transaction. Therefore, the credit institution should use the results of the risk assessments carried out at the level of its business operations to substantiate its decision on the appropriate level and type of measures of customer due diligence to apply to the individual business relationships and the occasional transactions.

The Law Article 61(2)

34. Article 61(2) of the Law requires obliged entities to apply identification procedures and customer due diligence measures, but allows the extent of such measures to be determined according to the degree of risk, taking into account at least the variables listed in Appendix I to the Law. Obliged entities should be able to demonstrate to the competent Supervisory Authorities that the extent of the measures is commensurate with the risks of money laundering and terrorist financing that they face.

35. The implementation of a risk based system must strike a balance between the costs incurred by credit institutions and their customers with the risk of using their services in relation to money laundering and terrorist financing. Therefore, the implementation of risk-based measures and procedures enables credit institutions to focus their efforts in areas where there is a greater need to address money laundering and terrorist financing risks.

36. With the purpose of assisting the overall objective of preventing the abuse of the banking system for illegal activities the risk based approach should:

    - recognise that the money laundering or terrorist financing risk varies across customers, countries/territories, products and services;

    - allows the Board of Directors and Senior Management to differentiate between customers in a way that matches the risk of their particular business;

    - allows the Board of Directors and Senior Management to apply their own approach in the formulation of policies, procedures and controls taking into account the credit institution's particular circumstances;

    - helps produce a more cost-effective system;

    - assists in the correct prioritisation of efforts and actions of the credit institution considering the likelihood of money laundering or terrorist financing occurring;

37. The risk-based approach requires specific measures to be taken in order to manage the risks of money laundering and financing of terrorism confronting the credit institution. Such measures are:

    - the identification and evaluation of money laundering and terrorist financing risk depending on the size and nature of the credit institution's operations and the characteristics of its customers,

    - the management and reduction of the assessed risk by implementing appropriate and effective policies, procedures and controls, depending on the risk appetite,

    - continuous monitoring and implementation of measures to improve the functioning of policies, procedures and controls,

- dynamic risk management ensuring the availability of systems and controls to identify emerging risks of money laundering and terrorist financing, the assessment of these risks and, on a per case basis, their timely integration into both the institution's overall risk assessment and the individual risk assessments they carry out, and

- the recording in appropriate manuals, documents and internal circulars of the policies, procedures and controls in order to achieve their uniform application throughout the credit institution by competent persons appointed by the Board of Directors and the Senior Management.

3.2 Risk identification and assessment

38. The AMLCO is responsible for the identification, recording and assessment of all possible risks. However, the successful implementation of systems and controls on a risk based approach requires the full commitment of Senior Management and the active cooperation of the other units of the credit institution. It is also necessary to clearly communicate the agreed policies and procedures to all the competent staff of the credit institution together with the introduction of robust mechanisms for their effective implementation, the early identification of weaknesses and the implementation of corrective action.

39. A risk-based approach starts with the identification, recording and assessment of the risk that has to be managed. Credit institutions need to assess and evaluate the risk they are facing through the potential use of their services by criminals for the purpose of money laundering or terrorist financing. During the identification of the aforementioned risks associated with a business relationship or occasional transaction, credit institutions should examine the relevant risk factors, including the identity and occupation of their customer, the countries or the geographical areas in which the customer operates, the specific products and specific services and transactions requested by the customer, as well as the channels used by the credit institution for the provision of such products, services and transactions. The particular circumstances of each credit institution will determine the suitable procedures and measures that need to be applied to counter and manage risk. In the cases where the business, products and customer base of a credit institution are relatively simple, involving relatively few products and customers, or customers with similar characteristics, a simple, standard approach is more appropriate for most customers, with emphasis on those customers who fall outside the 'norm'.

40. Credit institutions shall form an overall picture of the risk associated with each case considering the risk factors referred to in the "Risk Factors Guidelines" published jointly by the European supervisory authorities in accordance with articles 17 and 18(4) of the European

Union Directive[4], while it is noted that, unless specified in the Law or the Directive of the Central Bank of Cyprus, the existence of individual risk factors does not necessarily imply the categorisation of a customer relationship at high or low risk. It should be noted that the risk factors included in these guidelines are not exhaustive and credit institutions are not expected to consider all risk factors for all cases.

41. The information about these risk factors for money laundering should originate from a wide range of sources in which access is obtained either individually or through commercially available tools or databases that gather information from various sources. Credit institutions should define the type and number of sources according to the degree of risk.

42. Credit Institutions should always consider the following sources of information:

    (i) The Supranational Risk Assessment of the European Commission,

    (ii) Information from the Government, such as the National Risk Assessment of Cyprus, the policy statements and warning indications, as well as the explanatory reports of the relevant legislation,

    (iii) The information from the Central Bank of Cyprus, such as circulars, guidelines and the justification derived from the imposition of regulatory fines,

    (iv) Information from MOKAS, the Police such as threat reports, warnings and typologies,

    (v) Information on the customer identification and the creation of the economic and risk profile of the customer at the beginning of the business relationship.

43. Other sources of information credit institutions may consider in this context are:

    (i) The knowledge and professional expertise of the credit institution,

    (ii) Typologies and information on emerging risks of the industry,

    (iii) Information from civil society, such as corruption indices and country reports,

[4] Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The Risk Factors Guidelines").
https://eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf

(iv) Information from international standard-setting bodies, such as mutual evaluation reports or legally non-binding "blacklists",

(v) Information from credible and reliable open sources such as reports in reputable newspapers,

(vi) Information from credible and reliable commercial organizations such as risk and intelligence reports, and

(vii) Information from statistical organisations and academia.

44. As part of this assessment, credit institutions may decide to weigh factors differently depending on their relative importance.

45. When weighting risk factors, credit institutions should make an informed judgement about the relevance of different risk factors in the context of a business relationship or occasional transaction. This often results in credit institutions allocating different 'scores' to different factors; for example, credit institutions may decide that a customer's personal links to a country associated with higher money laundering and terrorist financing risk is less relevant in light of the features of the product they seek.

46. The weight given to each of these factors is likely to vary from product to product and customer to customer (or categories of customers) and between credit institutions. When weighting risk factors, credit institutions should ensure that:

- weighting is not unduly influenced by just one factor
- the risk rating is not influenced by economic or profit considerations
- weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
- the provisions of the Law and the Directive regarding situations that always present a high money laundering risk cannot be over-ruled by the credit institutions weighting; and
- they are able to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores should be documented appropriately.

47. Where a credit institution uses automated IT systems to allocate overall risk scores to categorise business relationships or occasional transactions and does not develop these in

house but purchases them from an external provider, it should understand how the system works and how it combines risk factors to achieve an overall risk score. A credit institution must always ensure that the scores allocated reflect the credit institution's understanding of ML/TF risk and it should be able to demonstrate this to the Central Bank of Cyprus.

48. The identification, assessment and management of the risks stemming from the quality of data held by the credit institution should be adequately addressed, as insufficient data quality will lead to incorrect alert messages, management reports and decisions.

3.3 Design and implementation of controls for risk management and mitigation

49. When the credit institution identifies the risks it faces, it should design and implement the appropriate systems and controls to manage and mitigate them in accordance with the procedures provided for in this Directive. The proper management and mitigation of risks related to money laundering and terrorist financing requires measures and procedures for the identification of customers, collection of information for the building of their economic and risk profile as well as the monitoring of their transactions and activities.

50. In order to implement the most appropriate and effective policies, procedures and controls to prevent money laundering and terrorist financing, credit institutions should, considering the assessed risk, define the type and extent of the measures that need to be applied to manage and reduce the risks at the least possible cost. These measures may, indicatively, include:
    - Adaptation of the customer identification and customer due diligence measures according to the estimated risk for money laundering and terrorist financing from each particular business relationship.
    - Application of minimum standards for the quality and extent of the required identity data for each category of customers (documents from independent and reliable sources, information from third parties, evidence, etc.).
    - Requirement to obtain additional data and information from customers, whenever this is deemed necessary, for the proper and comprehensive understanding of the activities and sources of their assets so as to effectively address any increased risks arising from the specific business relationship, and
    - Monitoring on a continuous basis of customers ' transactions, activities and relationships based on the assessed risk.

51. Risk assessment and the implementation of measures mentioned above should lead to the categorisation of customers and occasional transactions according to the assessed level of money laundering and terrorist financing risk.

52. These categories will be based on criteria that reflect the possible causes of risk and each category will be accompanied by corresponding diligence measures, periodic monitoring and controls. Credit institutions should decide which is the most appropriate way of classifying risk. This decision depends on the nature and size of the institution's activity and on the types of risk of money laundering and terrorist financing to which it is exposed. Although credit institutions often categorize the risk as high, medium and low, it is possible to classify it in other categories.

53. The decision on the due diligence measures to be applied should be based on the "Risk Factors Guidelines".

The Law Article 63(1)

54. The Law allows obliged entities to apply simplified customer due diligence measures, provided that they are previously satisfied that the business relationship or transaction has a low risk level.

    It is understood that the obliged entity monitors the transaction and the business relationship sufficiently to enable the identification of unusual or suspicious transactions.

The Law Article 63(2)

55. Therefore, where there is evidence of an attempt to launder money or terrorist financing or where the credit institution has doubts as to the accuracy of the information it receives, it should not simplified due diligence measures. Additionally, simplified due diligence measures should not be applied in cases where there is obligation to implement enhanced due diligence measures.

56. In assessing the risks of money laundering and terrorist financing, relating to categories of customers, geographical areas and specific products, services, transactions or channels through which the services are provided, the obliged entity should take into account at least the factors listed in Appendix II of the Law, which relate to situations of potentially lower risk.

The Law Article 64(3)

57. The high risk customer category should include business relationships defined as high risk under articles 64(1)(a), (b) and (c) of the Law and section 4.14 of this Directive and any other business relationship that the credit institution itself has decided to classify as such. Related is Article 64(3) of the Law that requires that enhanced customer due diligence measures, depending on the degree of risk, should be taken also in other cases than those referred to in both the Law and this Directive which by their nature present a high risk for money laundering or terrorist financing.

The Law Article 64(4)

58. Article 64(4) of the Law requires that credit institutions examine, as far as reasonably practicable, the background and purpose of all complex and unusually large transactions and all unusual types of transactions that occur without apparent economic or legal purpose and in particular, the obliged entity intensifies the extent and nature of the monitoring of the business relationship in order to determine whether these transactions or activities appear suspicious.

59. As a consequence of this, the credit institutions are obliged, under the responsibility of the AMLCO, to be able to generate customer reports at any time, indicating the customer risk category and including the names of the customers and the ultimate beneficial owners, account number, the branch in which the account is held, date of commencement of the business relationship, date of last update and classification of high risk customers.

60. It is reiterated that the credit institution must be able to demonstrate to the Central Bank of Cyprus that the extent of the implemented systems and control procedures is commensurate with the risks it faces from possible money laundering and terrorist financing activities by customers/users of the services and products it offers.

3.4 Monitoring and improving the operation of the internal procedures

61. Credit institutions should assess, on a regular basis, the effective functioning of internal policies, procedures and controls. In this context, credit institutions should apply:

- Appropriate procedures for the timely detection of changes in the economic and risk profile of their customers.
- Procedures for the examination and control of new products, services of new business practices, including new channels for the provision of services and the use of new or developing technologies for new or existing products and any methods used by criminals for money laundering or terrorist financing.
- Procedures for assessing the adequacy of the provided training and staff education.
- Methods for controlling and evaluating the degree of compliance (e.g. Compliance Unit, Internal Audit).
- Appropriate automated systems and non-automated controls.
- Appropriate management information systems.

- Submission of reports by competent officers to the Board of Directors and the Senior Management.

- Effective communication methods with the Central Bank of Cyprus and MOKAS.

3.5 Dynamic Risk Management

62. Risk management is an ongoing process that is conducted on a dynamic basis. Risk assessment is not an isolated event of limited duration. The systems and controls should be regularly revised so as to achieve the continuous and effective tackling of risks arising from changes in the characteristics of existing customers, new customers, products and services and geographical dispersion.

63. The activities of the customers change (without the credit institution always knowing) as well as the products and services offered by the credit institution. The same is true for the products and transactions used by criminals who legitimise proceeds from illegal activities or finance terrorist acts. Hence, credit institutions should evaluate the information they receive in the context of the ongoing monitoring of a business relationship and examine whether this affects the risk assessment.

64. Credit institutions should also ensure that they have systems and controls to identify emerging risks of money laundering and terrorist financing and that they are able to assess the risks and, where appropriate, incorporate them in a timely manner both in the institution overall risk assessment and in the individual risk assessments they carry out.

65. Examples of systems and controls that credit institutions should have to identify emerging risks include, inter alia, the following:

    (i) Procedures to ensure the regular review of internal information for the purpose of identifying trends and emerging issues, both in the individual business relations and in the business activity of the credit institution.

    (ii) Procedures to ensure the regular review of relevant sources of information, such as the sources of information specified in paragraphs 42 to 43 of this Directive. These procedures should include, in particular, the following elements:

        a. regular review of media reports relating to the sectors or jurisdictions where the credit institution operates,

        b. regular review of the warnings and reports of law enforcement agencies,

c. ensuring that the credit institution is aware of the changes in the warnings of terrorist act and the sanctioning regimes at the time of such changes, e.g. by reviewing regularly the warnings of terrorist act and seeking updates to the sanctioning systems, and

d. regular review of thematic overviews and similar publications issued by the competent authorities.

(iii) Procedures for the collection and review of information in relation to the risks associated with new products.

(iv) Cooperation with other representatives of the sector and with the competent authorities (e.g. round table discussions, conferences and training providers) and procedures for the information of the competent staff on any findings.

(v) Developing a culture of information exchange within the credit institution and strong corporate ethics.

66. Examples of systems and controls that credit institutions should have to ensure that they keep up-to-date both the institution overall risk assessment and the individual risk assessments, include among other things:

(i) Setting a date for the next update of the risk assessment to ensure that risk assessments include new or emerging risks. In case that the institution is aware that a new risk has arisen or that there has been an increase in an existing risk, this should be reflected in the risk assessments as soon as possible.

(ii) Careful recording, throughout the year, of issues that could have an impact on risk assessments, such as internal suspicious transaction reports, cases of non-compliance and information from customer service personnel.

67. As the initial risk assessments, each update of risk assessment and adjustment of accompanying due diligence measures should be proportionate and equivalent to the risk of money laundering and terrorist financing.

3.6 Risk Management Report

68. Credit institutions should record and document their identification and risk assessment in relation to business relationships and occasional transactions and any change in the relevant risk assessments in the context of their review and monitoring to ensure that they are able to demonstrate to the Central Bank of Cyprus the adequacy of these risk assessments and related

risk management measures. Therefore, the detailed recording of the measures taken by the credit institution will help it to demonstrate:

- the ways they have used to identify and assess the risks of using their services for money laundering and terrorist financing;
- how they concluded to the introduction and implementation of the specific policies, procedures and controls for the management and mitigation of risks;
- the methods of monitoring and improvement where this is deemed necessary, of the specific policies, procedures and controls, and
- the setup for reporting to senior managers on the functioning of the control procedures.

69. The risk documentation and assessment report must be kept fully updated. It is therefore necessary to re-evaluate the risks, on an annual basis even where credit institutions consider that there is no need for revising the relevant assessment report. This report should be submitted on an annual basis through Senior Management to the Board of Directors of the credit institution for approval in order to recognise the residual risks that reflect the risk appetite of the credit institution. A copy of the approved report together with the minutes of the Board of Directors, where the views, the risk acceptance statement and the approval of the Board of Directors are recorded, should be submitted to the Central Bank of Cyprus with the Annual Report of the AMLCO.

4. CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES

4.1. Introduction

70. The risk assessment carried out by a credit institution should allow the determination of the actions to be taken in relation to risk management in the context of the prevention of money laundering activities and terrorism financing, both in accepting a new customer and throughout the duration of the business relationship.

71. Collecting and maintaining sufficient information about a customer, making use of that information for the purposes of customer identification, the establishment of the economic profile and the assessment of his/her risk profile forms the basis of all other procedures for the prevention of money laundering and terrorist financing. Further to minimising the risk of a credit institution's services being used for illicit activities, the possession of sufficient customer's identity information and also the creation of the economic profile of the customers enables the detection and recognition of suspicious transactions/activities and protects the credit institutions from possible fraud and the underlying risks to their financial robustness and reputation.

4.2. When to apply customer identification and due diligence procedures

The Law Articles 58 and 60

72. Articles 58 and 60 of the Law require obliged entities to apply adequate and appropriate policies, controls and procedures, according to their nature and size, in order to mitigate and effectively manage the risks related to money laundering and terrorist financing, in relation to the identification and exercise of customer due diligence, when, inter alia:

(i) establishing business relationships,

(ii) executing an occasional transaction that:

(a) amounts fifteen thousand euro (€15.000) or more, irrespective of whether the transaction is carried out in a single operation or in several transactions which appear to be linked, or

(b) is a transfer of funds as defined in paragraph (9) of article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council for an amount exceeding a thousand euro (€1.000),

(iii) there is suspicion of money laundering or terrorist financing, regardless of the amount of the transaction and irrespective of any derogation, exemption or threshold under the Law,

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

The Law Article 2

73. Article 2 of the Law gives the following relevant interpretations to the above:

- "business relationship" means the business, professional or commercial relationship between the customer and the obliged entity, which is connected to the professional activities of an obliged entity and is expected by the obliged entity at the time of the establishment of the contact, to have an element of duration.
- "Occasional transaction" means any transaction other than a transaction that takes place during a business relationship.
- "Customer" means a person who aims to enter into a business relationship, or carry out an occasional transaction, with an obliged entity in or from the Republic.

4.3. Identification and due diligence procedures

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

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

(ii) the identification of the beneficial owner's identity and taking reasonable measures to verify his/her identity in order to ensure that the obliged entity knows the beneficial owner in respect of legal persons, trusts, companies, institutions and similar legal arrangements, taking reasonable measures to understand the structure of ownership and control of the customer,

(iii) the evaluation and, where appropriate, the collection of information on the purpose and the intended nature of the business relationship,

(iv) The exercise of ongoing monitoring of the business relationship, with thorough examination of the transactions carried out during this relationship, in order to ensure that the transactions carried out are consistent with the obliged entity's knowledge of the customer, the business and the risk profile, including where necessary the source of funds, and ensuring that the documents, data or information held are kept up-to-date and the assurance of maintaining updated documents, data or information.

It is understood that in applying the measures in paragraphs (i), and (ii) above, obliged entities shall verify that any person who intends to act on behalf of the customer is duly authorised by the customer for that purpose, and identify and verify the identity of that person.

The Law Article 61(3)

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

(i). It is reasonably possible to ascertain that the customer is the person he/she claims to be, and

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

The Law Article 2

76. According to Article 2 of the Law, "beneficial owner" means the natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is carried out and includes at least:

(a) as regards a legal person:

(i) the natural person(s) who ultimately owns or controls the legal person, through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that legal person, inter alia, through bearer shares or through control by other means, other than a listed company on a regulated market, which is subject to disclosure requirements under European Union Law or subject to equivalent international standards which ensure sufficient transparency of information on the beneficial owner:

It is provided that:

(a) indication of direct ownership constitutes a holding of twenty five per cent (25%) plus one (1) share or an ownership interest of more than twenty five percent (25%) in the customer owned by a natural person, and

(b) indication of indirect ownership constitutes a holding of twenty-five per cent (25%) plus one (1) share or ownership interest of more than twenty five percent (25%) in a customer held by a legal person who is under the control of a natural person(s) or by several legal persons who are under the control of the same natural person(s):

It is further provided that control by other means can be ascertained inter alia on the basis of the criteria provided for in paragraph (b) of section (1) of article 142 and in article 148 of the Companies Law.

(ii) the natural person(s) holding a position of a senior management official(s) in the event that, after all possible means have been exhausted and with the condition that there are no

grounds for suspicion, no person is identified under the provisions of subparagraph (i) of this paragraph or if there is doubt that the person identified is the beneficial owner:

It is provided that an obliged entity maintains records of actions taken in accordance with the provisions of subparagraphs (i) and (ii).

(b) regarding trusts:

(i) the settlor,

(ii) the trustee,

(iii) the protector, if there is,

(iv) the beneficiary or, where the individuals benefiting from the legal arrangement or the legal entity have not yet been identified, the category of persons in whose interest the legal arrangement or legal entity has been established or operates,

(v) any other natural person exercising ultimate control of the trust through direct or indirect ownership or by other means; and

(c) as regards legal entities, such as institutions, and legal arrangements similar to trusts, it includes the natural person(s) holding an equivalent or similar position with a person referred to in paragraph (b) above.

77. The ways in which a credit institution complies with the requirements for the implementation of customer due diligence measures and the extent of the measures taken should reflect the risk assessment carried out by the credit institution and the assessment of the level of risk in each particular case.

4.4. Timing of customer identification

The Law Article 62(1)

78. Article 62(1) of the Law requires that the identification of the customer and the beneficial owner is performed prior to the establishment of the business relationship or the execution of a transaction.

The Law Article 62(2)

79. Nevertheless, article 62(2) allows, by way of derogation from the provisions of the previous paragraph, the completion of the verification of the identity of the customer and of the beneficial owner in the course of the establishment of the business relationships, if this is

required in order not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. In such cases, the procedures for verifying the identity of the customer should be completed as soon as practicable after the initial contact.

The Law Article 62(3)

80. Article 62(3) allows, by derogation from article 62(1) of the Law, the opening of an account with a credit institution or a financial organisation, including accounts allowing transactions in securities, provided that it is ensured that transactions will not be executed by the customer or on his/her behalf, before ensuring full compliance with customer due diligence requirements as provided in paragraphs (a) and (b) of section 1 of article 61 of the Law.

The Law Article 62(4)

81. Article 62(4) clearly requires that in cases where an obliged entity cannot comply with customer due diligence requirements as defined in article 61(1)(a), (b) or (c), it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction and shall terminate the business relationship and examines the possibility of submitting a report for a suspicious transaction, in relation to the customer, to MOKAS, in accordance with the provisions of Article 69 of the Law.

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

The Law Articles 60(d) και 62(6)

82. Article 60(d) of the Law requires obliged entities to apply the customer identification procedures and due diligence measures when there are doubts about the accuracy or adequacy of the documents, data or information previously collected for the identification of an existing customer. Furthermore, article 62(6) of the Law requires the application of customer identification procedures and due diligence measures not only to new customers but also to existing customers, at the appropriate time, on a risk-sensitive basis, including among other, when the relevant circumstances of the customer change.

83. Credit institutions must ensure that the customer identification records they hold for their customers as well as the information that form their economic and risk profiles remain completely updated throughout the business relationship. In this respect, credit institutions must examine and check on a regular basis the validity and adequacy of the customer identification data they maintain, and also other data or information in relation to the customer, the business relationship, the economic profile and the risk profile of the customer. The policy and the procedures for the prevention of money laundering and terrorist financing should determine the timeframe during which the regular review, examination and update of the customers identification data and other data and information 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 archived in the respective customer file.

84. Irrespective of the above and considering the level of risk, if at any time during the business relationship is perceived that reliable or sufficient data and information from the identity and economic profile of an existing customer is missing, then the credit institution must take all necessary actions by applying the identification procedures and due diligence measures provided for in this Directive in order to collect the missing data and information the soonest possible so as to create the complete customer's economic and risk profile.

85. In addition to the requirement for the update of the customer identification data on a regular basis or when it is observed that they do not maintain reliable or adequate data and information, credit institutions should check the adequacy of customers identification and economic profile data and information held, whenever one of the following events or incidents occurs:

    1) A transaction which appears to be unusual and/or significant compared to the normal pattern of transactions, the business activity and the economic profile of the customer.

    2) Significant change in the situation and/or legal status of the customer 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 settlor(s), trustee(s), protector(s), beneficiary(ies);

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

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

    3) Significant change in the way and rules of the operation of the account, such as:

        - Change in the persons that are authorised to operate the accounts,

        - application for the opening of new accounts or the provision of new banking services and/or products,

        - activation of a dormant account.

    4) Change of the risk level of the customer (e.g. customer from lower to higher risk).

5) Change in the customer's business activities.

6) Detection of negative information about the customer in the press or the internet or commercial information databases or information submitted by a competent supervisory authority or MOKAS or other credit institution or following an investigation which indicate the need for the update of the customer and/or possible change to the risk profile of the customer.

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

4.6. Simplified identification and due diligence procedures

The Law Article 63(1)

87. Article 63(1) of the Law states that obliged entities may apply simplified customer due diligence measures, if they have ascertained, in advance, that the business relationship or transaction presents a low degree of risk. It is provided that the obliged entity monitors the transaction and the business relationship sufficiently to enable the identification of unusual or suspicious transactions.

The Law Article 63(2)

88. Article 63(2) of the Law states that, in order to enable the credit institution to apply simplified due diligence measures the assessment of the risks of money laundering and terrorist financing, which relate to customer categories, geographic areas, specific products, services, transactions or delivery channels should consider at least the factors relating to situations of potentially lower risk as they are listed in Appendix II of the Law.

89. The application of simplified due diligence measures does not imply an exception to any due diligence measure, however credit institutions may adjust the extent, time or type of each or all due diligence measures in a manner to be proportionate to the low risk they have identified. At the same time, credit institutions should apply adequate procedures for monitoring transactions and the business relationship so as to identify suspicious or unusual transactions in a timely manner.

90. The simplified due diligence measures that credit institutions may apply include, indicatively, the following:

(i) Adjustment of the timing of customer due diligence, e.g. where the product or transaction being pursued has features that restrict its use for money laundering or terrorist financing purposes, for example through:

a) the verification of the identity of the customer or the beneficial owner during the establishment of the business relationship, or

b) the verification of the identity of the customer or the beneficial owner once transactions exceed a defined threshold or once a reasonable time limit has elapsed. Credit institutions should ensure that:

(1) this does not in fact mean an exception to the application of due diligence measures, i.e. credit institutions must eventually ensure the verification of the identity of the customer or the beneficial owner,

(2) the threshold or time limit is set at a reasonably low level,

(3) they have systems in place to detect when the threshold or time limit has been reached, and

(4) they do not postpone the application of due diligence measures or delay the collection of relevant information about the customer, in a way that the provisions of the Law or European Regulations (e.g. EC 2015/847) are violated.

(ii) Adjustment of the quantity of information received for the purposes of identification, verification or monitoring, for example through:

(a) the verification of identity on the basis of information obtained from one reliable, credible and independent document or data source only; or

(b) the acceptance of the nature and purpose of the business relationship because the product is designed solely for a specific use, such as a company's pension scheme or a shopping centre gift card.

(iii) Adjustment of the quality or source of information obtained for the purposes of identification, verification or monitoring, for example through:

(a) the acceptance of information received from the customer and not from an independent source when verifying the identity of the beneficial owner (note that this is not permitted in the context of the verification of the identity of the customer); or

(b) if the risk associated with all aspects of the relationship is very low, relying on the source of the funds to fulfil some of the requirements for the implementation of due diligence measures, e.g. when the funds constitute payments of state benefits or when the funds have been transferred from a credit or financial institution established within the European Economic Area from an account in the name of the customer.

(iv) Adjustment of the frequency of the customer due diligence update and review of the business relationship with regard to the implementation of due diligence measures e.g. an update and review only in case of activation events, such as when the customer seeks the provision of a new product or new service or when a certain transaction threshold has been reached; credit institutions must ensure that this does not in fact imply an exception from keeping customer due diligence information up-to-date.

(v) Adjustment of the frequency and intensity of transaction monitoring, e.g. by monitoring transactions that exceed a specified threshold only. Where credit institutions choose this measure, they must ensure that the threshold is set at a reasonable level and that they have systems to identify linked transactions which, in combination, exceed that threshold. It is stressed that even if customer transactions involve small amounts, the credit institution should check the origin and destination of the transactions as terrorist financing is usually associated with small amounts.

91. It should be noted that in Title III of the "Guidelines for the Risk Factors" jointly issued by the European Supervisory Authorities, additional simplified due diligence measures, which may have particular importance in different sectors, are mentioned. It is provided that from those are excepted those cases where this Directive explicitly determines the due diligence measures to be applied (e.g. "Client accounts" in the name of a third person).

The Law Article 61(6)

92. In accordance with article 61(6)(a) of the Law and in accordance with the provisions of article 61(6)(b), by derogation from the provisions of articles 61(1)(a)(b) and (c) and article 62 and on the basis of an appropriate risk assessment indicating that the risk of money laundering and terrorist financing is small, obliged entity may refrain from applying certain customer due diligence measures in respect to electronic money, if all the following conditions for mitigating the risk are fulfilled:

(i) the payment instrument is not reloadable or has a maximum monthly payment transaction limit of two hundred and fifty euro (€250) which can be used for payment transactions only within the Republic,

(ii) the maximum amount stored electronically should not exceed two hundred and fifty euros (€250),

(iii) the payment instrument is used exclusively for the purchase of goods or services,

(iv) the payment instrument cannot be funded by anonymous electronic money,

(v) the issuer has appropriate and adequate systems and procedures to monitor the transactions or business relationships so that unusual or suspicious transactions can be detected.

The provisions of article 61(6)(a) of the Law do not apply in the case of redemption in cash or cash withdrawal of the monetary value of the electronic money where the amount redeemed exceeds one hundred euro (€100).

The exception from the application of certain customer due diligence measures referred to in article 616(a) of the Law does not include the obligation to monitor the transactions and the business relationship on an ongoing basis and identify and report suspicious transactions.

93. The information received by a credit institution at the application of simplified due diligence measures should enable it to reasonably attest that its assessment of the low risk associated with the business relationship is justified. It should also be sufficient to provide it with enough information on the nature of the business relationship in order to be in a position to detect any unusual or suspicious transactions. The application of simplified due diligence measures does not exempt an institution from reporting suspicious transactions to MOKAS.

94. In case there are indications that the risk may not be low or if there are suspicions of attempted money laundering or terrorist financing or where the credit institution has doubts as to the veracity of the information received, simplified due diligence measures should not be applied. Also, simplified measures should not be applied where it is possible that specific high-risk scenarios may apply and an obligation to implement enhanced due diligence measures is provided.

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

The Law Article 66(2)

95. Article 66(2) of the Law prohibits obliged entities to open or maintain anonymous or numbered accounts or accounts in names other than those stated in official identification documents.

4.8. Transactions and products that favour anonymity

The Law Article 66(3)

96. Article 66(3) requires from obliged entities to pay particular attention to every threat or risk of money laundering or terrorist financing that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for such actions and apply as far as possible reasonable measures and procedures to counter risks arising from technological developments and new financial products.

4.9. Prohibition of correspondent relationships with "shell banks"

The Law Articles 66(1)(a) και (b)

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

The Law Article 2

98. According to article (2) of the Law, "shell bank" means a credit or financial institution or an institution that carries out activities equivalent to those carried out by credit and financial institutions, 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.

99. Additionally, corresponding relationship means:

The Law Article 2

(a) the provision of banking services by a bank (correspondent) to another bank (respondent) including the provision of a current or other liability account and related services and includes the management of cash reserves, international transfers of funds, cheque clearing, payable-through accounts and foreign exchange services, and

(b) the relationships between and among credit institutions and financial institutions, including where similar services are provided by an institution-correspondent to an institution-client, and including relationships established for securities transactions or transfers of funds.

4.10. Failure or refusal to provide identification evidence

The Law Article 62(4)

100. According to article 62(4) of the Law, where an obliged entity cannot comply with the customer due diligence requirements, as specified in paragraphs (a), (b) and (c) of section (1) of article 61, it shall not carry out a transaction through a bank account, does not enter into a business relationship or does not carry out the transaction, where applicable, terminates this business relationship and examines the possibility of reporting a suspected transaction in relation to the customer to MOKAS, in accordance with the provisions of article 69.

4.11. Economic profile construction

The Law Article 61(1)

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

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

(ii) the verification of the identity of the beneficial owner and taking reasonable measures to verify his/her identity, so as to ensure that the obliged entity knows the beneficial owner, in respect of legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable steps to understand the structure of ownership and control of the customer, and

(iii) the evaluation and, where appropriate, the collection of information for the purpose and the intended nature of the business relationship.

102. Credit institutions should be satisfied that they are dealing with a real person (natural or legal) and for this purpose they should obtain sufficient evidence of identity to establish that a prospective customer is who he/she claims to be. The identity of all customers should be identified and verified on the basis of reliable data, documents and information issued or obtained from independent reliable sources, i.e. those data, documents and information that are difficult to forge or obtain illicitly. Certified true copies of the identification evidence should always be retained by the credit institutions and archived in the customers' files. However, it must be stressed that no single form of customer identification can fully guarantee the correctness of the identity of a person, hence an ongoing procedure for the verification of the identity of customers should be in place.

103. It is noted that as an additional measure of verification of the identity of the customer and the beneficial owner, credit institutions may also use the information stored in the records referred to in article 61A of the Law. It is noted that an obliged entity is not allowed to rely solely on the information stored in the central register of beneficial owners defined in the Law for the fulfilment of the requirements of the due diligence measures and identification of the customer's identity.

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

105. Credit institutions should also verify and validate the identity of the actual/beneficial owners of the accounts and occasional transactions and, for legal persons, they should obtain adequate information, data and documents issued by independent and reliable sources so as to understand the ownership and control structure of the customer's assets. Irrespective of the customer's type (natural or legal person, sole trader or partnership) credit institutions should request and obtain sufficient data and information on the customer's business activities and the expected type and level of transactions. The credit institution should perceive the purpose and the intended nature of the business relationship and the expected operation of the account concerned, so that it can assess whether the proposed relationship is in accordance with the risk appetite and provide it with an essential basis for continuous monitoring. The data and information should be collected before the establishment of the business relationship and the execution of any transactions, with the aim of constructing the customer's economic profile, which, as a minimum, should include the following :

    (i) the purpose and the reason for opening the account or the provision of banking services,

    (ii) the anticipated account turnover,

    (iii) the nature of the transactions,

    (iv) the expected origin (e.g. countries and names of principal counterparties) of funds to be credited to the account and the expected destination (e.g. countries and names of principal counterparties) of outgoing transfers/payments,

    (v) the source and size of the customer's wealth and annual income,

(vi) the clear and detailed description of the main business/ professional activities/operations.

106. The above mentioned information as well as all data and information that form the customer's 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, directors, authorised signatories, financial information, ownership structure, information on the group that the company may be a part of (country of incorporation of the parent company, subsidiary companies and affiliated companies, main activities and financial information) should be recorded in a separate form designed for this purpose and should be archived in the customer's file along with all other documents and account opening information as well as with internal memos of minutes of meetings with the customers. It is understood that an identical form should also be used for recording similar information that make up the economic profile of a customer who is a natural person which, should also be archived in the respective customer's (natural person) file. The relevant form should be updated regularly or whenever new information exists about changes or additions to the data that comprise the economic profile of the customer.

107. For better understanding of the activities of their customers (including companies, partnerships, foundations, clubs, trusts and other legal entities, self-employed natural persons), as well as the source and use of their funds/assets, credit institutions shall obtain copies of recent audited financial statements. In cases where there is no obligation for the preparation of audited financial statements or where these are not available (at least for the previous two years) they shall obtain recent management accounts.

108. The structure, ownership and purpose and activities of the customer, in most cases, will be clear and comprehensible. However, customers may use complex or multilevel ownership structures, and it may be appropriate to take enhanced due diligence measures as regards identification. The use of complex or multilevel structures with no apparent legitimate commercial purpose may, however, raise concerns and increase the risk of money laundering or terrorist financing.

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

The Law Article 67(1)

109. Article 67(1) of the Law permits obliged entities to rely on third parties for the implementation of the procedures for customer identification and due diligence measures, as these are prescribed in article 61(1)(a),(b) and (c) of the Law.

110. Article 67(1) of the Law explicitly provides that the ultimate responsibility for performing the above mentioned measures and procedures remains with the obliged entity which relies on the third person and consequently, the responsibility to apply the procedures for customer identification and due diligence measures cannot be delegated to the third party.

The Law Article 67(2)

111. The Law considers as third parties the obliged entities specified in Article 2A(1)(a)(b)(c) and (d) of the Law or other similar institutions or persons located in the Member States or in a third country which:

(i) apply customer due diligence measures and record-keeping measures consistent with those laid down in the Directive of the European Union and

(ii) are subject to supervision consistent with the relevant requirements of the Directive of the European Union.

The Law Article 67(2)(b)

112. Credit institutions cannot rely on third parties established in high-risk third countries in accordance with article 67(2)(b) of the Law, unless the Central Bank of Cyprus has exempted from this prohibition branches and subsidiaries of majority participation of obliged entities established in the European Union, where such branches and subsidiaries fully comply with the policies and procedures applied at group level in accordance with article 68A of the Law.

The Law Article 67(2)(b)

113. It should be noted that the terms "financial institutions" and "obliged entities" do not include dealers in foreign exchange (Bureau de change).

The Law Article 67(3)

114. Article 67(3) of the Law provides that credit institutions should require from the third party to:

(i) submit, immediately, to them all available data, information and documents of identity collected during the application of the procedures for customer identification and due diligence measures in accordance with the requirements of the Law, and

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

The Law Article 67(4)

115. In the case of a group, the competent supervisory authority of the home Member State and the competent supervisory authority of the host Member State (for branches and subsidiaries) may consider that an obliged entity applies the measures referred to in Paragraphs 111-114 above, if the following are fulfilled:

(a) the obliged entity relies on information provided by a third party belonging to the same group.

(b) the said group applies customer due diligence measures, record-keeping rules and programmes to prevent money laundering and terrorist financing in accordance with the requirements of the European Union Directive or equivalent rules.

(c) the effective implementation of the measures referred to in the above paragraph shall be subject to supervision at group level by a competent supervisory authority of a home Member State or of a third country.

The Law Article 67(5)

116. Article 67(5) of the Law does not apply outsourcing or agency relationships under which, based on contractual arrangement, the provider of the external service or the agent is considered to be part of the obliged entity.

117. Credit institutions may rely on third parties only at the outset of establishing a business relationship for the purpose of ascertaining and verifying the identity of their customers. Any data and information for the purpose of updating the customer's business profile during the operation of the account, should be obtained directly from the natural person in the name of whom the account is maintained, or in the case of legal persons, from the natural persons who are the ultimate beneficial owner of the share capital of the legal persons or who exercise the ultimate control of the legal persons or who have the responsibility of decision making and who manage the operations of the customer. It is provided that the certification of documents may be performed by the third parties.

118. All copies of the identification documents, data and information obtained by a credit institution should be duly certified. Paragraphs 254-255 of this Directive as regards the certification of documents is relevant.

119. For customers with whom a business relationship was initiated following a recommendation by a third party, as defined in article 67 of the Law, and is engaged in the implementation of customer identification and due diligence measures, credit institutions are obliged to arrange a face-to-face meeting with the said customers in order

to verify the information and data which compose the customers' economic and risk profile, which have been obtained by the third party, and also to collect any other data and information deemed necessary to prove that the credit institution has acquired direct knowledge of such customers. In the case of legal persons, the meeting must be held with the natural person or persons who are the ultimate beneficial owners of the share capital of the legal persons or who exercise the ultimate control of the legal persons or have the responsibility of the decisions and the management of the operations of the customer. The said meeting should take place before executing any transaction. The meeting may be held over the internet on condition that adequate safeguards are in place such as sound/video recording of the meeting. Evidence for the meeting and its content should be readily available to the competent authorities.

120. Any meetings with the third party that recommended the customers to the credit institution or with persons directly or indirectly associated with the said third party or registered shareholders acting as nominees of the ultimate beneficial owner are not considered as compliance by the credit institution with the provisions of paragraphs 117-119.

121. The policy and the procedures should specify the measures taken by the credit institution so as to comply with the requirements of the Law and the Directive, including, as a minimum, the following:

(i) The AMLCO shall verify that the third party is an obliged entity as defined in paragraphs (a), (b), (c) and (d) of section (1) of Article 2A or another equivalent institution or person located in a Member State or a third country which;

a. Applies customer due diligence measures and record-keeping measures consistent with those laid down in the European Union Directive, and

b. is subject to supervision consistent with the relevant requirements of the European Union Directive.

(ii) The credit institution shall sign an agreement with the third party specifying the obligations of each party, including the financial conditions, the names and signatures of the persons designated by the third party, and who have the right to certify the documents.

(iii) For each third party mentioned above and before the business relationship commences, identification procedures and due diligence measures are applied.

(iv) The AMLCO evaluates the quality of the customers recommended by third parties. The evaluation must include at least the number of customers recommended by the third party, number of customers with whom the relationship was terminated for non-compliance reasons, number of internal suspicion reports and suspicion reports to MOKAS. If the quality is deemed unsatisfactory then the relationship with the third party is terminated.

(v) The AMLCO maintains a separate file in which the identity data is recorded, evidence ascertaining that the third party is subject to supervision under the Law and an assessment of the quality of the customers recommended by the third party. This information should be updated on an annual basis.

(vi) The AMLCO maintains a register with the following data/information on the third parties with which the credit institution has or had a business cooperation:

1. Name
2. Business address
3. Professional activities sector
4. Supervisory Authority
5. Commencement date of cooperation
6. Date of last evaluation
7. Date of next evaluation
8. Results of evaluation of customers recommended
9. Number of customers recommended to the credit institution in the last three years on an annual basis
10. Number of customers reported to MOKAS
11. Date and reason for the termination of the business cooperation, if applicable

(vii) The AMLCO maintains a register with the following data/information on the third parties with which a business cooperation was rejected:

1. Name
2. Business address
3. Professional activities sector
4. Supervisory Authority
5. Date of rejection
6. Reasons for rejection

(viii) The commencement of the cooperation with the third party and the acceptance of the verification of identity of customers by the third party must bear the written and duly justified approval of the AMLCO which is kept in the individual record file of the third party maintained by the credit institution.

4.13. Specific customer identification issues

4.13.1. Natural Persons

122. Credit institutions shall verify the identity of natural persons residing in Cyprus or abroad by obtaining the following information:

(i). real name and/or names used, on the basis of a valid official national identity card or passport,

(ii). complete permanent residence address, including postal code,

(iii). telephone number,

(iv). email address,

(v). date and place of birth,

(vi). details for business and other activities, including the employer/company's name, position,

(vii). signature specimen, and

(viii). any other information considered essential according to the assessed risk.

123. Customer identification must always be made on the basis of the official identity card or passport submitted by the beneficial owner of the account which must be valid.

124. Credit institutions after being satisfied with the original identity documents that have been presented to them, must keep copies of the pages containing the relevant information, which should be certified as true copies of the original (please refer to paragraphs 254-255 of this Directive).

125. Furthermore, where any doubt arises as to the identity of a person (passport, identity card) verification should be sought by the Ministry of Interior (competent issuing authority in the Republic) or the Embassy or Consulate of the country of issuance in Cyprus or by reputable financial institutions located in the customer's country of origin. It is understood that such official documents should bear a photograph of the customer.

126. Further to the verification of name, the customer's permanent residence address is verified by one of the following ways:

(i) visit to the place of residence (in such a case a relevant memo should be prepared and archived in the customer's file by the officer of the credit institution that made the visit),

(ii) the presentation of a recent (up to 6 months) utility bill (e.g. electricity, water), or housing insurance document, or municipal taxes and/or bank account statement.

The customer identification process is enhanced if that person has been referred by a trusted member of the credit institution's staff or by another existing trusted customer or a third party personally known to the credit institution's Management. Details of such references should be noted in the customer's personal file.

127. Credit institutions should request and receive information on public positions that the customer holds or has held during the last 12 months and whether he is a family member or close associate of such a person in order to ascertain whether the customer is a "Politically Exposed Person" (refer to part 4.14.2.4 of this Directive).

128. The above information is also necessary, further to the objective of preventing money laundering and terrorist financing, for the purposes of implementing financial sanctions, trade embargoes or measures related to terrorism, terrorist financing or the proliferation of weapons of mass destruction, as imposed against different persons by the United Nations and the European Union or other organisations with whom the credit institution complies on the basis of its internal framework, as well as the lists of the United Nations and the European Union concerning individuals designated as terrorists or linked to terrorism. Therefore, the number, date and country of issue of the passport and the date of birth of the customer must always be indicated on the copies of the data obtained, so that the credit institution can accurately ascertain whether the customer is included on a list of persons subject to sanctions issued by the United Nations or the European Union on the basis of the relevant UN Security Council Resolution and Regulation or Common Position of the Council of the European Union, respectively.

Article 4(1) of Law 58(I)/2016

129. According to article 4(1) of the Implementation of the Provisions of the United Nations Security Council Resolutions or Decisions (Sanctions) and the Decisions and Regulations of the Council of the European Union (Restrictive Measures) Law of 2016 (58(I)/2016), any person who contravenes any of the provisions of the Security Council Resolutions or Decisions (sanctions) and/or the Decisions and Regulations of the Council of the European Union (restrictive measures) is guilty of an offence and without prejudice to

any other provision of a law providing for a longer sentence, in the case of conviction, shall be subject to imprisonment not exceeding two years or to a penalty payment not exceeding one hundred thousand euros or to both sentences in the case of a natural person, and in the case of a legal person in a penalty payment not exceeding three hundred thousand euro.

Articles 3(2) and 6 of Law 58(I)/2016

130. According to Article 3(2) of Law 58(I)/2016, the supervisory authorities as defined in section 59 of the Law may take measures under the provisions of section (6) of article 59 of the Law where a person subject to their supervision fails to comply with the provisions of Law 58(I)/2016. Moreover, in accordance with Article 6 of Law 58(I)/2016 if a competent authority determines that a person undertakes any act in breach of any of the provisions of the Security Council Resolutions or Decisions (Sanctions) and/or Decisions and Regulations of the Council of the European Union (Restrictive Measures), reports the infringement to the Police for a relevant investigation.

Article 16B(1) of Law 110(I)/ 2010

131. Article 16B(1) of the Anti-Terrorism Law of 2010 (110(I)/2010) requires that obliged entities as defined in article 2 of the Law freeze all funds, financial assets and financial resources belonging to or controlled by a designated person or entity, owned or controlled in whole or in part, directly or indirectly, by a designated person or entity, derive or stem from funds or other assets owned or controlled, directly or indirectly, by a designated person or entity, owned or controlled by a person or entity, acting on behalf of, or following instructions by a designated person or entity.

Articles 16C(1) and (2) of Law 110(I)/ 2010

132. According to article 16C(1) and (2) of Law 110(I)/2010, obliged entities report to their supervisory authorities who they, in turn, report to the Ministry of Foreign Affairs any assets that have been frozen or any action taken in relation to compliance with the restrictive measures of the European Union and the sanctions of the Security Council of the United Nations, as referred to in article 17 of Law 110(I)/2010. If an obliged entity fails to comply with the provisions of article 16C(1), then the supervisory authority may take the measures as provided for in section 59(6) of the Law.

4.13.2. Customers within the scope of the Law 64(I)/2017

Law 64(I)/ 2017

133. Without prejudice to the provisions of paragraphs 122(i) and 123 on the identification of natural persons, exceptionally, and only for the purpose of applying the Comparability of Fees, the Payments Account Switching and access to Payment accounts Law of 2017 (N.64(I)/2017), the determination of the identity of persons legitimately residing in the Union, within the meaning of article 2 of Law 64(I)/2017, can be done by presenting to

the credit institution official documents issued by the competent Cypriot authorities provided that they meet the following criteria:

(a) bear the photograph as well as, at a minimum, the following personal information of the holder: name, date of birth and nationality/country of origin,

(b) bear expiry date and are valid (i.e. not expired),

(c) contain a unique identity or registration number/code.

134. Credit institutions should request natural persons falling within the scope of Law 64(I)/2017 to present during the opening of an account, if available, the national identity card or passport or copies thereof, or any other documents that could be helpful in their identification.

135. As regards the identification and verification of identity under paragraph 133 for persons who have applied for international protection or who have already been recognised as political refugees or as holders of subsidiary protection, in the event they get information or have reasonable suspicion as to the authenticity of the documents referred to in paragraph 133, credit institutions shall not apply to the Embassy or Consulate of the country of origin of the natural persons in Cyprus or to financial institutions located in the country of origin of the natural persons in order to verify the authenticity of such documents, except to the competent issuing authority of the Republic, on the basis of a written authorization given by the customer when opening an account.

136. Without prejudice to the provisions of paragraph 122(ii), in the case of (and only) the persons referred to in paragraph 133 and only for the purposes of the application of Law 64(I)/2017, the verification of the address of the customer's residence may be achieved, in addition to the preferred ways described in paragraph 126, in one of the following ways:

(i) With the address indicated in one of the official documents referred to in paragraph 133 and which may even represent the temporary address of the person applying for the commencement of a business relationship (e.g. a government centre for the admission of asylum seekers or a non-governmental organisation assisting the person concerned).

(ii) By a statement confirmed by oath (affidavit) of their address and also the obligation to inform the credit institution, as soon as possible, in case of change of address.

137. Credit institutions establish policies and procedures, take adequate measures and apply control procedures based on the assessed risk for business relationships with persons falling within the scope of Law 64(I)/2017.

138. The combination of geographic risk and uncertainty regarding the identification documents of natural persons falling within the scope of Law 64(I)/2017 may involve an increased risk of money laundering and terrorist financing for credit institutions, which may, however, be manageable, by implementing appropriate measures and procedures based on the assessed risk. Measures and procedures targeted towards the specific categories of persons may include, inter alia, the following:

(i) limits/restrictions, based on the assessed risk, on the products and services to be provided by credit institutions aiming to better manage the risk of money laundering and terrorist financing without compromising compliance with the characteristics of a payment account with basic features (article 18(1) of the Law 64(I)/2017),

(ii) appropriate control procedures to ensure that the holder of the account will provide the required documents in good time and as soon as they expire,

(iii) incorporating of the specificities of the persons within the scope of Law 64(I)/2017 (e.g. asylum seekers, political refugees, holders of subsidiary protection, victims of trafficking and/or exploitation of persons) to the measures, procedures and systems of credit institutions. These specificities may concern frequent changes in the residence address of the persons concerned, the conduct of frequent small transactions with the countries of origin and the receipt of state aid (e.g. beneficiaries of minimum guaranteed income),

(iv) sending the correspondence of these persons through registered post or through a member of the staff of the credit institution, as an additional diligence measure to verify the customer's address.

139. It is provided that the obligation of credit institutions to apply the necessary due diligence measures such as the creation of the customers economic profile and the continuous monitoring of transactions is valid as for all customers.

140. In case where credit institutions decide to refuse or limit the services of the payment account with basic features for the purpose of complying with the prevention of money laundering and terrorist financing, they must substantiate the reason for these actions and be prepared to demonstrate to the competent authority that those measures were appropriate and proportionate to the risk arising from the business relationship with the specific natural person.

141. For all cases of persons within the scope of Law 64(I)/2017, the special residence permit and, in the case of political refugees, the refugee travel document issued by the Civil Registry and Migration Department of the Ministry of Interior satisfy the criteria (a) to (c) of paragraph 133 of this Directive and therefore credit institutions should request these documents in the case of persons falling within the scope of the Law. Copies of these documents, which must be presented as originals by the person requesting the opening of an account, are listed in Appendices 3A, 3B and 3C.

142. It is noted, as an additional control measure, that credit institutions should ask natural persons within the scope of Law 64(I)/2017 to present at the opening of an account, if they have, an identity card or passport or copies thereof, or any other documents issued by their country of origin which may be helpful in their identification.

4.13.2.1. Identification documents for specific categories of natural persons within the scope of L. 64(I)/2017

143. Applicants of international protection (whose application is examined by the competent Cypriot authorities and therefore do not have a special residence permit and a refugee travel document which satisfy the criteria (a) to (c) of paragraph 133 of the Directive) may request the opening of a payment account with basic features, by presenting the confirmation of submission of application by the Asylum Service of the Ministry of Interior and the Alien Registration Certificate (attached as Appendices 3D and 3E respectively). Due to the fact that the aforementioned documents do not bear an expiration date, credit institutions provide the applicant with a specific form whereby the applicant gives his/her consent to the credit institution to get information regarding the examination status of his/her application for asylum by the Asylum Service of the Ministry of Interior (Appendix 3F). This form is sent by fax to the Asylum Service, which discloses the status of the application (under examination/completed) with the signature and stamp of the Service and is sent back to the credit institution in the same way. The aforementioned procedure is followed by the credit institutions according to the risk and for as long as the application of the individual concerned is under examination.

144. It is noted that the issuance of a special residence permit for political refugees or holders of subsidiary protection is usually made within one year from the date of the application, while six months after the submission of the application, the Asylum Service sends to the applicant, before and/or after the interview, a notification that his application is under examination. Credit institutions should request and receive from the customer these notifications as an additional control measure (Appendices 3G and 3H respectively).

145. Victims of trafficking and/or exploitation of persons may present the confirmation of recognition (Appendix 3I) issued by the Cyprus Police, which satisfies criteria (a) to (c) of paragraph 133 of the Directive and is valid for one month, until the issuance of the special residence permit by the Civil Registry and Migration department. Credit institutions should request and receive from the customer the special residence permit as soon as it is issued.

4.13.3. Joint Accounts

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

4.13.4. Proxies or representatives of third persons

The Law Article 61(1)

147. Article 61(1) of the Law provides that obliged entities shall, in the application of the measures referred to in paragraphs 61(1)(a) and (b), verify that any third person who intends to act on behalf of a customer is duly authorised by the customer for this purpose and shall identify and verify the identity of this person. As a result of this, credit institutions must take all necessary measures so as to ascertain and verify the identity of the customers and of the proxies or representatives acting on behalf of the beneficial owners of the accounts. For this purpose, credit institutions should always take a copy of the authorisation agreement concluded between the parties concerned.

4.13.5. Accounts of unions, associations, clubs, provident funds and charities

148. In the cases of opening of accounts in the name of unions, associations, clubs, provident funds and charities, credit institutions should ascertain the objectives of their operation and satisfy themselves as to their legitimacy by requesting the submission of their constitutional and other important documents including the registration certificate by the competent authorities (where such registration is required by law). Additionally, credit institutions should obtain a list of the members of the Board of Directors/Management Committee and verify the identity of all individuals that have been authorised to manage the account in line with the identification procedures for natural persons.

4.13.6. Accounts of unincorporated businesses/partnerships

149. In the cases of accounts of unincorporated businesses, partnerships and other entities without legal identity, the identity of their directors/partners/beneficial owners and of all persons duly authorised to operate the accounts, should be verified in line with the

procedures applied for natural persons. Furthermore, in the case of partnerships the original or a certified copy of the partnership's registration certificate should be obtained. Credit institutions should also obtain documentary evidence of the address of the management main offices, ascertain the nature and size of the business activities and receive all the information required under Section 4.11 above for the creation of the economic profile of the business. In cases where a formal partnership arrangement exists, credit institutions should request this as well as a written a mandate from the partnership, authorising the opening of an account and the persons responsible for its operation.

4.13.7. Accounts of legal persons (companies)

150. Due to the particular difficulties encountered in determining the real shareholders/beneficial owners of accounts in the name of organisatons with legal identity (companies), these are one of the most "popular" means of money laundering and terrorist financing, particularly when it concerns companies that do not have physical presence and activities in the country of incorporation (shell companies). Credit institutions should take all appropriate measures to fully establish the control structure and ownership of companies and verify the identity of the beneficial owners (natural persons) and the natural persons exercising the actual control of the company.

151. The term "shell company/entity" refers to a limited liability company or any other legal/business entity bearing the following characteristics:

a) Has no physical presence or activity in the country of incorporation/registration (other than a postal address);

The physical presence of a company/entity is interpreted as the existence of a place of business or activity (owned or leased buildings) in the country of incorporation/registration. Also, the absence of substantial management (meaningful mind) and administration could be interpreted as lack of physical presence. The presence of a third person who merely provides services as a representative/proxy person, including the duties of the secretary of the company, is not in itself an indication of physical presence and/or

b) It has no established business activity, little or no independent economic value and no evidence to the contrary.

Nevertheless, the following circumstances could indicate a business activity:

i. the company/entity was established/incorporated for the purpose of holding share capital or shares or equity instruments of another business entity or

entities dealing with legitimate business with identifiable ultimate beneficial owner(s),

ii. the company/entity was established/incorporated for the purpose of holding intangible or other assets, including immovable property, ships, aircrafts, investment portfolio, debt and financial instruments,

iii. the company/entity was established/incorporated to facilitate monetary transactions and assets transfers, corporate mergers, and also for the execution of asset management activities and the trading of shares,

iv. the company/entity acts as treasurer for companies recognised as a group or manages the activities of the group,

v. any other case where conclusive evidence can be provided that the company/entity is involved in a legitimate business, with identifiable ultimate beneficial owner(s).

152. If an entity falls under the above definition and

a) is registered in a jurisdiction where the companies/entities are not obliged to submit to the authorities audited financial statements by independent auditors/accountants and do not prepare financial statements voluntarily from independent approved auditors/accountants and/or

b) has tax residency in a jurisdiction which is included in the EU list of non-cooperative jurisdictions for tax purposes or in the list of non-cooperative jurisdictions of the World Forum for transparency and information exchange for tax purposes (Global Forum on Transparency and Exchange of Information for Tax Purposes) or any other list issued by a reputable organisation in relation to harmful tax practices, tax havens or has no tax residency,

then, business relations with such an entity should not be concluded or, if they exist, should be terminated.

153. In all cases of companies/entities, the institution must decide whether to engage in or maintain a business relationship by applying a risk-based approach in accordance with the legal and regulatory framework and providing fully substantiated justification of such a decision which should be evidenced/documented and duly recorded.

154. In relation to the above, the credit institution shall establish policies, procedures and controls to ensure its effective implementation and full compliance with the above requirements.

155. The verification of the company identity requesting the opening of an account requires to obtain information for the following:

(i) Registration number.

(ii) Registered name and trading name used.

(iii) Registered office address.

(iv) Full addresses of the head office/principal management offices.

(v) Telephone and fax numbers and email address.

(vi) Members of the Board of Directors.

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

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

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

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

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

(i) Certificate of company 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 of the company, certified by the company's Secretary, for opening an account and authorizing the persons who will operate the account.

(vii) In the cases where the registered shareholders act as nominees of the beneficial owner(s), a copy of the agreement concluded between the nominees and the

beneficial owners (trust deed), by virtue of which the shares are registered on the nominee's name on behalf of the beneficiary.

(viii) Ownership structure of the customer certified by the ultimate beneficial owner or the person who exercises the ultimate control on the legal person or the person who has the ultimate responsibility of decision making and who manages the operations of the customer.

(ix) Documents and data for the verification of the identity of the authorised signatories, the registered shareholders and ultimate beneficial owners in accordance with the provisions of this Directive.

(x) Certificate of registered shareholders for the companies participating in the ownership structure of the customer and which hold directly or indirectly share capital of the customer in accordance with article 2 of the Law.

(xi) Recent audited financial statements. In cases where there is no obligation for the preparation of audited financial statements or where these are not available (at least for the previous two years) they shall obtain recent management accounts.

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

158. As an additional due diligence measure, and on the basis of the assessed risk emanating from the business relationship with a specific company, credit institutions could 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 abroad (for non-Cypriot companies) and/or request information from other sources 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 relevant registry of the Registrar of Companies and that the company continues to be registered as an active business in the relevant registry of the appropriate authority in Cyprus or abroad. 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, economic and trading purpose of the transactions performed by the company via its account, then it is imperative that further reviews are effected for ascertaining the nature and any possible consequences of these changes on the documentation and information held by the credit institution for the company and collect all the necessary and additional information for completing and updating the economic profile of the company.

The Law Article 61A

159. According to article 61A of the Law, companies and other legal entities incorporated in the Republic must obtain and retain adequate, accurate and up-to-date information about their beneficial owners, including details of the rights held by the beneficial owners. The companies and legal entities mentioned above must provide the obliged entities, in addition to the information about its legal owner, information on the beneficial owner when the obliged entities take due diligence and identification measures specified in the Law.

The Law Article 61A(4)

160. Article 61A(4) of the Law provides that this information is kept in a central register of beneficial owners of companies and other legal entities, which is kept in the office of the Registrar of Companies in Cyprus (for domestic companies) and is accessible to obliged entities for the purpose of taking customer due diligence and identification measures. It is provided that credit institutions may use the information from the central register of beneficial owners only as an additional measure of customer identification and due diligence, always in accordance with the assessed risk.

161. In the event that the information provided by the customer differs from that held by the official authorities, the credit institution should investigate and where required a suspicion report should be submitted to MOKAS.

162. In case the customer requesting the account opening is a company, whose direct sole or major shareholder is another company (parent/holding) registered in Cyprus or abroad, then credit institutions should, prior to account opening, establish the ownership structure and verify the identity of the natural persons who are the ultimate beneficial owners and/or control the parent/holding company.

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

163. Credit institutions may conclude and maintain business relationships with persons engaging in the provision of financial and investment services, established and/or operating and supervised by a competent authority of a country in the European Economic Area or a lower risk third country by applying, depending on the assessed risk, appropriate due diligence measures in accordance with the requirements of the Law and this Directive.

164. In the case of investment funds, credit institutions should receive full information on the legal status of the fund, the purposes, the investment objectives and the control structure of the fund. In addition, and depending on the risk assessment, data and information are obtained for the identification and verification of the identities of the investment

managers and advisers, administrators and custodians, investors or any other important person involved in the operation of the fund.

165. In the case of establishing and maintaining a business relationships with persons that carry out the above activities and which are incorporated and/or operating in a third country other than those mentioned above, credit institutions should implement the requirements of Section 4.14. As a minimum, credit institutions should apply the following enhanced due diligence measures and procedures, in addition to the customer due diligence and identification measures required by the Law and this Directive for the identification and verification of the identity of natural and legal persons, including the ultimate beneficial owners:

(i) Approval of the AMLCO before the commencement of the business relationship.

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

(iii) Confirmation that the said person is subject to supervision in relation to the prevention of money laundering and terrorist financing.

(iv) A check of whether their license provides for the provision of advisory and/or portfolio management services.

(v) Adequate data and information in order to fully understand the control structure and management of the business activities and the nature of the investment and financial services provided by the customer.

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

(vii) Evaluation of findings for fines or reprimands imposed on that entity by their supervisory authority.

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

166. In the event of commencement of a business relationship with a company that is a subsidiary of another company (parent) that provides financial and investment services, credit institutions should apply the provisions of the above paragraph in relation to the parent company.

4.13.9. Safe custody and rental of safety deposit boxes

167. The credit institutions should treat with caution applications for the rental of safety deposit boxes for the storage of parcels, sealed envelopes, money or other objects. When, such facilities are requested by persons not having an account with the credit institution concerned, the customer identification and due diligence procedures prescribed in the Law and this Directive should be followed.

4.14. Enhanced Due Diligence Measures

4.14.1. Customer identification and due diligence on a risk based approach

The Law Article 64(3)

168. Article 64(3) of the Law requires obliged entities to apply the customer due diligence and identification measures as prescribed by the Law and to take additional and enhanced customer due diligence measures in cases which by their nature present a high risk of money laundering or terrorist financing.

The Law Article 64(1)

169. Article 64(1) of the Law requires obliged entities to apply enhanced due diligence measures in the following cases:

(i) When transacting with a natural person or legal entity established a third country of high risk.

(ii) In cross-border relationships with an institution-customer from a third country,

(iii) In transactions or business relationships with a Politically Exposed Person,

(iv) When the transactions are complex and unusually large, or transactions occur without apparent economic or legal purpose and in particular, the obliged entity intensifies the extent and nature of the monitoring of the business relationship in order to determine whether such transactions or activities appear suspicious.

170. The Central Bank of Cyprus requires the credit institutions to apply enhanced due diligence measures when entering into a business relationship with the following customer categories:

(a) Client accounts

(b) Accounts of Trusts and Foundations .

171. The customer acceptance policy of each credit institution must determine the categories of customers considered to be of potentially higher risk, as defined in the Law, in this

Directive (see Section 4.14.2 below) as well as for those customers the credit institution has classified as of higher risk on the basis of its risk assessment and policy.

172. The criterion for obtaining satisfactory data evidence of a customer's identity should take into account the risk-based approach of money laundering and terrorist financing deriving from each customer, and in each case credit institutions should make informed decisions about the appropriate measures to be applied. The extent and number of checks to be carried out for the verification of the identity data may vary depending on the assessed risk deriving from the customer's country of origin or the type of service, product or type of account requested by the customer, or the background and business or professional activities of the customer, the expected turnover of the account and the transactions, or the complexity of the customer's structure. Data on the expected source of money, namely how payments will be effected, from where and by whom, should always be recorded in order to facilitate the subsequent control of transactions.

173. For customers classified as high risk, credit institutions must take, in addition to the standard due diligence measures, enhanced and additional measures to manage and mitigate appropriately the risks. As a minimum, the enhanced due diligence measures must include obtaining approval from a senior management official for the commencement of a business relationship or the continuation of the business relationship or the execution of an occasional transaction, the taking of adequate measures to ascertain the source of wealth and the systematic and thorough monitoring of the transactional behavior of the customer. In addition to the above and without prejudice to section 4.5 of this Directive, the business relationship should be updated at least once a year or at a shorter interval if deemed necessary.

174. In determining the enhanced due diligence measures to be applied and the extent of such measures, credit institutions shall take into account, in addition to the specific requirements of this Directive, the Guidelines for the Risk Factors.

175. The credit institution should be in a position to demonstrate to the Central Bank of Cyprus, if so requested in the context of the latter’s supervisory role, that the extent of customer identification and due diligence measures applied are proportional to the money laundering and terrorist financing risks.

176. The AMLCO must be informed of the new high-risk customers that the credit institution intends to accept, as well as the existing customers who are re-classified into the high risk category and exercise an advisory role before the final decision is taken. It is stressed

that changing the risk category of high risk customers to a lower level requires the approval of the AMLCO.

4.14.2. High Risk Customers

4.14.2.1. Complex and unusually large transactions or unusual types of transactions

The Law Article 64(1)

177. Article 64(1) of the Law requires an obliged entity to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions and all unusual types of transactions carried out without apparent financial or legitimate purpose and in particular, the obliged entity intensifies the extent and nature of the monitoring of the business relationship in order to determine whether these transactions or activities appear suspicious.

178. The credit institution must apply adequate policies and procedures to identify complex and unusually large transactions or unusual types of transactions. Where a credit institution detects such transactions because:

(i) are greater than expected on the basis of the institution's knowledge of the customer, the business relationship or the category to which the customer belongs,

(ii) they constitute an unusual or unexpected type of transaction compared to the normal activity of the customer or the type of transactions associated with similar customers, products or services, or

(iii) are particularly complex compared to other similar transactions related to similar items, products or customer services,

and the credit institution was not informed of the relevant economic rationale or the legitimate purpose or has doubts as to the accuracy of the information received, it must apply enhanced due diligence measures.

179. Such enhanced due diligence measures should be sufficient so as to assist the credit institution to ascertain whether the specific transactions raise suspicions, and must include at least the following:

(i) application of reasonable and adequate measures to understand the background and purpose of these transactions, e.g. by locating the source and destination of the funds or by finding more information about the customer's business activity in order to determine the plausibility of the customer executing the specific transactions, and

(ii) monitoring of the business relationship and the implied transactions more frequently and with greater attention to the details. A company may decide to monitor individual transactions if such a measure is commensurate with the risk it has identified.

4.14.2.2. Accounts in the name of Trusts and Foundations

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

181. The Law defines the following persons as a beneficial owner of a trust:-

The Law Article 2

(i) the settlor,

(ii) the trustee,

(iii) the protector, if there is,

(iv) the beneficiary or, where the individuals benefiting from the legal arrangement or the legal entity have not yet been identified, the category of persons in whose interest the legal arrangement or legal entity has been established or operates,

(v) any other natural person exercising ultimate control of the trust through direct or indirect ownership or by other means.

The Law Article 61(5)

182. As regards the beneficiaries of trusts or similar legal arrangements, who are determined according to their specific characteristics or by category, obliged entities, in accordance with article 61(5) of the Law, must receive sufficient information for the beneficiary to ensure that they are able to determine the identity of the beneficiary at the time of payment or when the beneficiary exercises his acquired rights.

183. Furthermore, credit institutions should ascertain the nature, purpose of establishment and activities of the trust, as well as the source and origin of funds. The above information

must be verified on the basis of reliable and independent documents or information. Hence, credit institutions should view the trust deed and obtain copies of the relevant extracts of the said agreement, a certified copy of the registration of the said trust in the relevant register, as provided in the Regulating Companies Providing Administrative Services and Related Matters Law 196(I)/2012 and as subsequently amended, or in any other equivalent law of another country or jurisdiction, as well as other relevant information provided by the trustees. All relevant data and information should be recorded and archived in the customer's file.

184. According to the report of FATF ‘’Report on the misuse of corporate vehicles’’ a foundation may be used for similar purposes as a trust. A foundation is a legal entity which can carry out activities and its income derived from the principal assets is used to fulfil the statutory purposes of the foundation. A foundation is controlled by a Board of Directors and does not have owners.

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

4.14.2.3. <u>“Client accounts” in the name of third persons</u>

186. In the context of the performance of their usual professional activities, third persons acting as intermediaries, hold funds on behalf of their customers in "client accounts" opened with credit institutions in the name of the third person. Such accounts may be general (“pooled accounts”) and credited with funds from many customers or they may be opened specifically to be credited with funds belonging to a single customer (“specific client account”).

187. Credit institutions may open "client accounts" in the name of financial institutions from countries of the European Economic Area or a lower risk third country, as defined in paragraph 3 of Appendix II of the Law, by applying, according to assessed risk, the requirements of section 4.6 of this Directive.

188. Where considered necessary and depending on the risk, credit institutions should be satisfied that the financial institution implements adequate and appropriate due diligence measures for their customers and their ultimate beneficiaries. In relation to credit institutions and depending on the risk assessment, they may take measures to assess the adequacy of policies and procedures for the implementation of due diligence measures by requesting, on a sample basis, data and documents from the financial institution for specific customers and transactions.

189. In the event that a Licensee ("licensee") requests to open a general client account, as defined in the Betting Law 106(I) of 2012, credit institutions may proceed to open and maintain such an account, provided that the licensee holds a license by the National Betting Authority or by a corresponding EU Member State authority and is subject to supervision for the purpose of complying with the prevention of money laundering and the terrorist financing. In this respect, credit institutions depending on the risk assessment, may take measures to assess the adequacy of policies and procedures as regards the application of due diligence measures by requesting sample data and documents from the licensee for specific customers and transactions.

190. In the case that the opening of a “client account” is requested by a person acting as auditor/accountant/tax consultant or independent professional lawyer/attorney or trust and corporate service provider or a real estate agent, coming from a country of the European Economic Area or a third country of lower risk as defined in paragraph 3 of Appendix II of the Law, credit institutions may proceed to open it provided that the following are satisfied:

    (i) For “pooled client accounts”, the credit institution verifies the identity of all beneficiaries of credit transactions which equal or exceed 15.000 euro, regardless of whether the transaction is carried out in a single operation or with more transactions which seem to be related.

    (ii) For “specific client accounts”, the identity of the ultimate beneficial owner is verified before opening the account.

    (iii) The credit institution obtains all data and documents, for the verification of the identity of the beneficial owners, duly certified as true copies of the original by the third person during the opening of the account or before the execution of any credit transaction, as the case may be.

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

192. In the cases referred to in paragraphs 190-191 it is pointed out that credit institutions may open "pooled client accounts" provided that the credit institution can hold sub-accounts or connected accounts in its system and is in a position to know, and has verified, the identity of the beneficial owners of credit transactions for amounts equal to or exceeding 15.000 euro. Otherwise, a "specific client account" should be opened and the identity of the beneficial owner should be verified before the opening of the account. In both cases supporting documentation related to the specific transactions should be obtained.

193. Without prejudice to the generality of the above paragraph, transactions for amounts equal to or exceeding 15.000 euro related to payments to Government departments (e.g. Registrar of Companies, Value Added Tax "VAT", Income Tax) may be performed through the "pooled client accounts" without the use of any sub-accounts or connected accounts. It is understood that for the above cases credit institutions are required to verify the identity of the beneficial owners of credit transactions for amounts equal to or greater than 15.000 euro and to obtain documentary evidence of the transactions.

194. For all the above cases, credit institutions must exercise ongoing monitoring of the above mentioned business relationships and transactions in order to ascertain that the funds belong to their customers' customers and not used for their own use. Business relationships should be reviewed on an annual basis.

4.14.2.4. Accounts of Politically Exposed Persons

The Law Article 64(1)(c)

195. Article 64(1)(c) of the Law requires, for transactions or business relationships with Politically Exposed Persons, from obliged entities to:

(i) have appropriate risk management systems, including risk based procedures, to determine whether the customer or the beneficial owner is a Politically Exposed Person

(ii) apply the following measures in the event of a business relationship with a Politically Exposed Person:

(aa) obtain senior management approval for the establishment or maintenance of a business relationship with such person,

(bb) take sufficient measures to verify the source of the assets and the origin of the funds relating to a business relationship or transaction with such a person;

(cc) shall carry out enhanced and ongoing monitoring of this business relationship.

(iii) apply the measures referred to in subparagraphs (i) and (ii) to family members or persons known as close associates of a politically exposed person.

196. It is provided that when a Politically Exposed Person has ceased to have a prominent public function in the Republic or in a Member State or in a third country or in an international organisation, the obliged entity considers the risk that continues to be imposed by the person concerned and takes appropriate measures, depending on the degree of risk, for a period of at least 12 months until such person is considered to no longer bear the risk specific to the Politically Exposed Persons.

197. Article 2 of the Law defines that Politically Exposed Persons means natural persons who have or had been entrusted with prominent public functions in the Republic or in a foreign country, as well as family members, or persons known to be close associates, of such persons.

The Law
Article 2

(i) For the purposes of this definition, "prominent public function" means any of the following public functions:

(a) Head of state, head of government, minister, deputy or assistant minister,

(b) member of parliament or similar legislative body,

(c) member of a governing body of a political party,

(d) member of supreme court, a constitutional court or other high-level judicial body whose decisions are not subject to further appeals, except in exceptional circumstances,

(e) member of court of auditors and of the board of directors of Central Banks,

(f) ambassador, charge d'affaires and high-ranking officer of the armed and security forces,

(g) member of an administrative, management or supervisory body of a state-owned enterprises,

(h) director, deputy director and member of the board or equivalent function in an international organisation,

(i) mayor.

It is provided that the none of the above mentioned public functions shall be understood as covering middle-ranking or more junior officials:

(ii) "family members" shall include the following persons:

(a) the spouse, or a person considered to be equivalent to a spouse of a Politically Exposed Person;

(b) the children and their spouses or persons considered to be equivalent to a spouse of a Politically Exposed Person; .

(c) the parents of a Politically Exposed Person.

(iii) "Person known to be a close associate of a Politically Exposed Person" means a natural person:-

(a) who is known to have a joint beneficial ownership of a legal entity or legal arrangement or any other close business relation with a Politically Exposed Person,

(b) who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a Politically Exposed Person.

198. The establishment of a business relationship with Politically Exposed Persons may expose the credit institution to increased risks. Credit institutions should be even more cautious when such persons come from a country that is well known to be facing widespread corruption problems in public life and economic destabilisation and whose laws and regulations against money laundering and terrorist financing are not equivalent to internationally accepted standards. In order to deal with potential risks from the above, credit institutions should evaluate the countries of origin of their customers, in order to identify those countries that are most vulnerable to corruption or having laws and regulations which significantly lag behind the recommendations of the FATF against money laundering and terrorist financing (see part 4.14.2.6 of this Directive). In relation to the issue of corruption, a useful source of information is the index called "Transparency

International Corruption Perceptions Index", which can be found on the website of the International Transparency Organisation – www.transparency.org. In relation to the adequacy of implementation of the FATF recommendations , credit institutions may derive information from the evaluation reports of the countries prepared by the FATF, regional bodies operating on the FATF standards (e.g. Moneyval Committee of the Council of Europe), the International Monetary Fund and the World Bank.

199. Credit institutions should adopt, in addition to the provisions of the Law, the following due diligence measures when concluding a business relationship with a Politically Exposed Person:

(i) Introduce appropriate risk management procedures to enable them to determine whether a prospective customer is a Politically Exposed Person. Such procedures should include, depending on the degree of risk encountered by each credit institution, the acquisition and installation of a reliable commercial electronic database for Politically Exposed Persons from the market, seeking and obtaining information from the customer himself or from publicly available information which, inter-alia, can be searched and retrieved from the internet. In the case of companies, legal entities and arrangements, the procedures should aim at verifying whether the beneficial owners, authorised signatories, directors and persons duly authorised to act on behalf of the company are Politically Exposed Persons. 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 to establish or maintain a business relationship with a Politically Exposed Person should be taken by a senior management official of the credit institution and at an appropriate level of hierarchy and according to the risk level following a short report on the customer's profile by a competent officer of the credit institution, in order to take informed decisions on issues that directly affect the risk profile of the credit institution.

(iii) When a business relationship is established with a customer (natural or legal person) and then it is found that the natural persons involved are or have become Politically Exposed Persons, then an approval should also be obtained from a senior management official of the credit institution and at an appropriate level of hierarchy and according to the level of risk for the continuation of the business relationship or the operation of the account. In this respect, the credit institution's systems should,

at regular intervals and at least once a month, check their customers (and their connected natural persons) to identify such cases.

(iv) When deciding on the approval of a relationship with a Politically Exposed Person, the senior management official should take his/her decision on the basis of the level of risk of money laundering or terrorist financing to which the credit institution may be exposed in the event of the conclusion of such a business relationship, and the extent to which the credit institution has appropriate means for the effective management of that risk.

(v) Before a business relationship with a Politically Exposed Person is established, the credit institution should take sufficient evidence to enable it to ascertain not only his/her identity but also to assess the professional reputation and integrity (e.g. letters of recommendation from third parties).

(vi) Credit institutions should establish the customer's economic profile by requesting the data and information listed in section 4.11 above. The data on the expected level and the nature of the customer's operations should form the basis for future monitoring. The data comprising the customer's economic profile should be reviewed on a regular basis and updated with any new data and information. Credit institutions should be particularly attentive and diligent when their customers are involved in businesses that are vulnerable to corruption such as trade in oil, cigarettes and alcoholic beverages.

(vii) Credit institutions apply appropriate measures to determine the source of wealth and the origin of funds to be used in the context of the business relationship so that it can be assured that the credit institution is not managing revenue originating from corruption or other criminal activity. The measures that credit institutions should take to determine the source of wealth and the origin of funds of the Politically Exposed Person depend on the degree of risk associated with the business relationship. Where the risk is particularly high, credit institutions should verify the source of wealth and the origin of funds on the basis of reliable and independent data, documents or information.

(viii) Credit institutions should carry out enhanced and ongoing monitoring of both the transactions and the risk profile of the customer. Unusual transactions should be identified and information available to the credit institution should be re-examined on a regular basis to ensure timely identification of any new or emerging information that could affect the risk assessment. The frequency of monitoring should be

determined by the level of high risk associated with each relationship. Without prejudice to the above, the account and the economic profile of the customer should undergo an **annual review** with the purpose of deciding whether or not it will be allowed to continue operating. The officer responsible for monitoring the account should prepare a short report stating the results of the review. The report will be submitted to a senior management official of the credit institution for review and approval and will be archived in the customer's file.

4.14.2.5. Cross-border correspondence relationships with an institution-customer from a third country

The Law Article 64(1)(b)

200. Article 64(1)(b) of the Law requires obliged entities to apply the following enhanced due diligence measures in the cases of cross-border correspondence relationships with an institution-customer from a third country:

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

(ii) The assessment of the systems and procedures applied by the institution-customer for the prevention of money laundering and terrorist financing.

(iii) Obtaining the approval of a senior manager before concluding new correspondent bank relationships.

(iv) Documenting the respective responsibilities of the institution – correspondent and the credit institution-customer.

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

201. According to article 2 of the Law, "correspondent relationship" is:

The Law Article 2

(i) the provision of banking services by a bank ("correspondent") to another bank ("respondent"), including the provision of a current or other liability account and related services, and includes cash management, international transfers of funds, cheque clearing, payable-through accounts and foreign exchange services,

(ii) the relationships between and among credit institutions and financial institutions including where similar services are provided by an institution-correspondent to an institution-respondent, and including relationships established for securities transactions or funds transfers.

202. Credit institutions should always document adequately the enhanced due diligence measures they apply, as well as their decision-making procedures.

203. Although the institutions-correspondents are obliged to apply each of these enhanced due diligence measures to institutions-customers domiciled in a third country, they may adjust the extent of these measures according to the level of risk.

204. In addition to the above, credit institutions should ensure that:

(i) the bank requesting the opening of a correspondent account is affiliated to a regulated financial group or maintains a physical presence with a full manned office in its country of incorporation from which it conducts real banking services, i.e. the applicant bank is not a "shell bank". "Shell Bank" means a credit or financial institution set up in a jurisdiction in which it has no physical presence involving meaningful mind and management and which is unaffiliated with a regulated financial group. The existence and status of operation of the applicant bank as well as the regulatory framework governing its operations should be verified in one of the following ways:

a) verification with data from the Central Bank or other competent supervisory authority of the country of incorporation, or

b) obtaining from the applicant bank evidence of its group structure as well as the license or authorisation held for conducting banking and financial operations.

(ii) they collect sufficient information about the institution-customer in order to fully understand the nature of the business activity of the customer and therefore make it possible to ascertain the extent to which the business activity of the institution-customer exposes the correspondent institution to a higher risk of money laundering. To this end, measures should be taken to understand and assess the risk as to the nature of the customer base of the institution-customer and the type of activities the institution-customer will perform through its correspondent account.

(iii) they identify, on the basis of publicly available information, the reputation of the institution and the quality of supervision. This means that the correspondent institution should assess its assurance that the customer institution is adequately supervised in terms of its compliance with the relevant local obligations to prevent money laundering. In this regard, correspondent institutions may be facilitated in their work from various publicly available sources, such as the FATF or FSAP assessments, which contain sections on effective supervision.

(iv) they assess the audits on the prevention of money laundering and terrorist financing carried out by the institution-customer. This means that the correspondent institution is required to carry out a qualitative assessment of the control framework for the prevention of money laundering and terrorist financing of the institution-customer, and not to be satisfied just on the receipt of copies of the policies and procedures for the prevention of money laundering and terrorist financing by the institution-customer. This assessment should be duly substantiated. In accordance with the risk-based approach, where the risk is particularly high and, in particular, where the volume of the correspondent banking transactions is significant, the correspondent institution should examine the possibility of on-site visits and/or sample checks to ensure that the policies and procedures for the prevention of money laundering of institution-customer are effectively implemented.

(v) obtains Senior Management approval before the establishment of new correspondent relationships.

(vi) the competent senior management official granting the approval should not be the officer that proposes the establishment of the relationship, while the higher the risk associated with the relationship, the higher the hierarchical position should be held by the senior manager that is responsible for granting the approval. Correspondent institutions should keep Senior Management informed of high-risk banking correspondent relationships and the measures they take in order to effectively manage the risk.

(vii) they document the responsibilities of each institution. This documentation may be part of the standard terms and conditions of the correspondent institution, but the correspondent institutions must determine, in writing, how and by whom this service of correspondent banking can be used (e.g. if it can be used by other banks through their relationship with the institution-customer) and what are the

responsibilities for preventing money laundering and terrorist financing of the institution-customer. If the risk associated with the relationship is high, it is appropriate that the correspondent institution shall ensure that the institution-customer exercises the responsibilities assigned to it by the relevant contract, e.g. through monitoring after the execution of the transaction.

(viii) as regards payable-through accounts and nesting accounts, they ensure that the credit institution-customer or the financial organization customer has verified the customer's identity and applies ongoing due diligence in respect of the customer who has direct access to the accounts of the correspondent institution and that it can provide customer due diligence data upon request of the correspondent institution. Correspondent institutions should seek to obtain confirmation from the institution-customer that the relevant data can be transmitted upon request.

4.14.2.6. Transactions with a natural person or legal entity established in a third country of high risk

The Law Article 64(1)

205. According to Article 64(1) of the Law, credit institutions should apply enhanced customer due diligence measures, in addition to the measures referred to in articles 60, 61 and 62 of the Law, when transacting with a natural person or legal entity established in a third country of high risk.

The Law Article 2

206. High risk third country means a third country, indicated by the European Commission[5] under the provisions of paragraph (2) of article 9 of the European Union Directive through the publication of delegated acts, which presents strategic deficiencies in its national system for combating money laundering and terrorist financing, which are seen as major threats to the financial system of the European Union, and a third country, which is classified by the obliged entities as high risk, in accordance with the risk assessment provided for in article 58A of the Law, risk assessment.

The Law Article 64(2)

207. It is provided that, automatic application of enhanced customer due diligence measures is not required in the case of a branch or a subsidiary of majority participation in a high risk third country and the ownership status belongs to an obliged entity established in the

[5] COMMISSION DELEGATED REGULATION (EU) 2016/1675 of 14 July 2016, supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R1675&from=EN. This Regulation was subsequently amended by the delegated acts 2018/105 and 2018/1467.

European Union, where this branch or a majority-holding subsidiary complies fully with the policies and procedures applied at group level in accordance with the provisions of article 68A and, in that case, the obliged entity implements a risk-based approach.

208. Credit institutions monitor and consider the information on countries that seem to be linked to terrorist financing.

The Law Article 64(3)

209. Additionally, section 64(3) of the Law requires credit institutions, inter alia, to consider the "Geographic Risk Factors" listed in Appendix III of the Law in its risk assessment, and to implement enhanced customer due diligence measures in order to manage and mitigate these risks. The risk factors include, among others, countries that have been identified, according to reliable sources, such as mutual assessments, detailed assessment reports or published monitoring reports, to lack of effective systems for the prevention and combating of money laundering and terrorist financing

210. The above risk factors include announcements published by the Financial Action Task Force (FATF), for countries that do not apply requirements for anti-money laundering and terrorist financing in line with the recommendations of the FATF. Specifically, in order to protect the international financial system from risks of money laundering and terrorist financing and to encourage countries to comply rapidly with international standards, FATF publishes after each meeting of its members, two documents with the names of countries having strategic weaknesses/deficiencies in the field of money laundering and terrorist financing, and working with them to address these deficiencies.

211. According to recommendation no. 19 of the FATF, credit institutions are required to apply enhanced due diligence and monitoring measures with business relationships or transactions with natural or legal persons or financial institutions that originate from countries that do not or inadequately apply the FATF recommendations.

212. Credit institutions may apply the following enhanced due diligence measures:

(i) Increase of the amount of information received for the purposes of applying due diligence measures:

i. information about the identity of the customer or the beneficial owner, or the structure of ownership and control of the customer, in order to ensure that the risk associated with the relationship is fully comprehensible. In this context, it may be necessary to obtain and evaluate information about the reputation of the customer

or the beneficial owner, as well as the assessment of any allegations against the customer or the beneficial owner. Examples include, inter alia:

(1) information on family members and close business associates,

(2) information on the past and current business activities of the customer or the beneficial owner,

(3) adverse media.

ii. information on the intended nature of the business relationship in order to ascertain the legitimacy of the nature and purpose of the business relationship and to facilitate the credit institution in the preparation of a more comprehensive risk profile of the customer. This may include obtaining information about the following:

(1) number, size and frequency of transactions likely to be carried out through the account, in order for the credit institution to be able to identify deviations that may raise suspicions (in some cases it might be appropriate to request evidence),

(2) the reason for which the customer requests a specific product or service, especially when the reason why the customer's needs cannot be better covered in another way or in another jurisdiction, is not clear,

(3) the destination of funds,

(4) the nature of the business activity of the customer or the beneficial owner in order for the credit institution to be able to better understand the potential nature of the business relationship.

(ii) Increase of the quality of the information received for the purposes of applying due diligence measures to verify the identity of the customer or the beneficial owner, including in the following ways:

i. requirement by which the first payment must be effected by means of an account for which it can be verified that it is kept in the name of the customer in a bank applying due diligence measures which are not less stringent than the corresponding standards defined in Chapter II of the European Union Directive, or

ii. safeguard that the customer's assets and funds used in the context of the business relationship do not constitute revenue from criminal activity and that the source of wealth and the origin of funds are consistent with the data the credit institution knows of the customer and the nature of the business relationship. In certain cases

where the risk associated with the relationship is particularly high, the verification of the source of wealth and the origin of funds may be the only appropriate means of reducing the risk. The source of funds or wealth can be verified, inter alia, on the basis of VAT returns and income tax returns, copies of audited accounts, paychecks, public documents or references by independent media.

(iii) Increase of the frequency of review to take the assurance that the credit institution is still able to manage the risk associated with the individual business relationship or to conclude that the relationship is not in line with the credit institution's risk appetite and to facilitate the identification of any transactions requiring further examination, inter alia, in the following ways:

i. obtain the approval of Senior Management for the commencement or continuation of the business relationship in order to ensure that Senior Management are aware of the risk to which the credit institution is exposed and that they can make an informed decision as to whether they have the appropriate means to manage that risk,

ii. review of the business relationship on a more frequent basis in order to ensure that any changes in the customer's risk profile are identified and evaluated and relevant measures are taken, if considered appropriate, or

iii. conduct more frequent or thorough monitoring of the transactions in order to identify any unusual or unexpected transactions which may raise suspicions of money laundering or terrorist financing. This may include verification of the destination of funds or the reason for which certain transactions are made.

4.15. On-going monitoring of the business relationship, accounts and transactions

The Law Article 61(1)(d)

213. Article 61(1)(d) of the Law requires that identification procedures and customer due diligence measures include the exercise of ongoing monitoring in relation to the business relationship, with a thorough examination of the transactions effected during this relationship, in order to ensure that the transactions carried out are consistent with the data and information held by the obliged entity regarding the customer, the business and risk profile of the customer, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

The Law Article 58(e)

214. Article 58(e) of the Law requires, inter alia, credit institutions to examine in detail any transaction which, due to its nature, is deemed to be particularly susceptible to being linked with money laundering activities or terrorist financing, and in particular complex

or unusually large transactions and all unusual types of transactions carried out without apparent economic or clear legal purpose.

The Law Article 60(d)

215. According to article 60(d) credit institutions apply the identification procedures and customer due diligence measures where there are doubts about the accuracy or adequacy of the documents, data or information previously collected for the identification of an existing customer.

216. Identification procedures and customer due diligence measures shall be applied when negative information about the customer, his/her transactions or activities, are detected in the press or internet or information submitted by a competent authority or MOKAS or another financial institution. In such a case the credit institution should carry out a relevant investigation and evaluation as soon as possible and take measures in accordance with the legal and regulatory framework. The results of the investigation are archived and if some findings are considered important then the Central Bank of Cyprus is informed.

217. Part IV of Appendix 3 of the Central Bank of Cyprus' Directive on Governance and Management Arrangements which defines the "principles for a sound and an effective operation of information technology systems in the context of managing operational risk" imposes on credit institutions the obligation to apply, for the systems and services offered via the internet, inter alia, the following:

(i) automated systems for the monitoring of transactions, whose effective operation will be the basis for the creation, by the institution, of statistical models of customers' transactions. These systems, based on the profile established for each customer, should be in a position to identify any transactions indicating extraordinary behavior and produce, in real time, alerts for the investigation of potential cases of fraud.

(ii) effective management of the risk of money laundering and terrorism 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, institutions are expected to install filters and monitoring tools/systems which, as a minimum, will impose limits on specific groups or categories of transactions, thus, providing the possibility of delaying the execution of a transaction until the verification of specified details etc, and

(iii) capability of easily accessing and processing the details of historic 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 potential cases of fraud, money laundering, terrorism financing, provision of investment services and other transactions.

218. Ongoing monitoring of customer accounts and transactions is an essential element of any effective system of anti-money laundering and terrorist financing procedures. Credit institutions must have a full understanding of the normal and justified movement of their customers' accounts and of their overall economic profile so that they can identify transactions outside the ordinary form of account movement, or complex or unusual transactions or transactions carried out without any apparent economic purpose or clear legitimate reason. Without such knowledge, credit institutions will not be able to fulfil their legal obligation for the identification and reporting of suspicious transactions/activities to MOKAS. It is noted that pursuant to article 70 of the Law, it is required from persons who conduct financial or other activities to refrain from carrying out transactions for which they know or suspect that they are related to money laundering offences or terrorist financing, before reporting their suspicion to MOKAS in accordance with articles 27 and 69 of the Law.

219. The procedures, the frequency and intensity of the examination of transactions and the monitoring of accounts should consider the level of risk and achieve, as a minimum, the following:

(i) The periodic review of the customer database to identify Politically Exposed Persons and other accounts of higher risks. Hence, the management information systems of credit institutions should be able to produce analytical statements for each group of high risk customers in order to facilitate the task of monitoring their accounts and their transactions.

(ii) The identification of complex or unusually large transactions, or unusual types of transactions carried out without apparent economic or clear legitimate reason or suspicious transactions incompatible with the economic profile of customers for purposes of further investigation.

(iii) The identification of transactions that might be linked with terrorist financing.

(iv) The creation of warning messages/alert rules for suspicious or unusual transactions, according to the parameters and scenarios defined.

(v) The investigation of unusual or suspicious transactions by competent employees appointed for this purpose. The results of the investigations should be recorded on a separate note and be readily available for inspection.

(vi) Taking all necessary measures and actions on the basis of the findings of the investigation including the internal reporting of suspicious transactions/activities to the AMLCO.

(vii) The identification of the source and origin of the money credited to accounts in relation to the economic profile of the customer.

(viii) The filtering of the credit institution's customer base and transactions on the basis of the lists of persons or entities subject to restrictive measures, issued on the basis of relevant European Union Regulations and Decisions of the Security Council of United Nations. The filtering is carried out in real time at the beginning of the business relationship or the execution of the transaction. With the introduction of new persons in existing lists or new lists, the information system filters the customer base of the credit institution including the connected persons, in order to ascertain whether it maintains or maintained a business relationship with the specific persons or entities, the kind of relationship and every related transaction. The credit institution should be assured at regular intervals that the relevant information system uses the correct and updated lists.

(ix) The periodic check of the customer base to identify possible negative information about the customers or other persons connected with them.

220. Monitoring can be done in real time, i.e. it will focus on transactions and activity when receiving information or orders from a customer, before or during the processing of the order, or subsequently, through the revision of the transactions and/or customer activities. Monitoring the transactions and activity in real time possibly reduces the exposure of the institution to money laundering and terrorist financing. Monitoring after the execution of the transactions may be more effective at detecting unusual patterns.

221. Monitoring may include non-automated and automated processes. Automated monitoring processes may add value to non-automated processes by recognizing transactions or activities that do not fall within specified parameters. This is particularly true when a credit institution processes large volumes of customer transactions. It is provided that the use of automated monitoring methods does not eliminate the need for a credit institution to remain vigilant, since factors such as staff intuition, direct contact with a customer and the ability, through experience, to recognize transactions and activities that do not seem to be meaningful cannot be automated.

222. Credit institutions should introduce and implement adequate automated management information and administration systems, that will be able to provide, on time, to the Senior

Management, the AMLCO and other competent employees with reliable essential information for the identification, analysis and effective monitoring of customer accounts and transactions on the basis of their assessed risk of involvement in money laundering and/or terrorist financing.

223. The monitoring of accounts and transactions must be carried out in relation to certain types of transactions, the economic profile of the customer, the usual turnover/activities of the customer and comparing at regular intervals the movement of the account with the expected movement, as it was declared at the opening of the account, as well as with the movement of the account and the nature of the transactions carried out by other customers operating in the same business sector. Significant deviations should be further investigated and the findings should be recorded in a separate memo which is archived in the customer's file.

224. Moreover, the procedures should cover customers who do not have direct contact with the credit institution, dormant accounts showing unexpected movement, unusual transactions carried out through automated teller machines, early loan repayments, etc. It is also necessary to monitor cash deposits and/or withdrawals, whether the transaction is carried out in a single operation or in several operations which appear to be linked. The automated/computerised management information and administration systems should also be used to extract information in relation to data missing from account opening documents, the customer's identity and economic profile, and overall data on the customer's business relationship with the credit institution.

225. In general, computerised/automated systems should be able to aggregate the balances and movement of all connected accounts on a consolidated basis and detect unusual or suspicious transaction types and activities. This can be done by setting limits for a particular type or category of accounts (e.g. high risk accounts) or transactions (e.g. cash deposits or withdrawals, incoming and outgoing fund transfers above a predetermined limit) considering the customer's economic profile, the country of origin, the source and the destination of funds, , the counterparties, the transaction type or other risk factors. Particular attention should be given to transactions that exceed the predefined limits. Certain types of transactions should alert the credit institution's mechanisms that a customer may be involved in unusual or suspicious activities. These may include transactions that do not seem reasonable from a financial or commercial standpoint or include large amounts of cash or other financial instruments or several large incoming funds transfers that are incompatible with the normal and expected customer's

transactions. Very high account turnover, incompatible with the size of the balance, may be an indication of money laundering through the account.

226. The effectiveness of a monitoring system in detecting unusual activity, will depend on the quality of the parameters and criteria that define the scenarios of the alerts and the ability of the staff to assess and act appropriately with regard to these results. The needs of each credit institution will therefore be different and each system will vary depending on the relative risk assessment and its capabilities according to the size, nature and complexity of the institution. It is important to have a balance in the definition of alerts so as not to generate a large number of "false positive" alerts that require excessive resources for investigation but, on the other hand, not to generate a small number of alerts, thereby increasing the risk of not identifying suspicious transactions. The added value provided, i.e. whether they create the conditions for a true positive result or not, is essential for the set-up of the systems. In each case, the credit institution shall keep in writing the parameters, criteria and any limits that determine the relevant scenarios of the alert messages.

227. Regardless of the above, the definition of parameters and scenarios should be based on the assessment of money laundering and terrorist financing risks by the credit institution and the specific risks faced by the credit institution. Also, parameters and scenarios should be updated periodically so as to consider and reflect changes in laws and directives, as well as any other information the credit institution determines as relevant.

228. For unduly justified alerts the procedure of section 7 of this Directive should be followed.

229. Credit institutions should ensure that the staff involved in the monitoring and investigation of alerts have received appropriate and adequate training for this purpose.

230. Account and transaction monitoring procedures should include, inter alia, measures for monitoring (e.g. audit trail) of alerts and ensuring their proper management.

231. In order to ensure the correct and effective operation of the procedures in relation to the examination and investigation of the alerts produced by the computerised system, credit institutions, depending on the size and nature of their operations, should apply the "four eyes principle". In addition, the management of the alerts should be audited by the Internal Auditor.

232. Credit institutions must make sure that the data stored in the banking system is accurate and valid to ensure that the data flowing through the computerised systems for the purposes of monitoring the accounts and transactions is complete and accurate.

233. Computerised automated transaction monitoring systems should also be able to produce statistical data for each individual customer and for categories of customers with common characteristics. Credit institutions should monitor these statistics at regular intervals depending on the risk involved and apply additional due diligence measures, where deemed necessary.

234. The credit institution evaluates the transaction and account monitoring system at least once every 2 years or if necessary earlier. The evaluation should include, inter alia, the correctness of data sources, administrative and managerial supervision, the policy, procedures and controls, its effectiveness and whether it responds to the risks of money laundering and/or terrorist financing undertaken by the institution.

235. Credit institutions should apply appropriate measures to ensure that the resources available, human and technological, are adequate for the correct and timely examination and investigation of the alerts produced by the computerised system.

5. CASH DEPOSITS AND WITHDRAWALS

5.1 Cash Deposits

236. Despite the rapidly changing face of crime, the increase in cyber-crime and the ever-diversified practices used by criminals, money laundering detected by prosecuting authorities at European level remains overwhelmingly traditional. Although the use of cash has been gradually reduced by the consumers, it is however one of the preferred methods used to legalise the proceeds of all types of crime. Cash is usually used at the placement stage, but it also plays a role in the other two stages of money laundering. It is noted that in the European Union a large percentage (approximately 30%) of the suspicious transaction reports originates from the use of cash[6].

237. Hence, the most effective way of preventing but also of detecting money laundering activities is at the initial stage when criminals attempt to place cash from illegal activities in the financial system.

238. It is therefore imperative that credit institutions apply appropriate procedures for accepting and checking cash deposits for amounts equal to or exceeding 10.000 euro or the equivalent in foreign currencies. In particular, credit institutions are required, depending on the assessed risk, to carry out checks in order to ascertain the source and origin of the cash and also to determine whether the amount and nature of the transaction is consistent with the activities/operations and economic profile of the customer. In addition, and depending on the limits and controls to be set by each credit institution, appropriate documentary evidence and data on the financial, commercial or other purpose of the cash deposit should be obtained, which should be performed after approval by a senior management official. Similar checks should also be carried out for cash deposits below 10.000 euro or the equivalent in foreign currencies when it is suspected that the transaction is likely to be linked to money laundering or financing of terrorism.

5.2 Deposits of cash imported from abroad

5.2.1 Prohibition to accept deposits of cash in foreign currencies imported from abroad.

239. Credit institutions are prohibited from accepting cash deposits in foreign currencies of a value equal to or greater than 10.000 euro imported from abroad where:

[6] https://www.europol.europa.eu/newsroom/news/cash-still-king-criminals-prefer-cash-for-money-laundering

(i) these are not accompanied by the relevant import declaration to the Customs and Excise Department ("Cash Declarations") under Regulation (EC) 1889/2005 of the European Parliament and of the Council on controls of cash entering or leaving the Community[7] and the Control of Cash Entering or Leaving the Community and the Exercising of Intra-Community Cash Controls Law (N. 53 (I) of 2009)[8] or

(ii) the import declaration contains incomplete, incorrect or false information.

240. In that regard, it is clarified that under Regulation (EC) 1889/2005 of the European Parliament and of the Council on controls of cash entering or leaving the Community and the Control of Cash Entering or Leaving the Community and the Exercising of Intra-Community Controls Law (N. 53 (I) of 2009), any natural person entering Cyprus from a third country or another Member State of the European Union carrying cash of a value equal to or more than 10.000 euro is required to declare the amount in question to a competent officer of the Customs and Excise Department.

241. For cash deposits in foreign currencies imported from abroad which equal or exceed the aforementioned amount, credit institutions should receive and archive together with the transaction, the original of the import declaration. Credit institutions have an obligation to immediately inform the Customs and Excise Department on all cases of customers who intend to deposit cash in foreign currencies imported from abroad which are not accompanied by the relevant import declaration or the import declaration presented contains incomplete, incorrect or false information.

5.2.2 Acceptance of cash deposits in foreign currency

242. An occasional deposit of cash in foreign currency that has been imported into Cyprus from abroad beyond the equivalent of 100.000 euros, by any person or group of connected persons, will only be accepted with the written approval of the AMLCO of the credit institution.

243. Furthermore, the deposit of cash in foreign currency on a continuous and regular basis which exceeds or is foreseen to exceed the equivalent of 100.000 euro, within the same calendar year, by any person or group of connected persons, will be accepted only with the written approval of the AMLCO of the credit institution. It is understood that the deposit of cash below the threshold of 100.000 euro, by any person or group of connected persons, should also be subject to the written approval of the AMLCO when, as a result of that deposit, the total deposits of cash carried out by the person or group of connected persons within the same calendar year shall exceed the equivalent of 100.000 euro.

[7] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0009:0012:EN:PDF
[8] http://www.mof.gov.cy/mwg-internal/de5fs23hu73ds/progress?id=PVdtZkLYnQtLbcRt7JXvklWpqzDlxtIy16jhkKoMgV8,

5.2.3 Definitions of group of connected persons and connected cash deposits

244. "Group of connected persons" consists of:

(i) family members (i.e. spouse and children),

(ii) a natural person and an business entity in which the natural person and any member of his family is a partner or shareholder or director or beneficial owner or has in any other way the control,

(iii) a natural person and a company in which the natural person is a director or possesses substantial interest either on his own or with other members of his family or together with other partners,

(iv) a legal person and parent company, subsidiaries, affiliates, connected companies or other entities which have a substantial interest in the legal entity,

(v) two or more persons, natural or legal, who have economic dependency or are associated in such a way that they may be considered to represent a single risk.

245. For the purposes of the above, "substantial interest" in a company means the interest in any class of shares of the company's capital, with a rate of 25% or more in the class of such shares or interest which gives in any way the ability to someone to decide the election of the majority of the company's Directors or to exert significant influence.

5.2.4 Internal procedures and responsibilities of the AMLCO

246. Applications for the acceptance of cash deposits in foreign currencies mentioned in the above paragraphs should be submitted in writing to the AMLCO by the competent officers of the branches/units of the credit institution that hold the customer account and should be accompanied with full details of the customer, the customer's activities, the nature of the transaction, the source of the cash and, for customers that intend to make deposits on a continuous and regular basis, copies of their most recent annual audited accounts and/or management accounts. After examining the application and the information submitted, the AMLCO shall notify, in writing, his decision to accept or not the deposit if it concerns a customer requesting an occasional transaction, or acceptance of the deposits if it concerns a customer requesting the execution of cash deposits on a continuous and regular basis. Copies of the applications and the decision of the AMLCO should be kept in a separate file by the AMLCO as well as in the customer's file.

247. The AMLCO should ensure, in the context of the "know your customer" principle and before giving his written consent for the acceptance of an occasional deposit or deposits on a regular and continuous basis beyond the set limits, that the size of the cash deposit or deposits in foreign currency is consistent with the financial situation and cash flow of the customer's business and other activities. Furthermore, the AMLCO must ensure that the customer due diligence and identification procedures provided for in section 4 of this Directive have been fully implemented and that the cash does not originate from illegal activities.

248. The AMLCO should record and keep the full details of customers or group of connected customers (name, address, account number(s), branch/unit that holds account(s)) for which a written consent for acceptance of an occasional cash deposit or a series of cash deposits on a continuous and regular basis has been provided. In this respect, the AMLCO should keep separate registers for customers involved in: (i) occasional cash deposits, and (ii) cash deposits on a continuous and regular basis.

249. The AMLCO monitors, at least on a monthly basis, the volume of foreign currency cash deposits effected by the customers for whom he/she has given his/her written consent to accept such deposits on a regular and continuous basis. Within this framework, the AMLCO prepares a detailed monthly statement with data on the cash deposits carried out by these customers during the month in question and the accumulated deposits for the period from the beginning of the year until the end of the month mentioned.

5.2.5 Exempted Cash Deposits

250. Irrespective of the above the following exceptions apply:

(i) Deposits of foreign currency by the Government of the Republic.

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

(iii) Deposits of foreign currency by other credit institutions operating in Cyprus.

5.3 Cash withdrawals

251. Withdrawals of large sums of cash may expose the credit institutions to risk, when the money is used by the final recipients to finance illegal activities or terrorist financing.

252. Consequently, credit institutions are required to apply appropriate procedures for checking cash withdrawals for amounts equal to or greater than 10.000 euro or the equivalent in foreign currencies. In particular, credit institutions are required, depending on the assessed risk, to carry out checks in order to ascertain the purpose and destination of the money, and whether the transaction is consistent with the activities/operations and the customer's

economic profile. Moreover, and depending on the limits and controls that each credit institution puts in place, credit institutions must request and obtain the appropriate supporting documentation and data for the economic, commercial or other purposes of each cash withdrawal which will be performed after approval by a senior management official.

6. RECORD KEEPING PROCEDURES

6.1 Introduction

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

253. Article 68(1) and (2) of the Law requires obliged entities to retain the following documents and information, for a period of five years after the end of their business relationship with the customer or after the date of the occasional transaction:

(a) copy of the documents and information required to comply with the customer due diligence requirements as set out in the Law,

(b) the relevant evidence and records of the transactions which are necessary to identify the transactions,

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

Obliged entities shall ensure that all the above documents are provided promptly and without delay to MOKAS and the competent supervisory authorities for the purposes of carrying out the tasks entrusted to them by Law.

254. The copies of the customer identification evidence must be certified by the credit institution employee who verifies the identity of the customer or the third person to whom the credit institution relies for the purpose of verifying the identity of the customer. The aforementioned certification should bear the name and signature of the person certifying the document and the date of certification. In the case of a third person, it should bear the stamp of the third person to whom the credit institution relies for the purpose of verifying the identity of the customer.

255. For non-Cypriot natural persons and/or legal persons or entities incorporated outside Cyprus, credit institutions may obtain documents translated into Greek or English, apostillee in accordance with the Hague Convention. Credit institutions should obtain original documents, carring the distinctive serial number granted by the Central Authority responsible for implementation of the Hague Convention in the country of issue. The credit institution, after having seen the original documents, may maintain true copies of the said documents in the customer file. The said copies must be certified by an employee of the credit institution, bear the name of the employee, the signature of the employee who certifies the documents as well as the date of the certification.

The Law Articles

256. Article 70B of the Law provides that the processing of personal data carried out under the provisions of the Law is subject to the provisions of the Law providing for the Protection of

70B(1), (2) and (3)

Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018). Also, personal data are processed by obliged entities only for the purposes of the provisions of the Law and are not subject to any other incompatible processing. The processing of personal data for purposes other than those provided for by Law, such as commercial purposes, is prohibited.

The Law Article 70B(4)

257. Obliged entities must provide their new customers with the information required under article 11(1) of the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018), prior to the commencement of a business relationship or the execution of an occasional transaction. Obliged entities should provide information to their new customers before commencing the business relationship or executing an occasional transaction about the processing of personal data under the provisions of the Law for the purpose of preventing money laundering and terrorist financing.

The Law Article 70B(5)

258. The right of access by the data subject to the data relating to it may be partially or wholly waived in accordance with the provisions relating to the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018) -

(a) for the purpose of the proper fulfilment of the duties of obliged entities and supervisory authorities, as they derive from the Law,

(b) in order not to obstruct the conduct of official or legal investigations, analysis or procedures for the purposes of the Law and to ensure that the prevention, investigation and detection of money laundering and financing of terrorism are not jeopardised.

The Law Article 70B(6)

259. The processing of personal data under the provisions of the Law in order to prevent money laundering and terrorist financing is considered a matter of public interest in accordance with the provisions of Directive 95/46/EC.

The Law Article 68B

260. Furthermore, credit institutions must implement systems and procedures which enable prompt response to questions from MOKAS or the Central Bank of Cyprus or other supervisory authority with the necessary competence as to whether they have or had, during the last five years, a business relationship with specific natural or legal persons as well as the type of this business relationship.

261. MOKAS needs to detect with sufficient evidence the route of illegal money including the final destination and to form the economic profile of the account and customer under investigation. In order to achieve the above, credit institutions should ensure that, within the framework of the

investigation of a suspected transaction by MOKAS, they will be able to promptly provide the following information:

(i) the identity of the account holders,

(ii) the identity of the actual owners/beneficiaries of the account,

(iii) the identity of persons who have the right to manage the account,

(iv) data relating to the volume and the transactions which are executed through the account,

(v) connected accounts,

(vi) in relation to specific transactions:

1. the source of money,
2. the type and amount of the transaction currency,
3. the way in which the money has been deposited or withdrawn, i.e. cash, cheques, electronic remittances, etc.,
4. the identity of the person who carried out the transaction,
5. the destination of the money,
6. the nature of the instructions and the authorisation provided, and
7. the type and identification number of the account involved in the transaction.

6.2 Form of data

262. It is acknowledged that copies of all the data and documents cannot be kept, practically, indefinitely, and it is therefore necessary to set a number of priorities. Although the Law establishes a specific period of record keeping, it is stressed that in cases where the data and documents relate to investigations that are still in progress, then these should be kept until the competent authority conducting the investigation confirms that the investigation has been completed and that the case has been closed.

263. It is also acknowledged that keeping the data for the identity, transactions, correspondence and other information that make up the customer's economic profile creates a huge volume of documents that need to be stored. Therefore, the keeping of the data can be made in other forms, except for the original documents, e.g. in electronic or other similar formats. The main purpose is to allow credit institutions to promptly and without delay retrieve relevant information.

264. In view of the above, when credit institutions define their policy for record keeping and archiving, they should take into account both the requirements of the Law and the possible needs of MOKAS and the competent supervisory authorities.

The Law Article 47

265. Article 47 of the Law provides that in the cases where the relevant information is stored in a computer, it must be possible to present them in a format that is visible and legible, so that they can be transmitted to MOKAS unaltered.

6.3 Electronic transfers of funds

Regulation (EU) 2015/847

266. On 26th June 2017, Regulation (EU) 2015/847 of the European Parliament and of the Council of 20th May 2015 on the data accompanying transfers of funds and repealing Regulation (EC) 1781/2006[9] entered into force. The purpose of this Regulation is to align European legislation with recommendation No. 16 of the international standards for the prevention and combating of money laundering and the financing of terrorism and the proliferation of nuclear weapons, which was adopted in 2012 by the FATF.

267. Regulation (EU) 2015/847 aims to make it more difficult to misuse transfers of funds for terrorist financing and other financial criminal acts and to enable the competent authorities to fully identify such transfers where this is necessary for reasons of prevention, detection and investigation of money laundering or terrorist financing.

268. For this purpose Regulation (EU) 2015/847 -

- specifies rules on the details of the payers and beneficiaries accompanying transfers of funds, in any currency, when at least one of the payment service providers involved in the transfer of funds is established in the Union,

- requires the payment service provider of the payee and the intermediary payment service provider to establish effective procedures to ascertain whether there are deficiencies in the information of the payer and the payee, and

- requires the payment service provider of the payee and the intermediary payment service provider to implement effective risk-based procedures, which determine whether to execute, reject, or suspend the transfer of funds that are not accompanied by the required complete information for the payer and the payee and for the taking of appropriate monitoring measures.

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R0847&from=EL

269. However, regulation (EU) 2015/847 does not specify in detail what payment service providers and intermediate payment service providers should do to comply. Therefore, article 25 of that Regulation requires the European Supervisory Authorities (ESAs) to issue guidelines to the competent authorities and payment service providers on the measures to be taken by payment service providers and intermediate payment service providers to comply with regulation (EU) 2015/847, in particular with regard to the application of articles 7, 8, 11 and 12.

270. On 22 September 2017, the ESAs published common guidelines[10] on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage transfers of funds lacking the required information. Therefore, credit institutions should consider the relevant guidelines in the application of their obligations under Regulation (EU) 2015/847 and this Directive.

The Law
Article 71

271. Article 71 of the Law provides that the non-execution or delay of execution of any transaction on behalf of a customer, by an obliged entity, due to failure to provide sufficient data or information, for the nature and economic or commercial purpose of the transaction and/or for the parties involved, as required by directives of the competent supervisory authority or Regulation (EU) 2015/847 or due to knowledge that money held in the account or the transaction are likely to be linked to money laundering or terrorist financing, does not constitute breach of any contractual or other obligation by the said person to its customers.

[10] Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-to-prevent-transfers-of-funds-can-be-abused-for-ml-and-tf/-/regulatory-activity/press-release

7. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES

7.1 Introduction

272. Although it is difficult to give a definition of the suspicious transaction as the types of suspicious transactions that may be used by criminals involved in money laundering and terrorist financing are almost unlimited, a suspicious transaction is usually incompatible with the known, legitimate business of the customer or personal activities or with the usual turnover of the specific account or, more generally, with the economic profile that was created by the credit institution for its customer. It is therefore imperative that credit institutions ensure that they always keep sufficient information, that they have built a comprehensive economic profile and that they are aware of the activities of their customers so that they are able to promptly recognize that a transaction or a series of transactions is unusual or suspicious.

273. In addition to the identification of suspicious transactions related to money laundering, credit institutions must ensure that there are infrastructures in place for identifying suspicious transactions involved in terrorist financing. The funding of terrorist organisations is done from revenue originating from both legal and illegal sources. Criminal activities for obtaining revenue include, among other things, abductions (demanding ransom), extortion (demanding money for "protection"), smuggling, tax evasion, theft, burglaries and drug trafficking. Legitimate methods for obtaining revenues used by terrorist organisations include, inter alia, subscriptions collection, selling books, cultural and social events, donations, and fundraising.

274. Transactions that may be linked to terrorist financing usually involve small amounts and cannot be traced promptly. For this reason credit institutions should always keep adequate and up-to-date information about their customers and their financial activities and should apply appropriate procedures so that they can identify when a transaction or a series of linked transactions or unusual transactional behavior might be linked to terrorist financing. Furthermore, the financing of terrorism is mainly linked to the final destination of the funds, since the source and origin may concern legitimate activities.

275. It is emphasised that the financing of terrorism has a huge impact on both the international and the national level and for this reason credit institutions should ensure that there exist necessary preventive measures and controls.

7.2 Examples of suspicious transactions/activities

276. A criminal seeking to legalize income from illegal activities or to finance terrorism will try to use any product or service offered by credit institutions as a means of converting money from illegal to legal. This process can vary from a simple cash transaction to more pretentious and complex

transactions. A list containing examples of suspected transactions/activities related to money laundering and terrorist financing is attached as Appendix 4 to this Directive.

277. This list is not exhaustive, nor does it contain all types of transactions that may be used and therefore must be updated and adapted to the situations and new ways and methods used for money laundering and terrorist financing since it is impossible to define them fully. However, the relevant list can assist credit institutions and their staff in identifying the main ways in which illegal revenues are legalized and terrorism is financed, as well as understanding the methodologies used. The identification by credit institutions of any of the transactions listed in the Appendix should be the subject of further investigation and a reason for seeking additional information and/or explanations concerning the source and origin of funds, the nature and the economic/commercial purpose of the transaction as well as the events associated with the specific activity.

7.3 Internal Report of suspicious transactions/activities

The Law Article 27

278. Under Article 27 of the Law it is an offence for any person who knows or reasonably suspects that another person is engaged in money laundering or financing of terrorism offences, and the information on which the knowledge or reasonable suspicion is based has come to his attention during his or her employment, profession or business, and does not report to MOKAS this information, as soon as is reasonably practical, after it comes to his/her attention. Failure to report in these circumstances is punishable with a maximum of two (2) years imprisonment or a fine not exceeding 5.000 euro or both of these penalties.

The Law Article 26

279. In the case of personnel of obliged entities, article 26 of the Law provides that the internal suspicion report to the AMLCO constitutes fulfilment of the legal obligation to disclose information deriving from article 27. Therefore, credit institutions should ensure that all staff are aware of their legal obligations and of the person (i.e. the AMLCO) to whom they will report their knowledge or suspicion of money laundering or terrorist financing.

The Law Article 69A

280. In accordance with article 69A, disclosure in "good faith" of information by an obliged entity or by an employee or by a director of such obliged entity, in accordance with the provisions of article 69, does not constitute a breach of any contractual or legislative, regulatory or administrative ban on disclosure of information, nor does it involve any kind of liability for the obliged entity or its directors or employees, even if the circumstances did not allow them to know exactly what the basic illegal activity was and irrespective of whether the illegal activity was actually committed.

The Law Article 69B

281. Credit institutions, in accordance with Article 69B of the Law, must provide protection against any threat or hostile action or any exposure to threats or hostile acts and in particular from adverse

or discriminatory actions at the workplace towards a person who submits an internal report or a report to the Unit (MOKAS) for suspicious transactions under the provisions of article 69.

282. All "Internal Suspicion Reports for money laundering and terrorist financing" must be archived and kept in a separate file by the AMLCO.

283. As part of the review, other connected accounts or relationships of the customer that was reported should be considered. This relationship may occur commercially or through other natural persons (professional intermediaries, shareholders, authorised signatories, directors, etc.).

284. From the time of submission of the internal suspicion report, all subsequent transactions of the involved customer and the other connected accounts should be monitored by the AMLCO.

285. If as a result of the evaluation described above, the AMLCO decides not to disclose the relevant information to MOKAS, then he/she should fully explain the reasons for the decision in the "Evaluation of Internal Suspicion Report for money laundering and terrorist financing" which, as already mentioned, should be archived in the relevant file.

7.4 Reports to MOKAS

The Law Article 70

286. Article 70 of the Law requires obliged entities to refrain from carrying out transactions, for which they know or suspect that they are related to money laundering or terrorist financing, before they report their suspicion to MOKAS in accordance with articles 27 and 69 of the Law. As stated above, the obligation to report to the MOKAS includes an attempt to conduct such suspicious transactions. If avoiding the execution of the transaction is impossible or may impede the prosecution of the persons for whom the alleged money laundering or terrorist financing is carried out, the obliged entities should inform MOKAS right after the transaction.

287. The AMLCO must include in the Suspicion Report all relevant information concerning the customer, transactions or activities, according to the information in his/her possession.

288. All Suspicion Reports of the AMLCOs to MOKAS must be submitted according to its instructions, within a reasonable period of time. Obliged entities must implement a system which will allow them to produce these Suspicion Reports in printed form for inspection purposes.

289. After submitting the Suspicion Report, the credit institution may wish to discontinue the relationship with the customer to avoid the risk involved in continuing the operation of that account. In such a case, credit institutions should be particularly attentive so that, in accordance with article 48 of the Law, they do not disclose to the customer that a suspicion report has been submitted to MOKAS. Therefore, there must be close contact with MOKAS to avoid any impediments or difficulties in conducting the investigations.

290. After submitting the Suspicion Report, credit institutions must follow any instructions given by MOKAS, in particular whether they will complete a particular transaction or keep the specific account in operation. It is noted that Article 26(2)(c) of the Law provides the authority to MOKAS to instruct credit institutions not to execute or delay the execution of a customer's order without such action being considered as a violation of any contractual or other obligation of the credit institution and its employees.

291. Furthermore, after submitting a Suspicion Report to MOKAS, the accounts of the customers involved and any other connected accounts should be placed under the close monitoring of the AMLCO.

8. STAFF TRAINING AND EDUCATION

The Law Article 58

292. Article 58 of the Law requires obliged entities to establish adequate and appropriate systems and procedures to inform their employees about:

(i) the systems and procedures under the requirements of article 58(a) – (e) of the Law,

(ii) the Law,

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

(iv) the European Union directives on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and

(v) the relevant requirements for the protection of personal data.

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

293. During the preparation of the annual training plan, credit institutions should take into account the nature and size of their activities as well as the nature and extent of the risks of money laundering and terrorist financing to which they are subject. The relevant information will be obtained from the National Risk Assessment and also from the risk assessment of the institution itself.

294. The Board of Directors and the Senior Management must be informed of their responsibilities under the Law and this Directive as well as the changes and new developments in the legal and regulatory framework. Although the training of Senior Management of the credit institution is not the same as the one offered to the rest of the staff of the institution, the Senior Management must understand the importance of the requirements of the Law and the relevant Directives, the consequences of non-compliance and the risks for the institution. Without a general understanding of the aforementioned requirements, the Board of Directors and the Senior Management will not be able to provide adequate management supervision, approve policies, procedures or provide sufficient resources for the effective prevention of money laundering and terrorist financing.

295. The effectiveness of the procedures and recommendations contained in the Directive and other relevant circulars of the Central Bank of Cyprus concerning money laundering and terrorist financing depends on the extent that the staff of the credit institutions realizes the severity of the facts that led to the enactment of the Law and the extent given to the subject matter by the Board

of Directors and the Senior Management. There is personal legal responsibility of each member of staff as regards omission to disclose information relating to money laundering and terrorist financing in accordance with the internal reporting procedures in force. Therefore, all staff of credit institutions should be encouraged to cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is even the slightest suspicion that they may be related to money laundering or terrorist financing.

296. It is important that credit institutions introduce comprehensive measures to ensure that their staff is fully informed of their duties and responsibilities and obligations under the Law. The duties and responsibilities of the staff should be documented in an easily accessible place so that the staff can refer to them throughout the duration of their employment. In this respect, the AMLCO of the credit institution has the responsibility, in cooperation with other competent departments of the credit institution (e.g. personnel and training departments, etc.) to prepare and apply, on an annual basis, a training programme and education of the Board of Directors and the staff within the framework defined by the Law and the Directive. The AMLCO must monitor and evaluate the adequacy and effectiveness of the seminars and the provided education and training of the staff and inform the Senior Management of any identified weaknesses in the implementation of the staff education and training programme.

297. The AMLCO ensures that the credit institution keeps detailed information for all staff with the training seminars/courses carried out in connection with the prevention of money laundering and terrorist financing, such as:

(i) employee name by branch, by position (managerial staff, officers, newcomers, etc.). The list should include all the staff of the institution even if they did not attend any seminar,

(ii) date of participation in a seminar, title and duration of the seminar as well as the names of trainers,

(iii) whether the lecture/seminar was prepared within the credit institution or offered by an external organisation or consultants, and

(iv) summary information for the programme/content of the lectures/seminars.

298. The time and content of the training of the staff of different departments should be tailored to the needs of the staff and to the risk profile of each credit institution. Moreover, the frequency of the training may vary depending on the amendments to the legal and/or regulatory requirements, the tasks of the staff as well as any other changes in the country's financial system.

299. The training programme should aim at informing staff about new developments in the area of preventing money laundering and terrorist financing, including practical methods and trends

used by criminals for this purpose as well as in the internal measures taken to protect the financial system.

300. The training programme should have a different structure for new staff, customer service personnel, Compliance Unit staff, staff moving from one department to another, or staff involved in attracting new customers, staff of departments engaged in offering specialized services/products such as trade finance, private banking, provision of services to shipping companies, correspondent services to other credit institutions, or any other group of employees required to receive specialised training. New staff should, immediately after their recruitment, be educated on the importance of the policy of preventing money laundering and terrorist financing and the procedures, measures and controls implemented by the credit institution. Customer service personnel should be trained in new customers identification and verification, demonstrating due diligence on an ongoing basis, handling existing customer accounts and detecting types of unusual and suspicious activity. The training should be repeated at regular intervals in order to ensure that staff is reminded of their duties and responsibilities and kept informed of any new developments.

301. It is important that, all directly involved staff fully understands the need and consistently implements the policy and procedures of the credit institution to prevent money laundering and terrorist financing. Therefore, the cultivation and promotion of a culture of understanding the importance of the prevention of money laundering and terrorist financing, is the key to the successful implementation of any policy and procedures.

9. APPLICATION OF THE DIRECTIVE TO BRANCHES AND SUBSIDIARIES OF CREDIT INSTITUTIONS

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

302. Article 68A(1) and (2) of the Law requires that obliged entities belonging to a Group to implement policies and procedures at group level, including data protection policies, as well as the policies and procedures for the exchange of information within the group, for the purpose of preventing money laundering and terrorist financing. In addition, they shall ensure that these policies and procedures are effectively implemented at branches and subsidiaries located in another Member State and in a third country.

The Law Article 2

303. According to article 2 of the Law, a group shall mean a group of undertakings consisting of a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries have a holding, as well as undertakings connected between them in a relation within the meaning of article 22 of Directive 2013/34/EU. The proper management of money laundering and terrorist financing risks, when a bank operates in other jurisdictions, involves examining the legal requirements of the host country. Given the risks, each group should develop policies and procedures to prevent money laundering and terrorist financing at group level which are implemented consistently and supervised within the whole group. In turn, the policies and procedures at the branch or subsidiary level, although reflecting the local business considerations and the requirements of the host jurisdiction, must be compatible and support the broader Group policies and procedures. In cases where the host country's requirements are more stringent than the group's requirements, the group's policy must allow the relevant branch or subsidiary to adopt and apply the local requirements of the host country.

304. Where credit institutions maintain presence in another Member State, they shall ensure that these entities comply with the corresponding legislation of the other Member State.

305. Credit institutions which maintain branches or subsidiaries located in a third country, where minimum requirements for preventing and combating money laundering and the financing of terrorism are less stringent than the requirements of the Cyprus legal and regulatory framework, these branches and subsidiaries apply the requirements laid down in the Law and in the respective Directives and Circulars issued by the Central Bank of Cyprus, to the extent permitted by the legislation of the third country in which they are located.

306. If the legislation of a third country does not permit the application of the aforementioned policies and procedures, the obliged entity which maintains branches and subsidiaries in that third country must immediately inform the Central Bank of Cyprus and take additional measures to effectively address the risk of money laundering or terrorist financing. In addition, the Central Bank of Cyprus carries out additional supervisory actions, including -

(a) demands that the group does not conclude or terminate business relationships and not to execute transactions, and

(b) if necessary, asks the group to terminate its activities in the third country, in case the additional measures which the obliged entities have to take are not sufficient.

307. For each third country, the credit institution as a minimum:

i. assesses the risk of money laundering and terrorist financing arising for their group, records this assessment, keeps it up-to-date and readily available to the competent authority,

ii. ensures that the risk referred to in point (i) is duly reflected in the policies and procedures applicable throughout the group,

iii. obtains approval by a senior management official at group level for the risk assessment referred to in point (i) and for the policies and procedures referred to in point (ii),

iv. provides targeted training to the competent staff members of the third country so that they can identify risk indicators for money laundering and terrorist financing. The credit institution ensures that the training is effective.

308. Article 45(6) of the European Union Directive requires the ESAs to prepare regulatory technical standards defining the type of additional measures referred to in paragraph 306 and also the minimum actions to be carried out by the credit and financial institutions in case the legislation of a third country does not permit the application of the measures required under paragraphs 302 and 305.

309. On 6th December 2017, ESAs submitted to the European Commission regulatory technical standards[11] for approval. These regulatory technical standards define the minimum actions that credit and financial institutions should take in such cases. These standards should be adopted within three months from the date of their approval.

310. Credit institutions with branches or subsidiaries in another Member State or third country should designate the Compliance Officer as coordinator to ensure implementation, by all companies of the group carrying out financial activities, of the Group policy as well as adequate and appropriate systems and procedures for the effective prevention of money

[11] https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries

laundering and terrorist financing. Therefore, the AMLCO should monitor on a ongoing basis compliance with obligations through on-site or offsite audits.

311. The policies and procedures of the credit institution for the exchange of information must include specific provisions obliging branches and subsidiaries to provide the Group AMLCO with information for the purpose of implementing due diligence measures, information about high-risk customers and activities, and more generally the assessment and management of money laundering and terrorist financing risks . Additionally, branches and subsidiaries must respond promptly to requests from the parent credit institution in connection with customer accounts. Also, branches and subsidiaries must submit information and analysis of transactions and activities that appear suspicious or unusual, including the submission of a Suspicious Transaction Report. Similarly, branches and subsidiaries should receive this information when relevant and appropriate for risk management. In relation to the above, there should be adequate safeguards regarding the confidentiality and the use of exchanged information, including the prevention of disclosure of information.

Credit institutions shall determine the purpose and extend of the exchange of information on the basis of the sensitivity of the information and relevance/relation/importance in the management of risks arising from money laundering and terrorist financing.

The Law
Article 49

312. Article 49(1) of the Law states that the prohibition of disclosure of information provided for in article 48 does not prevent disclosure between credit and financial institutions or between such institutions and their branches and majority-owned subsidiaries located in a third country, provided that such branches and subsidiaries comply with the group-wide policies and procedures, including procedures for the exchange of information within the group, in accordance with the provisions of article 68A, and that group policies and procedures meet the requirements laid down in the Directive of the European Union.

313. It is understood that the exchange of information regarding suspicions that the funds are a product of illegal activities or related to the financing of terrorism that are reported to MOKAS are the subject of an exchange within the group, unless MOKAS indicates otherwise.

314. The Group AMLCO, who manages the risk arising from money laundering and terrorist financing, should assess the potential risks arising from the activity reported by branches and subsidiaries of the Group and where necessary assess the risks on the Group by a particular customer or category of customers. The credit institution should have policies and procedures to determine whether other branches or subsidiaries have accounts of the same customer (including any related or connected parties). The credit institution should also have policies and procedures governing account relationships at group level that are considered to be of

higher risk or have been associated with possible suspicious activities, including procedures for escalation and guidance on limiting the activities of these accounts, including the closure of the accounts if deemed necessary. A credit institution's head office should be able to request all their branches and subsidiaries to investigate their records against specific directories or lists of individuals or organizations suspected of helping and assisting in money laundering or terrorist financing and report any matches. The credit institution should be able to inform its supervisory authorities, if requested, of the group's customer risk management process, risk assessment and group-wide policies and procedures for prevention of money laundering and terrorist financing, as well as of the group arrangements for the exchange of information.

10. SUBMISSION OF DATA, INFORMATION AND PRUDENTIAL STATEMENTS TO THE CENTRAL BANK OF CYPRUS

10.1 Submission of data and information

The Law Article 59(9)

315. In accordance with article 59(9) of the Law, the Central Bank of Cyprus may request and collect, from persons subject to its supervision, necessary or useful information for the exercise of its duties and to request within a specified deadline, the provision of information, data and documents. In the event of refusal of any person subject to its supervision to comply with its request for the collection of information within the prescribed deadline or in case it refuses to give any information or demonstrates or furnishes incomplete or false or falsified information, it has the authority to take all or any of the measures referred to in sub-section (6) of article 59 the Law.

10.2 Monthly statement of large cash transactions and funds transfers

316. As of September 1990, all banks in Cyprus submit on a monthly basis a statement of the large cash deposits as well as incoming and outgoing funds' transfers. As of November 2017, following relevant circulars of the Central Bank of Cyprus, the specific statement has been enriched to include cash withdrawals as well as analysis by country and currency of funds' transfers and channels used. The submission of the above monthly statement provides an opportunity to credit institutions to initially assess and subsequently to strengthen their internal control and operations monitoring systems of their with the aim of, in a timely manner, identifying cash transactions and large money remittances that may be unusual and/or which may entail an increased risk of money laundering. The circular letters of the Central Bank dated 3 November 2017 and 3 July 2018 are relevant.

10.3 Monthly statement of customer loans and deposits based on the country of permanent residence of the beneficial owner

317. In accordance with Chapter 3 of this Directive, credit institutions are required to apply appropriate measures and procedures, depending on the degree of risk, to prevent the use of their services for the purpose of money laundering or terrorist financing. It is noted that the risk-based approach includes, inter alia, the identification and assessment of money laundering and terrorist financing risks arising from specific customers, products, services and geographic areas of business of credit institutions and their customers and the management and mitigation of such risks by implementing appropriate and effective policies, procedures and controls.

318. In this regard, as of March 2013, credit institutions are required to submit on a monthly basis data on customer deposits and loans based on the country of permanent residence, irrespective of the nationality or citizenship, of the beneficial owner, as the term is interpreted in article 2 of the Law. It is clarified that, in the case of legal persons/entities belonging to more than one beneficiary, the country of residence of the beneficiary with the highest percentage of ownership should be taken into account. In the case of beneficiaries residing in different countries and owning the same percentage of ownership, the country in which the company or group to which it belongs has a physical presence should be indicated. The monthly statement must be submitted no later than 15 days after the end of the month to which it relates. The circulars of the Central bank dated 5 December 2012, 3 January 2013 and 26 May 2015 are relevant.

10.4 Bi-annual Report (RBA)

319. As of February 2014 credit institutions are required to send to the Central Bank of Cyprus the six-monthly RBA reports. These reports should be sent to the Central Bank of Cyprus by the 15th day of the following month of the reporting period, i.e. until 15/1 and 15/7.

10.5 General Requirements

320. In order to achieve the above, the Central Bank of Cyprus requires all credit institutions to adapt their automated software systems to enable the submission of accurate and complete data in these reports thereby improving the ability of credit institutions to identify and monitor transactions deemed to involve a greater risk of money laundering and terrorist financing.

321. The AMLCO should confirm the accuracy of the data sent to the Central Bank of Cyprus, evaluate them and, where appropriate, investigate any trends which may indicate risks of involvement in transactions of money laundering or terrorist financing and ensure that he/she is ready to answer questions posed by the Central Bank of Cyprus.

11. REPEAL AND CANCELLATION OF PREVIOUS CIRCULAR, DIRECTIVES AND AMENDMENTS

322. The following that have been issued at different times by the Central Bank of Cyprus are revoked and cancelled:

A) Directive to credit institutions for the prevention of money laundering and terrorist financing of December 2013 and its subsequent amendments issued by the Central Bank of Cyprus in accordance with article 59(4) of the "Prevention and Suppression of Money Laundering Activities Law", and

B) The circular letter dated 2 November 2018, entitled "Shell companies/entities".

APPENDICES

APPENDIX 1

INTERNAL MONEY LAUNDERING SUSPICION REPORT

REPORTER

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

CUSTOMER

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

INFORMATION/SUSPICION

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

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

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

FOR MONEY LAUNDERING COMPLIANCE OFFICER'S USE

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

APPENDIX 2

ANTI-MONEY LAUNDERING COMPLIANCE OFFICER'S

INTERNAL EVALUATION REPORT

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

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

ENQUIRIES UNDERTAKEN (Brief description)

.....

.....

.....

DOCUMENTS RESEARCHED/ATTACHED

.....

.....

.....

DECISION OF THE AMLCO

.....

.....

.....

FILE REFERENCE.....

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

APPENDIX 3

Documents for identification of specific categories of natural persons falling within the scope of the Law N. 64(I)/2017

APPENDIX 3A

APPENDIX 3B

APPENDIX 3C

APPENDIX 3D

APPENDIX 3E

APPENDIX 3F

APPENDIX 3G

APPENDIX 3H

APPENDIX 3I

APPENDIX 4

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

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 size of customer's activities.

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

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

(v) Cash transactions involving large rounded amounts.

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

(vii) Unusually large cash deposits made to the account of an individual or company whose business activities would normally be operated 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 using numerous deposit slips in such a way that each individual deposit is not noticeable, but the total of the above deposits is important.

(x) Accounts of companies of which almost all transactions, both deposits and withdrawals, are made in cash as opposed to other forms of debit or credit normally used in connection with commercial activities (e.g. issuance of cheques, issuing letter of credit, electronic remittances, etc.).

(xi) Customers who deposit cash and then request the issuing of bankers' draft or transfer of funds or the acquisition of various negotiable and highly liquid means of payment.

(xii) Customers requesting the exchange of large quantities of low-denomination banknotes with other high-denomination banknotes.

(xiii) Frequent conversions of cash from one currency to another.

(xiv) Branches with much greater than the regular number of cash transactions (the statistics of a credit institution's head office must be used to detect such large cash transactions).

(xv) Customers whose deposits contain counterfeit banknotes or falsified means of payment.

(xvi) Customers transferring large amounts of money to or from abroad, with further instructions for paying other persons in cash.

(xvii) Large cash deposits using overnight safe-keeping facilities, systematically avoiding direct contact with the credit institution.

(xviii) The purchase or sale of foreign currencies in large quantities with cash settlement, despite the customer's account held with the credit institution.

(xix) Numerous deposits of small amounts in various branches of the same credit institution or by a group of people entering the same branch simultaneously. Money is then often transferred to another account, usually in another country.

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

(i) The use of accounts in the name of proxies, trusts or client accounts in the name of professionals without appearing or needing to do so or not in line with the activities of the account holder.

(ii) Claims for a refund with the excuse that they were accidentally sent to the account.

(iii) Multiple transactions are carried out in one day at the same branch but with an obvious attempt to use a different customer service officer.

(iv) Customers who maintain multiple accounts and carry out separate cash deposits in each of them and where the total of the various credit transactions is large.

(v) Any person or company whose account is not particularly moving for personal or professional activities, but is used only for receipts or payments of large amounts which have no apparent purpose or relationship with the account owner and/or his/her business (e.g. significant or unusual increase in account transactions).

(vi) Customers who maintain accounts with different credit institutions in the same geographic area, in particular when the credit institution is aware that the balances of the accounts are consolidated before any transfer of money orders.

(vii) Payments that are evidently derived from deposits made in cash the same or the previous day.

(viii) High value deposits of third-party cheques incompatible with the movement of the account.

(ix) Accounts to which money is deposited on a periodic basis and remain inactive 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 a group of customers. The use of sealed packets deposited and withdrawn.

(xii) Contact with companies' representatives who seem to avoid direct contact with the credit institution.

(xiii) Customers who refuse to provide information that under normal circumstances would make the customer eligible for significant credit facilities or for other banking services.

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

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

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

(i) Purchasing of securities on behalf of the customer which are to be held by the credit institution in safe custody, where this does not appear to be the most appropriate arrangement given the customer's personal circumstances.

(ii) Deposits/loans from/to subsidiaries 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 funds is unclear or not consistent with the customer's apparent standing or needs as known by the credit institution.

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

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

4. Funds transfers/international transactions

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

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

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

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

(v) Electronic incoming funds and simultaneously outgoing transfers by customers without these transactions going through a specific account.

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

(vii) Frequent deposits of travellers' cheques and foreign currency drafts from abroad.

(viii) Numerous incoming funds transfers received in a specific account where each transfer is below the reporting requirement in the remitting country.

(ix) Funds transfers to/from a high risk country without an apparent business reason or when it is inconsistent with the customer's business or other customer details.

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

(xi) Funds transfers to or from 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 either in total or the biggest part is almost immediately transferred to another country in a manner which is inconsistent with the specific customer's business activities or history.

(xiii) Large incoming funds transfers from a customer residing abroad, with no apparent reason.

(xiv) Wire funds transfers which are unexplained, repetitive, or show unusual patterns. Payments or receipts with no apparent links to legitimate contracts, goods, or services.

5. Correspondent accounts

(i) Wire funds transfers of large amounts, where the correspondent account has not previously been used for similar transfers.

(ii) The routing of transactions from the bank that holds the correspondent account in various countries and/or financial institutions prior to or following the crediting of the account without any apparent purpose other than to disguise the nature, source, ownership or control of the funds.

(iii) Frequent or numerous funds transfers to or from the correspondent account held by the foreign bank originating from or going to a country which does not apply or which applies inadequately FATF's recommendations on money laundering prevention.

6. Secured and unsecured lending

(i) Customers who repay problematic loans unexpectedly.

(ii) Requests to borrow against assets (i.e. a security or a guarantee), held by third persons where the primary origin of the assets is not known or when the assets offered as collateral for a loan are inconsistent with the customer's economic standing.

(iii) Request by a customer for securing or settlement of a credit liability where the source of the customer's financial contribution from own funds to the whole of the facility is unclear, particularly when immovable property is involved.

7. Customers who provide insufficient or suspicious information

(i) A customer who is reluctant to provide complete information when opening an account about the nature and purpose of his/hers business activities, anticipated account turnover, previous relationships with credit institutions, names of directors and managers, or information about the business address. The customer usually provides minimal or misleading information that is difficult or expensive for the credit institution to verify.

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

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

(iv) A customer effects frequent or large transactions with no records of past or recent professional experience.

8. Activities which are inconsistent with the customer's economic profile

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

(ii) Unnecessarily complex transaction compared to its commercial purpose.

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

(iv) The types of transactions of the business indicate a sudden change which is inconsistent with the normal activities of the customer.

(v) A large volume of bankers drafts, money orders, and/or funds transfers credited or purchased through an account when the nature of the customer's business activities would not appear to justify such activity.

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

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

9. Characteristics of the customers and of their business activities

(i) Shared address for individuals involved in cash transactions, particularly when the address is a business location and/or does not seem to be connected to a specific professional activity (e.g. student, unemployed, self-employed, etc).

(ii) The stated occupation of the customer is not commensurate with the level or type of activity (e.g. a student or an unemployed individual who receives or sends large numbers of funds transfers or withdraws cash daily at different locations over a wide geographic area).

(iii) Financial transactions by non-profit or charitable organisations for which there appears to be no logical financial purpose or link with the activity of the organisation and the other parties in the transaction.

(iv) A safe deposit box use by a commercial business when the business activity of the customer is unknown or the nature of its activities does not appear to justify the use of a safe deposit box.

(v) Unexplained inconsistencies arising during the identification and verification of the customer's identity (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents issued to verify the name, address and date of birth).

10. <u>Transactions by employees or agents or trustees</u>

(i) Changes in the lifestyle of employees, e.g. luxurious way of life or avoiding absenteeism for holidays.

(ii) Changes in the performance, behaviour of employees.

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

(iv) Customers who always insist to transact with the same employee even if these are routine transactions or who stop transacting with the credit institution at the period which the specific employee is absent.

(v) Complex trust or proxies structure.

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

(vii) Trustee's uunwillingness to keep the necessary information or exercise the necessary control required for the proper discharge of his/her duties.

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

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

B) TERRORIST FINANCING

1. Sources and methods

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

- Collection of membership subscriptions
- Sale of books and other publications
- Cultural and social events
- Donations
- Community solicitations and fund raising appeals from society

Funds originating from illegal sources are laundered by terrorist groups via 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, purchase of monetary instruments (bankers draft, traveller cheques), use of credit and debit cards, wire funds transfers using "straw men" or false identities or companies without physical presence or proxies (nominees) from the close family environment, 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 specific purpose which is used to channel funds to a terrorist group.
- Terrorists infiltrate a non-profit organisation with a legitimate humanitarian or charitable mission to divert funds collected for an ostensibly legitimate purpose for the support of a terrorist group.

- The non-profit organisation serves as an intermediary or cover for the movement of funds internationally.

- The non-profit organisation provides administrative support to the activities of terrorist groups.

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

- Inconsistencies between the apparent sources and amounts raised or handled.

- A mis-match between the type and size of financial transactions and the stated mission of the non-profit organisation.

- A sudden increase in the frequency and size of financial transactions of a non-profit organisation.

- Large and unexplained cash transactions.

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