CYPRUS GAMING + CASINO SUPERVISION COMMISSION
ΑΡΧΗ ΠΑΙΓΝΙΩΝ + ΕΠΟΠΤΕΙΑΣ ΚΑΖΙΝΟΥ ΚΥΠΡΟΥ
Κυπριακή Δημοκρατία
Republic of Cyprus

CYPRUS GAMING AND CASINO SUPERVISION COMMISSION

DIRECTION ISSUED PURSUANT TO ARTICLE 59(4) OF THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES LAWS OF 2007 TO 2019 (188(I)/2007) AND REGULATION 18(3) OF CASINO OPERATIONS AND CONTROL LAW (GENERAL) REGULATIONS 2016 (R. 97/2016).

Version 0.1

19 November 2019

Table of Contents

DEFINITIONS

“AMLCO” means the Anti-Money Laundering Compliance Officer of the Operator.

“AML/CFT” means Anti-Money Laundering and Combating the Financing of Terrorism.

“Board of Directors/Board” means the Board of Directors of the Operator.

"Business relationship" means business, professional or commercial relationship between the customer and the Operator, which is linked to the professional activities of the Operator and that the Operator expects, at the time of its establishment, to have certain duration.

“Casino Operator” or “Operator” means a person holding the integrated casino resort license and is licensed to operate the temporary, satellite casinos and integrated casino resort in the Republic of Cyprus.

“Customer” means a person that establishes a business relationship or performs an occasional transaction with the Operator.

“Person” means both natural person and legal entity.

“The Commission” means the Cyprus Gaming and Casino Supervision Commission.

“EU Directive” means 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 purpose of Money Laundering and Terrorist Financing.

"High-risk third country" means a third country, which is flagged by the European Commission under the provisions of paragraph (2) of Article 9 of the EU Directive by means of delegated powers, and which has strategic deficiencies in its national AML/CFT regime that pose significant threats to the financial system of the Union, and a third country which is classified by the Operator as high risk, according to the risk assessment referred to in Article 58a of the Law.

“The Law” or “AML Law” means the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2019 (L.188 (I)/2007).

“Junket Operator” has a meaning given to this term by the Casino Operations and Control Law of 2015 (L. 124(I)/2015).

“MOKAS” means the Unit for Combating Money Laundering of the Republic of Cyprus.

"Occasional transaction" means any transaction other than a transaction which takes place during a business relationship.

"PEP" means a Politically Exposed Person as defined in the AML Law.

"Senior Management" means an officer or employee of the Operator with sufficient knowledge of the Operator's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure and need not to be a member of the board of directors.

"Regulation(s)" means the Casino Operations and Control (General) Regulations 2016 (R. 97/2016).

INTRODUCTION

1. In 1992 the Republic of Cyprus enacted the first law by which money laundering deriving from drug trafficking was criminalised. Furthermore, in 1996 the Prevention and Suppression of Money Laundering Activities Law (Law) was enacted, defining and criminalising money laundering deriving from all serious criminal offences. The Law was subsequently amended to adopt new international initiatives and standards in the area of money laundering, including the Second European Union Directive for the prevention of the use of the financial system for the purpose of money laundering (Directive 91/308/EEC).

2. In December 2007, the House of Representatives enacted the Prevention and Suppression of Money Laundering Activities Law by which the former Laws on the prevention and suppression of money laundering activities of 1996-2004 were consolidated, revised and repealed. Cyprus legislation was thereby 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). In the period between 2010 and 2016, the Law was further amended several times with the purpose of further harmonization with international initiatives and standards.

3. The last amendments in April 2018 and May 2019 had the purpose of harmonization with the Fourth European Union Directive on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing (Directive (EU) 2015/849). The EU Directive 2015/849 sets out a framework which is designed to protect the European financial system against the risks of money laundering and terrorist financing and is, to a large extent, based on the international standards adopted by the Financial Action Task Force (FATF). It requires EU member states to prohibit money laundering and to oblige the financial sector and a wide range of non-financial businesses and professions (including casinos), to identify their customers, keep appropriate records, establish internal procedures, to train staff

and guard against money laundering, and to report indications of money laundering to the competent authorities.

4. This Direction is issued in accordance with Article 59(4) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2019 and Regulation 18 (3) of the Casino Operations and Control (General) Regulations of 2016. It aims to lay down the specific policy, procedures and control systems that the Operator should implement for the effective prevention of money laundering and terrorist financing so as to achieve full compliance with the requirements of the Law.

5. It is emphasized that the Law explicitly states that Directions are binding and compulsory to all persons to whom they are addressed. Furthermore, the Law assigns to the supervisory authorities, including the Cyprus Gaming and Casino Supervision Commission, the duty of monitoring, evaluating and supervising the implementation of the Law and of the Directions issued to the supervised entities.

6. It should also be noted that section 6, **Financial Sanctions** is issued in accordance with the Article 3(2) of the Implementation of Provisions of the United Nations Security Council's Resolutions and Decisions (Sanctions) and Decisions and Regulations of the Council of the European Union (Restrictive Measures) Law of 2016 (58 (I)/2016) with the aim of laying down the control systems, policies and procedures that the Operator should establish in order to achieve compliance with financial sanctions legislation.

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

Risk based approach

Article 58 and 58A of the Law

7. Article 58(d) and Article 58A of the Law require the obliged entities (i.e. the Operator) to identify and assess money laundering and terrorist financing risks, and to establish and maintain proportionate policies, procedures and controls to mitigate and effectively manage the identified risks.

8. A risk-based approach to AML/CFT means that the Operator is expected to identify, assess and understand the money laundering and terrorist financing risks to which it is exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively. The risk-based approach starts with the identification, recording and assessment of the risk that has to be managed. The Operator needs to assess and evaluate the risk of how

it might be potentially exposed or vulnerable through the use of its services by criminals for the purpose of money laundering and terrorist financing.

9. The risk-based approach involves a number of steps in assessing the most effective way to manage and mitigate the money laundering and terrorist financing risks faced. These steps require the Operator to:

(a) identify the money laundering and terrorist financing risks that are relevant to the Operator

(b) design and implement appropriate policies, procedures and controls to manage and mitigate these risks

(c) monitor the effectiveness of implemented controls and improve them if needed

(d) document what has been done, and why.

10. The Operator should risk assess its business activity (Business Wide Risk Assessment) and the risk to which it is exposed as a result of business relationships or occasional transactions (Customer Risk Assessment). The Business Wide Risk Assessment is necessary for the Operator to understand the overall exposure of its business to money laundering/terrorist financing and to identify areas of business it needs to prioritise in the fight against money laundering and terrorist financing. The Customer Risk Assessment is necessary to understand its money laundering and terrorist financing risk exposure that is a result of a business relationship or occasional transaction.

11. The Operator should always identify and assess the money laundering and terrorist financing risks associated with the following groups of risk factors *as a minimum*:

(a) products, services and transactions it offers

(b) countries or geographic areas

(c) the customers it attracts and

(d) delivery channels it uses to service its customers.

Business Wide Risk Assessment

12. The steps taken for identification and assessment of money laundering and terrorist financing risk must be proportionate to the nature and size of the Operator. In this regard, the Operator must:

(a) keep an up-to-date record in writing of all the steps taken to identify and assess the money laundering and terrorist financing risks to which its business is exposed

(b) provide the written risk assessment it has prepared and the information on which it was based to the Commission on request.

13. The Business Wide Risk Assessment must be reviewed and updated at least annually and every time that there is a material change influencing the Operator's business – e.g. changes in regulation, introduction of new products/services, new technology, delivery channels etc.

14. The Business Wide Risk Assessment should be signed-off at the Board level and needs to be kept up to date. Once the Business Wide Risk Assessment has been completed, the Operator should be in the position to set a "risk-appetite" which means that the Operator decides the level of risk it is prepared to accept.

Customer Risk Assessment

15. Customer Risk Assessment should be completed in the context of a business relationship or occasional transaction and lead to categorization of customers and occasional transactions as low, medium or high risk.

16. The assessments of risk should be based on criteria that reflect the causes of risk and should be documented properly. Each category of risk should be accompanied by corresponding Customer Due Diligence measures, periodic monitoring and controls. A Customer Risk Assessment for every business relationship and occasional transactions should be documented accordingly and the Operator should be able to provide the Commission with evidence that its Customer Due Diligence measures are commensurate with the risk level.

Customer risk factors

17. When identifying the risk associated with its customers, including its customers' beneficial owners, the Operator should consider the risks related to:

(a) the customer's and (where appropriate) the customer's beneficial owner's business or professional activity in whatever country they are associated with

(b) the customer's and (where appropriate) the customer's beneficial owner's reputation in whatever country they are associated with and

(c) the customer's and (where appropriate) the customer's beneficial owner's nature and behaviour in whatever country they are associated with.

Country/geographic risk factors

18. Some countries pose inherently higher money laundering and terrorist financing risk than others. The Operator should utilise a variety of credible sources to determine a level of

money laundering and terrorist financing risk related to a specific country. In this regard, the Operator needs to take into consideration as a minimum the risk factors provided in the Law and any Guidelines issued by the Commission.

19. When identifying the geographic risk associated with countries and geographical areas related to a particular customer, the Operator should consider the risk related to:

(a) the jurisdictions in which the customer and any beneficial owner are based

(b) the jurisdictions that are the customer's and any beneficial owner's main places of business

(c) the jurisdictions to which the customer and any beneficial owner have relevant personal links.

20. When assessing country/geographic risk the Operator should as a minimum consider any association with financial sanctions orders, quality of controls, terrorism risk and levels of corruption or other criminal activity related to the country/geographic area.

Products, services and transactions risk factors

21. When identifying the risk associated with its products provided, services or transactions, the Operator should consider the risks related to:

(a) the level of transparency, or opaqueness, the product, service or transaction affords

(b) the complexity of the product, service or transaction and

(c) the value or size of the product, service or transaction.

Delivery channel risk factors

22. When identifying the risk associated with the way in which the customer obtains the Operator's products or services, the Operator should consider the risks related to:

(a) the extent to which the business relationship is conducted on a non-face-to-face basis

(b) any introducers or intermediaries the Operator might use and the nature of their relationship with the Operator.

RISK MANAGEMENT

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

Article 58, 58C and 58D of the Law

23. Regulation 18 of Casino Operations and Control (General) Regulations of 2016 introduces the obligation to the Operator to establish and maintain an anti- money laundering and terrorist financing (AML/CFT) programme. Furthermore, the Article 58(d) and Article 58A of the Law require the obliged entities, including the casinos, to establish and maintain proportionate policies, procedures and controls to mitigate and effectively manage the identified risks. Therefore, the Operator is required to establish a risk-based AML/CFT programme that contains policies, procedures and controls to effectively mitigate and manage its identified money laundering and terrorist financing risks.

24. This should inter alia include:

(a) customer identification and Customer Due Diligence measures

(b) record-keeping arrangements

(c) internal reporting and reporting arrangements to MOKAS

(d) internal control, risk assessment and risk management arrangements to prevent money laundering and terrorist financing

(e) detailed examination of each transaction which by its nature may be considered particularly vulnerable to association with money laundering or terrorist financing, in particular; complex or unusually large transactions and all other unusual patterns of transactions which have no apparent rationale, economic or visible lawful purpose

(f) risk management practices

(g) compliance management arrangements

(h) the recruitment and evaluation of the integrity of the employees.

25. The Operator also has the obligation to inform its employees in relation to:

(a) the systems and procedures it has established in accordance with Article 58 of the Law

(b) the AML Law

(c) the Directions issued by the Commission

(d) the European Union's Directives on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

(e) relevant data protection requirements.

26. The Operator's policies, procedures and controls must be:

(a) proportionate regarding the size and nature of the Operator's business

(b) approved by Operator's Senior Management.

Responsibility for addressing risk

27. The Operator's Board of Directors and Senior Management bear the final responsibility for ensuring that it applies an effective system to prevent money laundering and terrorist financing as well as responsibility for creating the culture of compliance. 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 Operator being used for money laundering and terrorist financing.

28. The commitment of Senior Management from all relevant areas of the Operator's business to the implementation of the AML/CFT measures is a key element for the design and implementation of a risk-based approach as well as active cooperation of all relevant employees. Senior Management must be fully engaged in the processes of the Operator's assessment of risks of money laundering and terrorist financing and be involved in decision making to develop and implement the Operator's policies and processes to comply with the Law. The Board of Directors has overall accountability for overseeing the AML/CFT risk management program and Senior Management's implementation of the AML/CFT program.

29. The Article 58D of the Law requires that the Operator appoint a competent member of the Board of Directors, to be personally responsible for the implementation of the provisions of the Law and relevant AML/CFT Directives and/or circulars and/or regulations, including any relevant acts, Directives and Regulations of the European Union.

30. The specific duties and responsibilities of the director appointed under Article 58D as responsible for AML/CFT matters need to be recorded in the Board of Directors corporate governance or operating procedures and be approved by the Board of Directors.

31. It is required that the Operator's responsible director will be the Board level executive responsible for the Operator's compliance with the Law, this Direction, any applicable acts, Directives and Regulations of the European Union and direction and the effectiveness of Operator's risk management arrangements. They will be responsible for the supervision of the

Anti-money Laundering Compliance Officer (AMLCO) and the implementation of the Law and Directions as well as any other applicable regulations.

32. Persons nominated for appointment as responsible executive, must submit a Casino Key Employee License Application form and any additional information and documents that may be requested by the Commission from time to time. The Operator must, within 14 days of the appointment, inform the Commission of the identity of the individual appointed under the Article 58D, and any subsequent appointments or changes to that position.

33. Article 58C of the Law provides that the Senior Management of the Operator shall approve the policies, procedures and controls applied by the Operator in relation to money laundering and terrorist financing, shall monitor and, where appropriate, strengthen the measures taken.

34. The Operator is required to establish the following measures, procedures and controls:

(a) The Board of Directors will define, record and approve the general principles of the Operator'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 recorded and clear message in relation to the risk appetite, which will determine the expectations, parameters and limits of operation of the program and the Operator's commitment to combatting money laundering and terrorist financing.

(b) The Board of Directors should give leadership by expressing the Operator's values and corporate compliance culture ensuring that its AML program behaviour reflects these values.

(c) The Board of Directors and the Senior Management should have knowledge of the level of risk of money laundering and terrorist financing that the Operator is exposed to, so as to decide whether all necessary measures are being taken for its management, according to its risk appetite.

(d) The Board of Directors designates an experienced person to the position of the AMLCO and ensures that the AMLCO and assistants have, and continually acquire the required knowledge and skills for their roles.

(e) There needs to be clear access and reporting mechanisms between the responsible executive and AMLCO for escalated incidents and monitoring the activity to manage money laundering and terrorist financing risk.

(f) The AMLCO should have sufficient resources to undertake their duties. This includes but is not limited to, competent staff, technological and equipment, and access to responsible executive(s) for the effective discharge of their duties. The AMLCO (and assistants) and any other person assigned with the duty of implementing or reviewing the programme and procedures for the prevention of money laundering and terrorist financing should have complete and timely access to all relevant data and information concerning customers' identity, transactions and other information maintained by the Operator so as to be effective in their duties.

(g) The Board of Directors and Senior Management shall ensure that policies, procedures and measures are applied across the Operator business activities so as the risk of money laundering and terrorist financing is identified, assessed and managed during the day-to-day operations of the Operator and in relation to:

(i) The development or introduction of new products, services, new business practices, including new delivery channels (including premises), new financial management arrangements, including contracts with affiliates or associates,

(ii) The use of new or developing technologies relating changes in existing products or their delivery, and

(iii) Possible changes in the business model /profile of the Operator.

Risk assessments should take place prior to the launch of the new/ changed products, business practices or the use of new or developing technologies.

(h) The Board of Directors and Senior Management shall ensure that proper governance arrangements, reporting and information management arrangements for managing money laundering and terrorist financing risk are in place and are based on the three lines of defence model with clear definition of the responsibilities of each department involved in the prevention of money laundering and terrorist financing.

(i) The ability to make proper decisions will be weakened by unclear information management arrangements or poor data quality. The Operator must ensure that its programme includes effective information management arrangements and arrangements to ensure data quality standards are maintained. Roles and responsibilities relating to data quality should be clearly defined and well organised. Data and information collected to meet the requirements of the Law

and this Direction and the Operator's program should be accurate, easy to retrieve and retained in line with the requirements defined by the Law and this Direction.

(j) The AMLCO is responsible in cooperation with other departments 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 and to ensure that the internal practices, procedures and controls are appropriately documented.

(k) The responsible director and Senior Management shall approve the AML/CFT policies and procedures and ensure this is effectively communicated to all managers and employees that manage, monitor or control the customers' transactions with responsibility for the application of the practices, measures and procedures determined.

(l) The Board of Directors shall assess and approve the AMLCO's Annual Report and shall take all actions as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report.

(m) The Board of Directors and Senior Management shall ensure that all requirements of the Law and Commission Directions are applied and that the Operator is able to assure the Commission with evidence that appropriate, effective and sufficient systems and controls are present for achieving the identification and management of money laundering and terrorist financing risk.

(n) All employees should be made aware of the person appointed as the AMLCO (and alternates/assistants) to whom they shall report information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing.

(o) The Board of Directors and Senior Management shall receive sufficient, regular and objective information to have an accurate picture of the money laundering/terrorist financing risk to which the Operator is exposed.

(p) The Board of Directors and Senior Management shall receive sufficient and objective information from the AMLCO and Internal Audit regarding the effectiveness of the measures and controls against money laundering and terrorist financing.

(q) All relevant employees shall receive sufficient training related to AML/CFT matters

necessary for performance of their roles at the Operator.

(r) The Operator shall apply explicit procedures and standards of recruitment and evaluation of the employees' integrity (existing and new recruits).

Role of the Anti-Money Laundering Compliance Officer

Appointment of Anti-Money Laundering Compliance Officer ("AMLCO")

Article 69 of the Law

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

(a) Appoint as the Anti-money Laundering Compliance Officer (AMLCO) a senior staff member who has the relevant skills, knowledge and expertise, to whom to report any information or other matter which comes to their attention and which, in their opinion proves or creates suspicion that another person is engaged in money laundering or terrorist financing.

(b) Require that any report be considered by the AMLCO in the context of all relevant information, to determine whether or not the information or other matter in the report proves this a fact or creates suspicion.

(c) Allow the AMLCO in line with the paragraph (b) above, to have direct and timely access to any information, records and documents which may be of assistance to him/her and which is available to the Operator and

(d) In case where they know or have reasonable suspicion that funds, irrespective of their amount, are revenue from illicit activities or related to the financing of terrorism, ensure that the Unit for Combating Money Laundering ("MOKAS") is immediately informed, at their own initiative, by the AMLCO referred to in paragraph (a), by submitting a relevant report and providing further information at the request of MOKAS.

36. The Law explicitly provides for the obligation to report to MOKAS any attempt to execute suspicious transactions.

37. The AMLCO should be appointed by the Board of Directors, after having been licensed to perform the role by the Commission. The Commission reserves the right to request his/her substitution if, in its opinion, he/she is no longer "fit and proper" to perform his/her duties. Additionally, the casino Operator should also appoint an Alternate AMLCO who should assist the AMLCO in performance of his/her duties and deputize for the AMLCO in case of absence.

38. The AMLCO should act independently and autonomously to perform their duties and possess the appropriate seniority so as to command the necessary authority. In order to ensure their impartial judgement, the AMLCO should not, for example, have business responsibilities or undertake responsibilities for the data protection framework or the operation of internal audit.

39. Persons nominated for appointment as AMLCO or assistant AMLCO, must submit a Casino Key Employee License Application form, which includes information regarding the person's career, including the qualifications held and work experience, as well as details of any sanctions or criminal convictions against the person and any additional information and documents that may be requested by the Commission from time to time.

40. In case of change of the AMLCO and assistant, the Operator needs to inform the Commission in writing within a period of 14 days about such change, providing explanation as to reasons for a change and the details of the new proposed candidate for the AMLCO or assistant AMLCO position.

Duties of the AMLCO

41. The role and responsibilities of the AMLCO and the Alternate AMLCO should be clearly specified by the casino Operator and documented in the relevant internal procedures and personal contract(s) of the individual(s).

42. Furthermore, the Operator's Compliance department should maintain a procedures manual for all AMLCO's tasks/responsibilities.

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

(a) The AMLCO has the responsibility, to record and assess on an annual basis all risks arising from existing and new customers, products and services as well as the measures or changes to the systems and procedures implemented by the Operator for the effective management of the aforesaid risks. This report (Business Wide Risk Assessment) should be submitted to the Board of Directors for consideration and approval, and the AMLCO is required to report to the Board of Directors and Senior Management of any change in these risks on an on-going basis. A copy of the Business Wide Risk Assessment and AMLCO's Annual report should be submitted to the Commission.

(b) The AMLCO shall prepare the AMLCO's Annual Report in line with the requirements of this Direction.

(c) The AMLCO is responsible in cooperation with other Operator departments for

designing policies, procedures and controls relevant to the prevention of money laundering and terrorist financing as required by the Law, this Direction and any other relevant regulations. This should include the clear definition of responsibilities and limits of responsibility of each department that is identified within the AML/CFT program and ensure that the internal practices, procedures and controls are appropriately documented.

(d) The AMLCO shall develop and establish the Operator's Customer Due Diligence capabilities and procedures including Customer Risk Assessment methodology which are submitted to the Board of Directors for consideration and approval.

(e) The AMLCO shall monitor and assess whether the policies, procedures and controls that have been introduced for the prevention of money laundering and terrorist financing are correctly and effectively applied. In this regard, the AMLCO should apply appropriate monitoring mechanisms (e.g. on-site visits to different departments/premises of the Operator) which will provide him/her with the necessary information for assessing the level of compliance with the procedures and controls currently in force. The AMLCO should regularly inform the Board of Directors and Senior Management regarding the findings of these audits and the level of compliance.

(f) The AMLCO shall ensure that the Operator prepares and maintains records of customers categorized following the risk-based approach into low, medium or high category and which should contain the information prescribed by the Law and this Direction.

(g) The AMLCO shall maintain a register of all cases of persons (prospective customers) for which the Operator declined the establishment of business relationship and/or terminated the business relationship for compliance reasons.

(h) The AMLCO shall verify that the third party with which the Operator intends to cooperate on Customer Due Diligence issues meets the requirements stipulated in the Law and this Direction and gives his/her written consent for the cooperation which should be duly justified and kept in the file of the third party. The AMLCO shall also evaluate the quality of customers recommended by third party.

(i) The AMLCO shall receive information from the Operator's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information shall

be received in a written report form (referred to as "Internal Suspicion Report"). All such reports should be registered and kept in a secure separate file.

(j) The AMLCO shall evaluate and examine the information received in the Internal Suspicion Report (ISR) by reference to other relevant available information and review the circumstances with the reporting employee and, where appropriate, their superiors. The evaluation of the ISR shall be completed as a separate written report (to be referred to as "Internal Evaluation Report") which will be documented and kept in a secure separate file.

(k) If as a result of completing the Internal Evaluation Report (IER), the AMLCO decides to notify MOKAS, then they shall complete a written report and submit it to MOKAS the soonest possible in the way and form prescribed by MOKAS. All such reports should be registered and kept in a secure separate file.

(l) Following submission of an AMLCO's report to MOKAS, the transactions of the customer(s) involved and related accounts shall be monitored by the AMLCO. Following any directions from MOKAS, the AMLCO shall investigate and examine all transactions. The conclusions of AMLCO monitoring and investigations should be accurately documented and kept in secure file.

(m) If following the evaluation and completion of the IER, the AMLCO decides not to notify MOKAS then they must fully document the reasons for the decision including all the steps and analysis that were performed during the course of the AML investigation. This will be recorded on the "Internal Evaluation Report" which should, be registered and securely retained.

(n) The AMLCO shall maintain a registry for ISRs, IERs and MOKAS reports with relevant management information (e.g. unit submitted the report, date of submission of the internal report, date of assessment, date of reporting to MOKAS).

(o) The AMLCO shall act as a first point of contact with MOKAS, for all operational matters. The AMLCO shall respond to requests from MOKAS and provide all the supplementary information requested and fully co-operate with MOKAS. The AMLCO shall respond to all requests and queries from MOKAS and the Commission, provide all requested information and fully cooperate with MOKAS and the Commission.

(p) The AMLCO is generally responsible for the timely and accurate submission of

reports to the Commission prescribed as necessary by this Direction or required to support investigations enquiries. The AMLCO shall respond promptly to any queries or clarifications requested by the Commission.

(q) The AMLCO shall maintain records for a period of five years after the termination of business relationship with the third party with the data/information of the third person as prescribed in section Reliance on third parties of this Direction.

(r) The AMLCO shall receive or suggest, depending on the case, corrective measures on issues related to the prevention and suppression of money laundering and terrorist financing in accordance with the findings of any Commission investigation.

(s) The AMLCO shall take or suggest, where appropriate, corrective measures regarding the matters related to prevention of money laundering and terrorist financing in line with the findings of any audit conclusions of the Commission.

(t) The AMLCO shall evaluate the findings of the Internal Audit regarding the taking of corrective measures on issues related to the prevention and suppression of money laundering and terrorist financing.

(u) The AMLCO shall provide advice and guidance to the employees of the Operator on matters related to prevention of money laundering and terrorist financing.

(v) The AMLCO shall monitor and determine the Operator's departments and employees need for training and education and organize appropriate training sessions/seminars. In this regard, the AMLCO shall prepare and apply an annual staff training program which must include mandatory testing of employee's knowledge of AML/CFT matters.

(w) The AMLCO shall ensure that the records in relation to the seminars and other training of the Operator's employees are kept and to assesses the adequacy of the education/training provided. Such records shall include:

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

  (ii) Date of the seminar, title, duration, names of lecturers

  (iii) Whether the lecture/seminar was organized internally or offered by an external organization or consultants

  (iv) Results of AML/CFT testing.

AMLCO's Annual Report

44. The AMLCO shall prepare an Annual Report which will assess the Operator's level of compliance with its obligations laid down in the Law, relevant regulatory framework and its program for the prevention of money laundering and terrorist financing.

45. The AMLCO's Annual Report should be prepared within two months from the end of each calendar year (i.e. by the end of February, the latest) and should be submitted for consideration and approval to the Board of Directors.

46. The Board of Directors shall evaluate and adopt the Annual Report. The Senior Management of the Operator shall then ensure the prompt and effective application of all appropriate measures to correct any shortcomings and/or omissions identified in the Report.

47. A copy of the Annual Report submitted to the Board of Directors shall also be forwarded at the same time to the Commission. Copies of the meeting minutes within which Board of Directors considered the Annual Report approval should be submitted to the Commission immediately after that meeting.

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

(a) Description of the business operations/model of Operator during the last year, identifying the products/services offered, number and size of premises, changes to the operations and/or structure and the introduction of new products, services, technological developments that affected the procedures and controls for money laundering/terrorist financing.

(b) Information on measures taken and/or procedures introduced to comply with any amendments to the Law and AML regulatory requirements which took place during the year.

(c) Information as to the inspections and reviews performed by the AMLCO, the Internal Audit and independent third parties, identifying material deficiencies and vulnerabilities identified in the Operator's anti-money laundering and terrorist financing policies and procedures. The report should state the significance of the deficiencies and vulnerabilities identified, the risk involved, recommendations and the action taken to rectify the situation.

(d) Information on inspections, audit and engagements with the Commission or any instructions or recommendations by the Commission, indicating any deficiencies

and weaknesses identified, the risks involved as well as the corrective measures and actions taken.

(e) Information on the procedures and information systems for the monitoring of the accounts and transactions of its customers by describing their main functions, including whether these are conducted in real time or after transactions, any weaknesses identified and the total number of alerts generated by the systems in place, the number of reports submitted to MOKAS as a consequence of these alerts, the number of false-positives alerts, increases/decreases in comparison with the previous year, and identified trends etc.

(f) The number of suspicious transaction cases investigated by the AMLCO but for which no report has been submitted to MOKAS.

(g) The number of internal money-laundering suspicious reports submitted by the Operator employees to the AMLCO, broken down by department. The number of reports submitted by AMLCO to MOKAS as a result of ISRs submitted by the Operator employees to AMLCO.

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

(i) Information as to the number of high-risk customers with whom the Operator has a business relationship, country of origin and information on the policy, procedures and controls applied by the Operator in relation to high risk customers with whom it maintains a business relationship.

(j) Data for the type and size of the customer base during the last year, the number of customers per risk category, the number of persons with whom the establishment of business relationship was not allowed for compliance reasons, the number of customers with whom the business relationship was terminated, the number of frozen accounts following a court order/MOKAS and comparisons to previous years.

(k) Information on the policy, procedures and controls applied by the Operator 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).

(l) 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.

(m) Information on the training courses/seminars attended by the AMLCO and assistant AMLCO(s) and on any other educational material received.

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

(i) The number of courses/ seminars organized/attended and their duration

(ii) The number of employees attending, specifying their seniority i.e. management staff, officers, newcomers etc.

(iii) Employees failing the courses provided.

(iv) Names and qualifications of the instructor(s), and

(v) Specifying whether the courses/seminars were developed in-house or by an external organization /consultant

(vi) Information on the following year's training program.

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

(o) Review of the structure and staffing of the AMLCO's department including recommendations for additional staff and technical resources which may be needed.

(p) Information (e.g. name, business address, business area, supervisory authority, date of commencement of business relationship, last review date, next review date, rating) on third parties or persons on whom the Operator has relied for performance of Customer Due Diligence measures and therefore has established a business relationship.

Internal Audit

Article 58B of the Law

49. The Operator is obliged to establish an internal audit capability to review and evaluate, on an annual basis, the effectiveness and adequacy of the policy, procedures and controls applied by the Operator for preventing money laundering and terrorist financing and verifies the level of compliance with the provisions of this Direction and the Law.

50. The internal auditor should have relevant expertise and experience of AML/CFT matters. Findings and observations of the internal auditor are submitted directly to the Cyprus Board of Directors or Board Committee and are subsequently notified to the AMLCO who takes the necessary measures to ensure the rectification of any weaknesses and omissions which have been detected by the internal auditor. The internal auditor monitors, on an ongoing basis, through progress reports, or other means the implementation of his recommendations and is directed by the Operator's Board of Directors or Board Committee. In any case, Board of Directors always remains accountable for proper implementation of recommendations of internal audit.

Education and training of employees

51. Article 58 of the Law requires the obliged entities to establish adequate and appropriate systems and procedures to make their employees aware with regard to:

(a) the Operator's systems and procedures for the prevention of money laundering and terrorist financing

(b) the Law and Directives issued by the competent Supervisory Authority

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

(d) relevant Data Protection requirements.

52. 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.

53. Staff of the Operator must be encouraged to report, without delay, matters that come to their attention in relation to transactions for which there is any suspicion that they are related to money laundering or terrorist financing. In this regard, the Operator must establish measures to ensure that staff is fully aware of their responsibilities and duties. Hence the responsibility of AMLCO in cooperation with other competent departments, to prepare and implement, on an annual basis, an education and training programme for the staff.

54. The training programme should educate staff on the latest developments in AML/CFT and terrorist financing including the practical methods and trends used by criminals for this purpose. Training needs to be:

(a) Of high quality, relevant to Operator's money laundering and terrorist financing risks, business activities and up to date with latest legal and regulatory obligations

(b) Obligatory for all relevant staff

(c) Tailored to the particular roles of the staff; the training programme should have a different structure for new staff, front-line staff, compliance staff, staff moving from one department to another etc.

(d) Effective, to be checked by requiring staff to pass tests and by monitoring levels of compliance with the AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected

(e) Ongoing, and relevant; not be limited to when staff are hired

(f) Complemented by AML/CFT information and updates that are disseminated to relevant staff.

55. The Board of Directors and the Senior Management must be informed of their responsibilities under the Law and this Direction and changes and developments in the legal and regulatory framework. Without this, the Board of Directors and the Senior Management will not be able to provide effective management supervision, approve policies, procedures or allocate sufficient resources for the effective prevention of money laundering and terrorist financing

56. The AMLCO will evaluate the adequacy of the training provided and maintain detailed data regarding the seminars/programmes carried out, such as:

- Names of employees participating in the seminar/training by department and by position
- The date, title and duration of the seminar and the names of the trainers
- Whether the lecture/seminar was organised internally or offered by an external agency or consultants and
- Summary information regarding the content of the training.

57. 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 the Operator. Moreover, the frequency of the training may vary depending on the amendments to the legal and/or regulatory requirements, introduction of new products, services or technologies, changes in the tasks of the staff as well as any other relevant changes.

58. It is important that all involved staff consistently implement the Operator's policy and procedures to prevent money laundering and terrorist financing and the promotion of a

culture that understands the importance of the prevention of money laundering and terrorist financing, is the critical to the successful management of risks.

Evaluation of integrity of employees

59. The obligation to apply appropriate policies, controls and processes that are proportionate to its nature and size, in order to mitigate and to effectively manage the risks of money laundering activities and financing of terrorism also relate to the recruitment and evaluation of the integrity of the employees.

60. The Operator should carry out screening of relevant employees appointed by the Operator, before and during the course of the appointment, involving an assessment of the skills, knowledge and expertise of the individual and their conduct and integrity.

CUSTOMER DUE DILIGENCE

General requirements

Articles 60 – 64 of the Law

61. Customer Due Diligence is the process of obtaining and reviewing sufficient information about a customer to ascertain the level of ML/TF risk related to the customer's activities. This process facilitates the assignment of a risk rating to the customer and determines the appropriate level of ongoing scrutiny required.

62. The casino Operator must apply Customer Due Diligence measures if it:

(a) Establishes a business relationship

(b) Suspects money laundering or terrorist financing

(c) Doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification

(d) Carries out an occasional transaction that is a transfer of funds as defined in Article 3(9) of Regulation (EU) 2015/847 with the amount of €1,000 or more

(e) Regardless of whether it has established a business relationship with the customer, suspect money laundering or terrorist financing, or doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification, the Operator must also apply Customer Due Diligence measures in relation to any transaction that amounts to €2,000 or more,

whether the transaction is executed in a single operation or in several operations which appear to be linked.

63. The Operator must also apply Customer Due Diligence measures:

    (a) At other appropriate times to existing customers on a risk-sensitive basis.

    (b) When the Operator becomes aware that the circumstances of an existing customer relevant to its risk assessment for that customer have changed.

64. Further details are described in the section Ongoing monitoring.

Application of Customer Due Diligence measures

Article 61 of the Law

65. Customer Due Diligence measures consist of:

    (a) identifying the customer

    (b) verifying the customer's identity

    (c) where there is a beneficial owner who is not the customer, identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner so that the Operator is satisfied that it knows who the beneficial owner is

    (d) assessing and, where appropriate, obtaining information on the purpose and intended nature of the business relationship

    (e) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that:

        (i) the transactions being conducted are consistent with the Operator’s knowledge of the customer and the risk profile

        (ii) their source of funds and

        (iii) documents, data or information held are kept up to date.

66. Where a person claims to act on behalf of a customer, the Operator must:

    (a) verify that the person is authorised to act on the customer's behalf

    (b) identify the person

    (c) verify the person's identity on the basis of documents or information which, in

either case, is obtained from a reliable source which is independent of both the person and the customer.

67. The Operator does not need to repeat Customer Due Diligence measures if a customer visits another casino premises operated by the Operator, but Customer Due Diligence records held by the Operator will need to be available across the Operator's different casino premises, and the policies and procedures must include details of how the Operator will manage this.

68. The ways in which the casino Operator meets the requirements for Customer Due Diligence and the extent of the measures it takes must reflect the risk assessment it has carried out, and its assessment of the level of risk arising in any particular case. This may differ from case to case.

69. In assessing the level of risk arising in a particular case, the Operator must take account of factors including, among other things:

(a) the purpose of a customer account, transaction or business relationship

(b) the amount deposited by a customer or the size of the transactions undertaken by the customer

(c) the regularity and duration of the business relationship

(d) the regularity and duration of occasional transactions.

Timing of Customer Due Diligence measures

Article 62 of the Law

70. The Operator must comply with the requirement of the Law to perform Customer Due Diligence measures before the establishment of a business relationship or the carrying out of the transaction.

71. Despite the above, Article 62(2) allows, by way of derogation, Customer Due Diligence to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is low risk of money laundering or terrorist financing. In such situations these procedures shall be completed as soon as practicable after the initial contact and before the execution of any transactions.

72. However, Article 62(4) explicitly requires that in situations where the Operator is unable to comply with the Customer Due Diligence measures stipulated in Article 61(1)(a) to (c), it may not carry out a transaction through a bank account, establish a business relationship

or carry out the transaction, shall terminate the business relationship, and shall consider whether under the circumstances a report should be filed with MOKAS.

Customer relationships

73. Customer means a person that establishes a business relationship or performs an occasional transaction with the Operator, while a person is defined as both natural person and legal entity. Customers/person may be both individuals and legal entities.

74. Consequently, within the context of a casino, a customer may be the person using the casino premises for gaming or the person that brings people and/or money or facilities to the casino for the purpose of gaming.

75. Customer relationships for AML purposes consist of three aspects:

(a) the establishment of the business relationship with the customer, requiring verification of the customer's identity (to a reasonable degree) and completion of customer due diligence

(b) the monitoring of customer activity (within a business relationship and risk relevant occasional transactions)

(c) the termination of the relationship with the customer.

76. At all stages of the relationship it is necessary to consider whether the customer is engaging in money laundering; whether there is a need to report suspicious activity; and level of risk posed to the Operator.

Establishment of a business relationship

77. A business relationship is a business, professional or commercial relationship between the casino Operator and a customer which is linked to the professional activities of the Operator and is expected by the Operator, at the time of its establishment, to have a certain duration.

78. In the context of the Operator, a business relationship occurs when:

(a) a customer opens an account with the Operator

(b) a customer becomes a loyalty member of a casino (when a membership scheme is operated by the Operator)

(c) a customer is introduced by a Junket Operator and plays at the casino

(d) a customer applies for or is granted a credit facility at the Operator

(e) a customer sends front money to the Operator

(f) a customer uses a safety deposit box at the Operator

(g) the casino Operator uses a Junket Operator to bring people and/or money to the casino for the purpose of gaming (in which case a business relationship with the Junket Operator is established)

(h) the Operator uses an e-wallet provider to bring money to the casino with the purpose of gaming (in which case a business relationship with the e-wallet provider is established).

79. The list above is not exhaustive, and the Operator will need to take into consideration any other situations when circumstances otherwise arise with a customer from which it expects or it could be reasonably inferred that it expects, that the relationship with the customer will have a certain duration.

Occasional transactions

80. An occasional transaction is defined as any transaction other than a transaction which takes place in a business relationship. Therefore, any transaction that is not performed during the course of a business relationship should be considered as an occasional transaction.

81. The Operator has the obligation to monitor the following occasional transactions:

(a) Individual transactions with the amount of €2,000 or more, for which the Operator has the obligation to perform Customer Due Diligence measures as described in Section 3, Customer Due Diligence.

(b) Linked transactions with the cumulative amount of €2,000 or more during a period of twenty-four hours from 6am until 6am of the next day1. The Operator is obliged to monitor linked transactions that are individually below the €2,000 threshold but that cumulatively meet or exceed this threshold, and in such case has the obligation to perform Customer Due Diligence measures as described in Section 3, Customer Due Diligence. Furthermore, in such case the Operator will need to consider whether a customer is deliberately spreading their wagering or collection of winnings over a number of transactions or days in order to circumvent the Customer Due Diligence requirements. The Operator should keep in mind that by separating the purchase or exchange of tokens from the payment to use gaming

[1] Please also check the relevant record keeping requirements – section 4, Record Keeping.

machines, there is the potential for customers to spend up to €2,000 in gaming machines in addition to the purchase of tokens up to €2,000.

(c) Occasional transactions that do not necessarily meet the requirements described under a) and b) above but are performed by customers that are gaming at the Operator on a regular basis. There may be situations where a customer performs transactions below the €2,000 threshold, but games with the Operator regularly, such that Operator needs to consider when they fall within the definition of a business relationship (i.e. having an element of duration).

(d) Occasional transactions that consist of the transfer of funds with the amount of €1,000 or more, for which the Operator has the obligation to perform Customer Due Diligence measures as described in Section 3, Customer Due Diligence.

82. The Operator needs to be aware that in case of customers performing individual transactions with the amount of €2,000 or more, linked transactions with total amount of €2,000 or more, customers performing occasional transactions on a regular basis, and customers performing occasional transactions in the form of transfer of funds of €1,000 or more (as described under points a, b, c and d above), the business relationship is established once the element of duration is present.

83. In case that the customer plays at the casino on a regular basis, the Operator needs to determine when the criteria for the establishment of a business relationship with the customer have been met and when it needs to perform Customer Due Diligence measures in line with Section 3 of this Direction.

84. The Operator should establish systems and procedures for detection and monitoring of linked transactions performed by the same customer within a single casino premises and across different casino premises.

Business to Business relationships (including Junkets)

85. The Operator may choose to establish a business relationship with a legal entity concerned with the provisions of items or services that is *not* considered a Junket under the Casino Operations and Control Law of 2015 as they neither receive commission based on the gaming revenues of a customer or customers, receive a share of the gross gaming revenue from the Junket customers or have not been designated as such by the Commission under the provisions of the Casino Operations and Control Law of 2015.

86. In such circumstances, the Operator must undertake appropriate Customer Due Diligence measures in line with the section 3, Customer Due Diligence of this Direction before

a contract is signed and the business relationship should be subject to ongoing Customer Due Diligence by the Operator as described in the section 3, Customer Due Diligence of this Direction and be monitored through the course of the relationship to ensure that ML/TF risks are identified and records of the monitoring kept and made available for examination by the Commission. Contracts exceeding €100.000 per annum must be notified to the Commission annually.

87. At this time, the Commission considers that any third party, not being an employee of the casino that brings customers to the casino by providing transport only and is paid on a per capita basis or in way completely unrelated to any gaming activity, gaming expenditure or loss of those customers or the gaming profit or loss of the Operator from those customers, shall not be considered a Junket and the customers not considered Junket customers.

88. The Operator may choose to establish a business relationship with third party Junket operators not excluded by the provisions of the above paragraph which requires a Junket licence from the Commission. The Operator must undertake appropriate Customer Due Diligence measures in line with section 3, Customer Due Diligence of this Direction before an application is submitted to the Commission and this business relationship must be subject to ongoing Customer Due Diligence obligations by the Operator as described in section 3, Customer Due Diligence of this Direction.

Identification and verification

89. Applying Customer Due Diligence measures involves several steps. The Operator is required to identify and verify customers identities. The verification of identity requires confirming claimed identity against documents, data or information obtained from a reliable and independent source.

90. For the purposes of customer due diligence, proof of identity is satisfactory if:

(a) It is reasonably possible to establish that the customer is the person he claims to be and

(b) The person who examines the evidence is satisfied, that the customer is actually the person he claims to be.

Natural persons

Identification

91. The Operator should identify the customers who are natural persons by obtaining the following information:

(a) True name and/or names used

(b) Full permanent address, including postal code

(c) Government issued document number, issuing date and country

(d) Telephone number

(e) E-mail address

(f) Date and country of birth

(g) Nationality

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

92. Information on occupation will assist the Operator's assessment as to whether a customer's level of gambling is proportionate to their approximate income, or whether it is suspicious.

Verification

93. Information about customer identity must then be verified through documents, data and information which come from a reliable and independent source. The acceptable method for the verification of a customer's identity is the reference to original documents which are issued by an independent and reliable source. At least one document used for verification purposes should include the customer's photo.

94. It is generally considered good practice and especially in high risk situations, to obtain from the customer at least one document from an authoritative source that verifies the customer's full name and address or full name and date of birth with photograph and supporting documentation that verifies their name and either date of birth or address.

95. The following sources may be used as the primary source of verification of customers:

(a) current passport

(b) current identity card

(c) current photo card driving licence.

96. For non-EU citizens, a current passport should always be obtained as a primary source of verification.

97. The above documents can be supported by a second document not used as a primary source of verification that may be:

(a) Utility bill or statement that can, on a risk basis, be verified as true by the company that issued it, commonly by confirmation of a reference number, name and address

(b) Bank statement or passbook containing current address that can, on a risk basis, be verified as true by the company that issued it - bank or credit cards alone will not be sufficient as these do not provide either residential address or date of birth.

98. Original documents should be examined so that, as far as reasonably practicable, forgeries are not accepted.

99. The Operator should recognise that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, the Operator should take practical and proportionate steps available to establish whether the document offered is a forgery or otherwise false. Commercial software is available to check the validity of passports of any country that issues machine-readable passports.

100. If documents are in a foreign language appropriate steps need to be taken to be reasonably satisfied that the documents provide factual evidence of the customer's identity.

101. If satisfied that the original and genuine identification documents have been presented, the Operator should keep copies of the pages containing all relevant information which must be certified as true copies of the original documents by the Operator's employee who verified the identity of the customer.

102. The certifier should:

(a) sign and date the copy document (showing his name clearly in capitals underneath) and

(b) such certification should be evidenced by a written statement stating that: the document is a true copy of the original document; the document has been seen and verified by the certifier; and (where the document contains a photo) the photo is a true likeness of the customer.

Legal entities

Identification

103. The identification of a legal person comprises obtaining information relating to the following:

(a) The registered number, country and date of registration

(b) The registered corporate name and trading name used

(c) Full address of registered office

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

(e) The telephone numbers and e-mail address

(f) The members of the board of directors

(g) The individuals that are duly authorised to act on behalf of the legal person

(h) The beneficial owners of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country with equivalent disclosure and transparency requirements

(i) The registered shareholders that act as nominees of the beneficial owners.

Verification

104. The verification of the identity of a legal person, comprises obtaining the following documents or documents similar to the below, depending on the jurisdiction:

(a) Memorandum and Articles of Association

(b) Certificate of Incorporation

(c) Certificate of Good Standing

(d) Certificate of Registered Address

(e) Certificate of Directors and Secretary

(f) Certificate of Registered Shareholders in the case of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country with equivalent disclosure and transparency requirements

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

(h) Documents and data for the verification of the identity of the persons that are authorised to act on behalf the legal person, as well as the registered shareholders and beneficial owners of the legal person.

Unincorporated businesses, partnerships and other persons with no legal substance

Identification

105. The identification of unincorporated businesses, partnerships and other persons with no legal substance comprises obtaining of the following:

(a) full name

(b) business address

(c) names of all partners/principals who exercise control over the management of the partnership

(d) names of individuals who own or control over 25% of its capital or profit, or of its voting rights.

Verification

106. In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, beneficial owners and other individuals who exercise control over the management of the partnership is verified according to the procedures set for identification and verification of natural persons. In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate is obtained and where it exists, the formal partnership agreement shall be obtained.

107. The Operator shall obtain documentary evidence of the head office address/trading address of the business, ascertain the nature and size of its activities.

Identification of beneficial owners

108. For the purpose of this Direction "beneficial owner" means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:

109. In the case of corporate entities:

(a) The natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

(i) A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person is an indication of direct ownership.

(ii) A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), is an indication of indirect ownership.

(iii) It is further provided that control by other means can be determined among others on the basis of criteria set out in paragraph (b) of subsection (1) of Article 142 and Article 148 of Cyprus Companies Law (KEF 113) 1968 to 2018.

(b) The natural person(s) who hold the position of senior managing official(s) in case that after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (a) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s).

110. In the case of trusts:

(a) the settlor

(b) the trustee(s)

(c) the protector, if any

(d) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates

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

111. In the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in paragraph (110) above.

112. In deciding who the beneficial owner is in relation to a customer who is not a private individual, identification and verification of beneficial owners extends to legal entities that own other legal entities. The Operator should look for the natural person(s) who ultimately exercises control through ownership or through other means of the legal entity that is the customer. Control through other means may, inter alia, include the criteria of control used for the purpose of preparing consolidated financial statements, such as through a shareholders'

agreement, the exercise of dominant influence or the power to appoint senior management. The Operator should verify the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than 25% in the legal person's ordinary share capital or voting rights.

113. There may be cases where no natural person is identifiable who ultimately owns or exerts control over a legal entity. In such exceptional cases, if all other means of identification have been exhausted, and provided there are no grounds for suspicion, senior managing official(s) are considered to be the beneficial owner(s).

114. The Operator should collect appropriate documents for verification of ownership structure including certificates of the registered shareholders for the companies participating in the ownership structure of the customer, ownership charts etc. as well as appropriate information and documents for verification of identity of individual that are ultimate beneficial owners.

Assessing and obtaining information on the purpose and intended nature of the business relationship

115. The Operator must understand the purpose and intended nature of the business relationship or transaction in order to assess whether the proposed business relationship/transaction is in line with the Operator's expectation and to provide the Operator with a meaningful basis for ongoing monitoring.

116. Depending on the Operator's risk assessment of the situation, information that is relevant must include as a minimum the following:

(a) The anticipated turnover/size of transactions and kind of wagering activities in which the customer is likely to engage

(b) The origin of funds

(c) The source and size of the customer's wealth and annual income

(d) Regularity or duration of the relationship.

Ongoing monitoring

Article 61.1(d) of the Law

117. The Operator must conduct ongoing monitoring of their business relationships and occasional transactions including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the

Operator's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

118. Moreover, Article 60(d) of the Law requires obliged entities to apply Customer Due Diligence measures when there are doubts about the veracity or adequacy of previously obtained customer identification documents, data or information. Furthermore, article 62(6) of the Law requires the application of Customer Due Diligence measures not only to new customers but also at appropriate times to existing customers, depending on the level of risk of being involved in money laundering or terrorist financing activities.

119. The ongoing monitoring must include the following:

(a) Scrutiny of transactions undertaken throughout the course of the relationship (including the source of funds) to ensure that the transactions are consistent with the casino's knowledge of the customer, the customer's business and risk profile. All such reviews and investigations should be properly documented, and relevant records kept for in line with Record keeping requirements of the Law and this Direction.

(b) Undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying Customer Due Diligence measures up-to-date.

120. The Operator needs to ensure that the arrangements it has in place are effective in monitoring customers and the accounts they hold are sufficient to manage the risks the Operator is exposed to.

121. The Operator's policies and the procedures should determine the timeframes for the regular review, examination and update of the customer identification data, depending on the risk categorisation of each customer. The outcome of the review should be recorded in a separate form and be kept in the respective customer files.

122. If at any time during the business relationship with an existing customer, the Operator becomes aware that reliable or adequate Customer Due Diligence data and information are missing regarding the customer, then the Operator should take all necessary action, by applying the Customer Due Diligence measures to collect the missing data and information, the soonest possible, so as to complete the customer's profile.

123. In addition to the requirement for the regular update of the Customer Due Diligence data and information, when it is observed that unreliable or inadequate data and information

or whenever there is a material event that could influence the overall customer's risk categorization or profile is being held this should be rectified. This could be inter alia:

(a) an individual transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions of the customer.

(b) identification of material negative information about the customer which points to the need for an update of the data and information about the customer or to a possible risk reclassification.

(c) any indication that the identity of the customer, or of the customer's beneficial owner, has changed.

(d) any transactions which are not reasonably consistent with the Operator's knowledge of the customer.

(e) any change in the purpose or intended nature of the Operator's relationship with the customer.

(f) any other matter which could affect the Operator's assessment of the money laundering or terrorist financing risk in relation to the customer.

124. The details of any periodic and off-cycle reviews of customer's profile should be documented accordingly together with the rationale for making all relevant decisions and for classification of a customer into a certain risk category. The records should include the Customer Due Diligence measures taken and the reasons for continuing/terminating the business relationship and the decision maker. This information should be kept within the customer file in line with the record keeping requirements defined by the Law and this Direction.

Simplified (customer) Due Diligence

Article 63 of the Law

125. The Article 63 of the Law provides that the Operator may apply Simplified Due Diligence measures in situations where the money laundering and terrorist financing risk associated with a business relationship or occasional transaction has been assessed as low.

126. Before applying Simplified Due Diligence measures the Operator is required to ascertain that the business relationship or occasional transactions presents a low degree of risk. Simplified Due Diligence is not an exemption from any of the Customer Due Diligence measures; however, the amount, timing or type of each or all of the Customer Due Diligence measures may be varied commensurate to the low risk that has been identified.

127. Simplified Due Diligence measures may include but are not limited to:

(a) adjusting the timing of Customer Due Diligence

(b) adjusting the quantity of information obtained for identification, verification or monitoring purposes

(c) adjusting the frequency of Customer Due Diligence updates and reviews of the business relationship.

128. The Operator must make sure that this does not result in a de facto exemption from keeping Customer Due Diligence information up to date.

129. The information the Operator obtains when applying Simplified Due Diligence measures must enable the Operator to be reasonably satisfied that its assessment that the risk associated with the relationship is low is justified.

130. It must also be sufficient to give the Operator enough information about the nature of the business relationship to be able to comply with the obligation to carry out sufficient monitoring of business relationships or transactions to enable it to detect any unusual or suspicious transactions.

131. Simplified Due Diligence does not exempt the Operator from obligation of ongoing monitoring and reporting suspicious transactions to MOKAS.

132. Where there are indications that the risk may not be low, for example where there are grounds to suspect that money laundering or terrorist financing is being attempted or where the Operator has doubts about the veracity of the information obtained, Simplified Due Diligence must not be applied. Equally, where specific high-risk scenarios apply and there is an obligation to conduct Enhanced Due Diligence, Simplified Due Diligence must not be applied.

133. When assessing the money laundering or terrorist financing risk the Operator shall take into consideration at least the relevant risk factors stipulated in the Law as well as information provided in this Direction and any Guidelines issued by the Commission.

Enhanced (customer) Due Diligence

Article 64 of the Law

134. The Operator must apply Enhanced Due Diligence measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. Enhanced Due Diligence measures cannot be substituted for regular Customer Due

Diligence measures but must be applied in addition to such Customer Due Diligence measures. Enhanced Due Diligence measures, including the extent of the additional information sought, and of the increased monitoring carried out, will depend on the reason why an occasional transaction or a business relationship was classified as high risk.

135. The Enhanced Due Diligence measures must be applied:

(a) if the Operator has determined that a customer or beneficial owner is a PEP, or a family member or a close associate of a PEP

(b) in any business relationship or transaction with a customer from a high-risk third country

(c) in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose

(d) in any other case which, by its nature or circumstances, can present a higher risk of money laundering or terrorist financing

136. In addition, the Operator is required to apply Enhanced Due Diligence measures in the following situations:

(a) For all customers introduced by Junket Operators

(b) For all customers using front money accounts

(c) For all customers using e-wallet to transfer money to the Operator

Politically Exposed Persons (PEPs)

137. Article 64 of the Law requires the Operator to apply Enhanced Due Diligence measures with respect to transactions or business relationships with PEPs. The definition of a PEP includes family members of such person and persons known to be close associates of such person.

138. With respect to transactions or business relationships with PEPs, the Operator is required to have in place appropriate risk procedures and management systems to determine whether the customer or the beneficial owner of the customer is a PEP.

139. In cases of business relationships or transactions with PEPs the following Enhanced Due Diligence measures must be applied:

(a) obtain Senior Management approval for establishing/continuing business relationships with such persons or performing a transaction.

(b) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons. This would mean obtaining a documentary evidence of source of wealth and source of funds.

(c) conduct enhanced, ongoing monitoring of those business relationships.

140. Where a PEP is no longer entrusted with a prominent public function, the Operator shall, for at least 12 months, be required to consider the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to PEPs.

141. Although under the definition of a PEP an individual cease to be so regarded after he has left office for 12 months, the Operator should apply a risk-based approach in determining whether or when it should cease carrying out appropriately enhanced monitoring of transactions. In cases where the PEP presents a high risk of money laundering or terrorist financing, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately decreased.

142. The Operator's policies and procedures should cover when and how customers will be checked for PEP status and how and when Senior Management approval will be sought and provided, and deal with how the customer will be dealt with if there is any delay to approval being provided by Senior Management.

143. There is a hierarchy of risk for individual PEPs, where some PEPs have higher relative risk and others have lower relative risk. The measures taken for particular PEPs should therefore be informed by the relative risk attributed to the PEP, including consideration of the jurisdiction from which they originate and the position they hold.

Unusual transactions

144. The Operator should put in place adequate policies, procedures and systems to detect unusual transactions or patterns of transactions. Where the Operator detects transactions that are unusual because:

(a) they are larger than what the Operator would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs

(b) they have an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers,

products or services, or

(c) they are very complex compared with other, similar transactions associated with similar customer types, products or services

(d) and/or the Operator is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given.

145. In such circumstances the Operator must apply Enhanced Due Diligence measures.

146. These Enhanced Due Diligence measures should be sufficient to help the Operator determine whether these transactions give rise to suspicion and must at least include:

(a) taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business/occupation to ascertain the likelihood of the customer making such transactions and

(b) monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. The Operator may decide to monitor individual transactions where this is commensurate to the risk it has identified.

High-risk third countries and other high-risk situations

147. When dealing with natural persons or legal persons established or residing in a high-risk third country and in all other high-risk situations, the Operator should take an informed decision about which Enhanced Due Diligence measures are appropriate for each high-risk situation. The extent of additional information sought, and of the increased monitoring carried out, will depend on the reason why an occasional transaction or a business relationship was classified as high risk.

148. In all cases the Enhanced Due Diligence measures must include as a minimum the following:

(a) obtaining approval by Senior Management for the commencement/continuation of a business relationship

(b) examining the background and purpose of the transaction and taking adequate measures to ascertain the source of wealth and source of funds

(c) systematic and thorough monitoring of the transactional behaviour of the customer.

149. The AMLCO should be aware of high-risk customers and act as an advisor to Senior Management before the establishment of a business relationship or performing the transaction. The approval of the AMLCO is required for the reclassification of high-risk customers to a lower risk level.

150. In some cases, depending on the risk it may be appropriate to apply and one or more of additional Enhanced Due Diligence measures. The Operator is not required to apply all the Enhanced Due Diligence measures listed below in all cases. For example, in some high-risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the business relationship.

151. Additional Enhanced Due Diligence measures the Operator should apply may include inter alia:

(a) Obtaining additional customer information, such as the customer's reputation and background from a wider variety of sources before the establishment of the business relationship and using the information to inform the customer risk profile

(b) Carrying out additional searches to better inform the customer risk profile

(c) Obtaining information about the intermediary's underlying customer base and its AML/CFT controls

(d) Undertaking further verification procedures on the customer or beneficial owner to better understand if the customer or beneficial owner may be involved in criminal activity

(e) Seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship

(f) Obtaining further documentary evidence for source of wealth

(g) Obtaining further documentary evidence for source of funds.

Reliance on third parties

Article 67 of the Law

General requirements

152. Article 67 of the Law allows the obliged entities to rely on third parties for the implementation of Customer Due Diligence measures, as these are prescribed in Article 61(1)(a),(b),(c) of the Law.

153. The Law explicitly states that the ultimate responsibility for performing the above-mentioned measures remains with the Operator if relying on a third party. The responsibility to apply Customer Due Diligence measures cannot be delegated to the third party.

154. Based on the Law the third parties are defined as:

(a) Obliged entities referred to in paragraphs (a), (b), (c) and (d) of subparagraph (1) of Article 2A of the Law (credit institutions, financial institutions, auditors, external accountants and tax advisers, independent legal professionals, trust or company service providers)

(b) Other institutions or entities located in the Member States or in a third country, which

(i) Apply Customer Due Diligence measures and keep records at the same level with those established by the EU Directive and

(ii) Are subject to supervision which is at the same level as relevant requirements of EU Directive.

155. A Junket Operator is not an obliged entity under the Law, nor can it be considered a third party as above. The Operator may not rely on Customer Due Diligence performed by a Junket operator.

156. Further, the Operator may not rely on due diligence measures of a third party established in a high-risk third country.

157. For the purpose of this Direction "high-risk third country" means a third country, which is flagged by the European Commission under the provisions of paragraph (2) of Article 9 of the EU Directive and which has strategic deficiencies in its national AML/CFT regime that pose significant threats to the financial system of the Union, and a country which is classified by the Operator as high risk, according to the risk assessment referred to in Article 58a of the Law.

158. The Operator must request from the third party to:

(a) make immediately available data, information and documents obtained as a result of the application of the Customer Due Diligence measures in accordance with the requirements of the Law and

(b) forward immediately to the Operator, copies of these documents and relevant information on the identity of customer or the beneficial owner which the third party collected when applying the above procedures and measures.

159.The Operator's relationship with a third party needs to be based on a written agreement in which the obligations of every party for the offering of relevant services are specified, including the financial terms. Customer Due Diligence measures need to be applied by the Operator on the third party before the business relationship commences.

Procedures for verification of suitability of a third party

160.The AMLCO has the responsibility to verify and properly document that any agreed third party fulfils the criteria specified in this Direction.

161.The AMLCO should maintain a separate file with the information on the identity of any third party, including the economic and risk profile of the third party, minutes of the meetings with third party and information that verifies that the third party fulfils the criteria of a third party as defined in this Direction.

162.The AMLCO should maintain a register with the following information relating to the third party with which the Operator has or used to have a business relationship:

(a) Name

(b) Business address

(c) Professional activity sector

(d) Supervisory authority

(e) Date of commencement of business relationship

(f) Date of latest evaluation

(g) Date of next evaluation

(h) Number of the customers introduced to the Operator per year

(i) Number of customers reported to MOKAS

(j) Date and reason for termination of business relationship, if applicable.

163.The commencement of the business relationship with the third party must bear the written and duly justified approval of the AMLCO and must be kept in the individual record file of the third party maintained by the Operator.

164.The AMLCO should maintain a register with the following information on the third party with which a business relationship proposal was rejected:

(a) Name

(b) Business address

(c) Professional activity sector

(d) Supervisory Authority

(e) Date of rejection

(f) Reasons for rejection

165. The Operator may rely on third parties as defined in Article 67 of the Law only at the outset of establishing a business relationship with the customer for the purpose of performing initial Customer Due Diligence measures. Any additional data and information for the purpose of updating the customer's information during the course of business relationship and/or examining unusual transactions needs to be obtained directly from the customer.

Transactions and products that favour anonymity

Article 66(3) of the Law

166. The Law requires the Operator to pay special attention to every threat or danger for money laundering or terrorist financing which may result from products or transactions which may favour anonymity. The Operator is required to take measures, to prevent the use of products and services that may favour anonymity for money laundering and terrorist financing activities.

167. The Operator is also required to establish and apply reasonable measures and procedures to identify the risks arising from technological developments and new financial products.

Prohibition of opening or maintaining anonymous or numbered accounts

Article 66(2) of the Law

168. It is prohibited for the Operator to open or maintain anonymous or numbered accounts or accounts in names other than those stated in their official identity documents. Maintaining anonymous safety deposit boxes is also prohibited.

Requirements to cease transactions or terminate relationship

Article 62(4) of the Law

169. Where the Operator is unable to apply the required Customer Due Diligence measures in relation to a particular customer, the Operator:

(a) must not carry out a transaction with or for the customer through a bank account

(b) must not establish a business relationship or carry out a transaction with the

customer

(c) must terminate any existing business relationship with the customer

(d) must consider whether it is required to make a report to MOKAS.

170. The Operator must have clear policies in place on how it will manage situations where it is unable to apply the Customer Due Diligence measures.

Safety deposit boxes

171. In the case if the Operator offers safety deposit boxes to its customers, it should ensure that in such cases Customer Due Diligence measures are always applied.

RECORD KEEPING

General requirements

Article 68 of the Law

172. The Operator is required to keep the following documents and information, for a period of five (5) years after the end of business relationship with the customer or after the date of the occasional transaction:

(a) A copy of the documents and information required in order to comply with the due diligence requirements, as defined in the Law and this Direction

(b) Supporting evidence and records of transactions that are necessary for identification of transactions

(c) Relevant correspondence with the customers and other persons with which it keeps a business relationship.

173. In relation to the evidence of a customer's identity, the Operator must keep a copy of any documents or information obtained to satisfy the Customer Due Diligence measures required under the Law and this Direction.

174. The Operator needs to ensure that it is able to link Customer Due Diligence information for a particular customer to the transactions that the customer conducts at the casino and that this information is retained for a period of five (5) years. The Operator needs to ensure that transactional information always includes at least the calendar date and time of the transaction.

175. The Operator has the obligation to apply systems which make possible the timely response to enquiries of MOKAS or the Commission as to whether it keeps or has kept during the last five (5) years a business relationship or has performed occasional transactions with specific persons and the type of this business relationship. The Operator needs to ensure that all the documents are made available in a timely manner and without delay to MOKAS and the Commission for the purpose of performing their duties by the Law.

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

177. MOKAS needs to be able to compile a satisfactory audit trail of illicit money and be able to establish the business profile of any account and customer under investigation. The Commission may also in certain circumstances need to obtain detailed information regarding customer's activity at the Operator.

178. To satisfy this requirement, the Operator must ensure, they will be able to provide the following information:

(a) the identity of the person undertaking the transaction

(b) the identity of the actual owners/beneficiaries if any

(c) information on connected persons/transactions if any

(d) information on the source of money

(e) the form in which the funds were placed and withdrawn i.e. cash, cheques, funds transfers etc., exact value of the funds placed and withdrawn (buy in and buy out) and exact value of winnings

(f) the type and amount of the currency involved

(g) the type, identifying number, calendar date and time of any transaction performed by the customer.

179. Where documents verifying the identity of a customer are held in one licensed casino premises within the Operator in Cyprus, they do not also need to be held in duplicate form in another licensed casino premises of the Operator in Cyprus. It is sufficient for the Operator to undertake identification and verification providing that the information is available to each premises or site. The records need to be accessible to all premises that have contact with the customer, the AMLCO and law enforcement.

180. The copies of the customer identification evidence must be certified by the Operator's employee who verifies the identity of the customer. The aforementioned certification for customers who are natural persons should be done in line with the requirements of this Direction provided in Section 3.6, Identification and verification. In the case of customers-natural persons introduced by the third person, it should bear the stamp of the third person to whom the Operator relies for the purpose of verifying the identity of the customer.

181. In case of business relationships with legal entities, the original documents should be obtained. However, after having seen the original documents, the Operator may maintain true copies of the said documents in the customer file. The said copies must be certified by an employee of the Operator, bear the name of the employee, the signature of the employee who certifies the documents as well as the date of the certification.

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

183. The Operator 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.

184. The Operator 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.

185. 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.

186. 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.

187. All information held by the Operator in order to comply with its obligations must be secure and accessibility should be limited to those approved by the AMLCO and responsible executive. AML/CFT records accessed must identify the person accessing them and include the time, date and reason.

Supporting records (gaming machines)

188. 'Ticket in, ticket out' (TITO) and 'smart card' technology means that machines produce supporting records that can be attributed to a customer who falls within the record keeping requirements, in which case such records must be retained in accordance with the Law and this Direction.

189. The essentials of any system of monitoring are that:

(a) it flags up transactions and/or activities for further examination

(b) these reports are reviewed promptly by the AMLCO

(c) appropriate action is taken on the findings of any further examination.

190. Monitoring can be either:

(a) in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place

(b) after the event, through the AMLCO's review of the transactions and/or activities that a customer has undertaken.

191. In either case, unusual transactions or activities should be flagged for further examination and details of relevant examinations and investigations properly documented and kept by the Operator.

192. In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer risk.

193. The scope and complexity of the monitoring process will be influenced by the nature and structure Operator's business activities, and size. The key elements of any system are the ability to have current and accurate customer information from all of its casinos, on the basis of which it will be possible to identify the unusual and ask questions as to the reasons for unusual transactions or activities, in order to judge whether they are suspicious.

SUSPICIOUS ACTIVITIES AND REPORTING

Internal reporting

Articles 26, 27 and 69 of the Law

194. 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, and not to report to MOKAS this information, as soon as is reasonably practical, after it comes to their attention.

195. In the case of Operator's employees, Article 26 of the Law recognises that internal reporting to the AMLCO will satisfy the reporting requirement imposed by virtue of Article 27. This means that once the Operator's employee has reported their suspicion to the AMLCO, they are considered to have fully satisfied their statutory requirements, under Article 27.

196. The Operator shall ensure that its employees are aware of their legal obligations and know the person (i.e. the AMLCO) to whom they should report money laundering or terrorist financing knowledge or suspicion. Internal reports to AMLCO and reports made by AMLCO to MOKAS, must be made as soon as is practicable.

197. All suspicions reported to the AMLCO should be documented or electronically recorded. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the grounds for knowledge or suspicion of money laundering or terrorist financing. All internal enquiries made in relation to the report should also be documented or electronically recorded.

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

Evaluation and determination by the AMLCO

199. The Law provides that the Operator's AMLCO must consider each report and determine whether it gives rise to grounds for knowledge or suspicion. The Operator must

permit the AMLCO to have access to any information, including Customer Due Diligence information, in the Operator's possession that could be relevant. The AMLCO may also require further information to be obtained, from the customer if necessary.

200. If the AMLCO decides not to make a report to MOKAS, the reasons for not doing so should be clearly documented or electronically recorded and retained. The Operator must have regard to the secure storage and access protocols of these records that should be kept securely and separately by the AMLCO.

External reporting to MOKAS

Article 69 and 70

201. The AMLCO must report to MOKAS for any transaction or activity that, after their evaluation, they know or suspect that may be linked to money laundering or terrorist financing. The obligation to report to MOKAS includes also any attempt to carry out suspicious transactions. Report must be made as soon as is practicable after information comes to the AMLCO and the AMLCO performs their evaluation. The AMLCO has the responsibility to keep records of all reports made to MOKAS.

202. Having submitted a report to MOKAS, the Operator needs to consider if the relationship with the customer needs to be terminated or not. Decision needs to be properly documented and retained. In such an event, the Operator should exercise particular caution, as per Article 48 of the Law, not to alert the customer concerned that a disclosure report has been filed with MOKAS.

203. After submitting the report to MOKAS, the Operator should adhere to any instructions given by MOKAS.

FINANCIAL SANCTIONS

204. As Member State of the United Nations (UN) and the European Union (EU), the Republic of Cyprus has an obligation to enforce/implement:

(a) International Sanctions adopted by the Security Council under chapter VII of the UN Charter and

(b) Restrictive Measures adopted by the Council of the EU via relevant Decisions and Regulations, within the framework of Common Foreign and Security Policy (CFSP).

205. Under the Article 3(1) of the Implementation of the Provisions of the Resolutions or Decisions of the United Nations Security Council (Sanctions) and of the Decisions and Regulations of the Council of the European Union (Restrictive Measures) Law 58(I) of 2016, the Commission has been established as competent authority for ensuring the implementation of the Provisions of the Resolutions or Decisions of the United Nations Security Council (Sanctions) and of the Decisions and Regulations of the Council of the European Union (Restrictive Measures) within the casino gaming sector in the Republic of Cyprus.

206. Article 23 of the Anti-Terrorism Law of 2019 75(I)/2019 requires that the Operator as an obliged entity as defined in article 2A 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.

207. In case that the Operator discovers that it is in possession or control of or is otherwise dealing with the funds or economic resources of a designated person, the Operator needs:

(a) To freeze the assets immediately

(b) Not deal with them or make them available to or for the benefit of the designated person

(c) Report to the Commission.

208. According to Article 24 of the Law 75(I)/2019, the Operator as an obliged entity must report to the Commission as their Supervisory Authority, who will, 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 25 of Law 75(I)/2019. If the Operator fails to comply with the provisions of Article 24 or Article 23 of the Law 75(I)/2019 then the Commission may take the measures as provided for in section 59(6) of the Law.

209. The Operator should identify and assess the sanctions risks to which it is exposed and implement a sanctions screening programme in line with its nature, size and complexity. Sanction screening is a control used to detect, prevent and manage sanctions risk. Systems should be in place to detect newly designated sanctioned individuals and to prevent dissipation of assets.

210. The Operator should consider the likelihood of sanctioned persons using its facilities, considering local demographics and its customer base including matters such as jurisdiction where it is operating and its proximity to sanctioned countries, locations where the customers are resident/based, jurisdictions where they perform business activities etc. The Operator should also take appropriate measures to mitigate these risks.

211. The Operators AML/CFT program should include a sanctions screening program that comprises screening policies, procedures and controls to monitor financial transactions preventing breaches of the financial restrictions legislation. The Operator should refer to the current versions of the legislation imposing the specific financial sanctions to understand exactly what is prohibited.

212. The sanctions screening programme created in line with the AML/CFT Program should include:

(a) Policies and Procedures: Outlining the requirements as to when screening needs to be done and at which frequency, how alerts should be handled and especially how to deal with the alerts if not enough information is available.

(b) Responsible person: Potential sanctions matches should be reviewed by person with appropriate skills and experience. The staff should be properly trained to know how to deal with potential sanctions matches.

(c) Risk Assessment: Risk-based approach should be applied to decision making regarding the set-up of sanctions screening programme and this needs to be clearly documented.

(d) Internal controls: It is necessary to document how the screening system is configured in order to demonstrate that it is reasonably expected to manage specific sanctions risk.

SUBMISSION OF DATA AND INFORMATION

Article 59(9) of the Law

213. According to Article 59(9) of the Law the Commission may request and collect from persons subject to its supervision information necessary or useful for the performance of its functions and request within a specified deadline the provision of information, data and documents. In case of refusal of any person under its supervision to comply with its request for the provision of information within the specified deadline or if the person refuses to give

any information or demonstrates or provides incomplete or false or manipulated information, the Commission has the power to impose an administrative fine in accordance with the provisions of subsection 6 of the above Article.

214. The AMLCO is responsible for preparation and submission of accurate monthly reports to the Commission. The Operator is required to provide the below information on monthly basis:

(a) Customer Due Diligence Measures Reporting

(b) Transactional Reporting

(c) Suspicious Activity Reporting

Customer Due Diligence Measures Reporting

215. The report must include the following:

(a) Total number of business relationships per country.

(b) Total number of new business relationships established within the reporting month per country.

(c) Total number of declined/terminated business relationships within reporting month per country.

(d) Total number of business relationships established with high risk customers in the reporting month per country.

(e) Total number of business relationships/occasional transactions with PEPs – Republic of Cyprus.

(f) Total number of business relationships/occasional transactions with PEPs – Foreign.

(g) Total number of:

- High risk customers
- Medium risk customers
- Low risk customers

(h) Number of customers for which the Operator was not able to perform Customer Due Diligence measures within the reporting month:

- Limassol

- Nicosia
- Larnaca
- Ayia Napa
- Paphos

Transactional Reporting

216. The report must include the following:

(a) Total number of individual transactions with the amount of €2,000 or more during the reporting month.

(b) Total number of customers who have performed individual transactions with the amount of €2,000 or more concerned at:

- Limassol
- Nicosia
- Larnaca
- Ayia Napa
- Paphos

(c) Total number of linked transactions with individual value below €2,000 but with cumulative value of €2,000 within same premises.

(d) Total number of customers who performed linked transactions with individual value below €2,000 but with cumulative value of €2,000 within same premises concerned at:

- Limassol
- Nicosia
- Larnaca
- Ayia Napa
- Paphos

(e) Total number of linked transactions with individual value below €2,000 but with cumulative value of €2,000 within different premises.

(f) Total number of customers who performed linked transactions with individual

value below €2,000 but with cumulative value of €2,000 within different premises concerned at:

- Limassol
- Nicosia
- Larnaca
- Ayia Napa
- Paphos

(g) Total number of individual redemptions in cash in excess of €10.000:

- Limassol
- Nicosia
- Larnaca
- Ayia Napa
- Paphos

(h) Total number of individual redemptions through funds transfers in excess of €10.000 from the Operator's account to an account of the casino customer's choice:

- Limassol
- Nicosia
- Larnaca
- Ayia Napa
- Paphos

(i) Total number of individual redemptions in cheques issued by the Operator in excess of €10.000:

- Limassol
- Nicosia
- Larnaca

- Ayia Napa
- Paphos

(j) Total number of individual redemptions in excess of €10.000 credited, in accordance with the casino customer's instructions into the casino customer's credit account or any other casino customer's account with the Operator:

- Limassol
- Nicosia
- Larnaca
- Ayia Napa
- Paphos

Suspicious Activity Reporting

217. The report must include the following:

(a) Number of ISRs submitted by the Operator's employees to the AMLCO relating to:

- Limassol
- Nicosia
- Larnaca
- Ayia Napa
- Paphos

(b) Number of investigations /evaluations conducted by the AMLCO for suspicious activity and for which a report was not submitted to MOKAS.

(c) Number of reports submitted by the AMLCO to MOKAS.

(d) The main reasons for suspicion identified within the report.