

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING PROCEDURE

1. INTRODUCTION

1.1. This site is operated by Omega Entertainment N.V., with company registration number 145632 and registered address located at Seru Loraweg 17-C, Curacao, that is authorized by the Government of Curaçao to conduct gaming operations under application (OGL/2024/558/0973) for a gaming license in progress with the Curaçao Gaming Authority.

1.2. This Anti-Money Laundering and Counter-Terrorism Financing Procedure (hereinafter "Procedure") outlines the general unified standards and procedures of Anti-Money Laundering ("AML"), Counter Terrorist Finance ("CTF"), Counter Fraud Procedures, regulations, Risk-Based approach.

1.3. Money Laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of funds originating from an illegal origin. Terrorist financing can be similarly described although the funds used for terrorist financing may in fact be of legitimate origin.

1.4. The ability to launder the proceeds of criminal activity through the financial systems of the world is vital to the success of criminal operations. Money is the lifeblood of terrorist organizations and vital to the mounting of terrorist activity.

1.5. Throughout this policy, the terms AML and CFT are to be used interchangeably.

1.6. Historically, efforts to combat money laundering concentrated on the activities of the traditional banking sector. However, criminals have responded to the measures taken by banks over recent years. They have invested in other methods of converting illegally obtained money.

1.7. Omega Entertainment N.V. will always seek to disrupt this activity by cooperating fully with the authorities and reporting all suspicious activity to Financial Intelligence Unit Curaçao.

1.8. All Omega Entertainment N.V. staff members are responsible for considering the AML manual and understanding responsibilities. All staff members must ensure that Omega Entertainment N.V. procedures are adhered to and must obtain all documentary evidence as outlined within Procedure. In addition, staff members must ensure that all suspicious circumstances are immediately reported to MLCO.

1.9. All contact with Law Enforcement Agencies will be handled by the MLCO.

1.10. The MLCO is responsible for providing and distributing information and updates to the legislation as and when they occur.

1.11. The Procedure is developed and periodically updated by the MLCO based on the general principles set up by the Company's Director in relation to the prevention of Money Laundering and Terrorist Financing.

2. DEFINITIONS

2.1. AML - Anti-Money Laundering.

2.2. CFT - Combating the Financing of Terrorism.

2.3. Money Laundering –

2.3.1. the conversion or transfer of property, in the knowledge that such property is derived from a criminal act or from involvement in such an act, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action.

2.3.2. the concealment or disguise of the true nature, origin, source, location, disposition, movement, rights with respect to, or ownership of property, in the knowledge that such property is derived from a criminal act or from involvement in such an act.

2.3.3. the acquisition, possession or use of property, in the knowledge, at the time of acquisition/transfer, that such property was derived from a criminal act or from involvement in such an act.

2.3.4. preparation attempts to commit and association to commit any of the acts referred to in points 2.3.1., 2.3.2. and 2.3.3. of this paragraph.

2.4. Terrorist financing - the financing and supporting of an act of terrorism and commissioning thereof within the meaning of Terrorist organization. A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act.

2.5. Money laundering compliance officer (hereinafter referred as to MLCO) - an independent officer with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure, with sufficient seniority to take decisions affecting its risk exposure, and who need not, in all cases, be a member of the management board.

2.6. Politically exposed natural person (PEP) means a natural person who is or who has been entrusted with prominent public functions including a head of State, head of government, minister and deputy or assistant minister; a member of Parliament or of a similar legislative

body, a member of a governing body of a political party, a member of a Supreme Court, a member of a court of auditors or of the board of a Central Bank; an Ambassador, a Chargé d'Affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a State-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organization, except middle-ranking or more junior officials.

2.7. Unusual monetary operation or transaction - a monetary operation or transaction relating to property, which is suspected of being, directly or indirectly, derived from a criminal act or from involvement in such an act and/or is, suspected of being associated with terrorist financing.

2.8. Customer (client) - a customer, who has the approved age and who participates in a game of chance.

3. LEGISLATION

3.1. According to the National Ordinance on Combatting Money Laundering and the Financing of Terrorism (as amended from time to time), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others (but not limited to):

- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2017, no. 99 (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no.73).
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2017, no. 92 (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.
- Sanctions National Ordinance (N.G. 2014, no.55).
- Kingdom Sanction Act (N.G. 2016, no.54).
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no.2).

- National decree for general measures of July 10, 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no.29).
- National Decree for general measures, as of July 10, 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no.28).
- National Decree for general measures, as of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006). 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no.30).
- The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70).

3.2. As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting international standards by regularly implementing these standards in its national legislation. On an international level, the FATF plays a very important role in the combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally. In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 39 countries are members of the FATF. Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, Omega Entertainment N.V. is free to develop additional procedures to comply with local regulations

4. OUR OBLIGATIONS

Omega Entertainment N.V. has robust policies and procedures in place in order to adhere to AML obligations, and its senior management is committed to combatting the abuse of its facilities, products and services.

4.1. Omega Entertainment N.V. designates a MLCO, who is a senior officer at management level and independent from the games operations, to be responsible for detection and deterrence of money laundering and terrorist financing as required by applicable laws and regulations, and for liaising with the Financial Intelligence Unit (FIU) of Curaçao. The MLCO has access to customer identification data and other CDD information, transaction records, and other relevant information in order to conduct their duties.

4.2. Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a compliance officer may be appointed as a MLCO.

4.3. MLCO obligations include but are not limited to:

4.3.1. establishment of appropriate internal control procedures with the purpose of prevention of monetary operations and transactions related to money laundering and/or terrorist financing: customer and beneficial owner due diligence, submission of reports and information to the Financial Intelligence Unit Curaçao, storage of information according to Money Laundering Regulation, risk assessment, risk management (taking into account the type of product, service or transaction, geographical risk, etc.), compliance management and communication;

4.3.2. undertaking of appropriate measures so that their relevant employees are aware at all times of the provisions currently in force. Such measures shall include participation of the relevant employees in special ongoing training programs to help them recognize operations which may be related to money laundering and/or terrorist financing and provision of instruction to said employees as to how to proceed in such cases.

4.3.3. controlling overall compliance policy for prevention of money laundering and/or terrorist financing and ensuring adequate resources are provided for the proper training of staff and the implementation of risk systems. This includes computer software to assist in oversight.

4.3.4. keeping copies of all training materials. Updated AML training is given annually at minimum plus additional training when the need arises, for example in the case of significant changes in the Legislation. Records must be retained of all training sessions including dates, personnel, who received training (name, surname, functions in the company, their signatures), compliance officer who trained staff (name, surname, functions in the company, their signatures);

4.3.5. monitoring all amendments in the Legislation aimed at prevention money laundering and/or terrorist financing and updating internal instructions according to up-to-date information. The internal instructions must be updated at least once a year;

4.3.6. investigating, analyzing, consulting and, if appropriate, report the activity to the FIU and take any other action considered legal and necessary.

In carrying out the above obligations, Omega Entertainment N.V. strives to always uphold and maintain the following principles:

- Omega Entertainment N.V. only carries on a business with persons who are adequately identified and do not detect any suspicion of criminal or terrorist activity.
- Omega Entertainment N.V. undertakes all measures at its capacity not to be used as a facility for laundering money or assisting others to do so intentionally or otherwise.
- Omega Entertainment N.V. endeavors to verify the data supplied by customers upon registration and first withdrawal request, through methods and data available depending on country of residence.
- Omega Entertainment N.V. obtains reasonable information, adequately documented and corroborated, about the identity of customers when required to do so under remote gaming regulations.
- Omega Entertainment N.V. provides training for its employees (including new employees, cashiers, audit staff, AML compliance staff, supervisors, managers, senior management, board of directors (as applicable) in anti-money laundering, prevention of terrorism and fraud procedures.
- Omega Entertainment N.V. takes all necessary measures to detect and prevent fraudulent customers and activity through regular monitoring of customer activity.
- Omega Entertainment N.V. complies with the applicable laws and regulations relating to anti-money laundering and the prevention of terrorism, and follows, as much as possible, the recommendations of FAFT.
- Omega Entertainment N.V. keeps records of all procedures carried out and reporting effected.

5. CUSTOMER'S RISK ASSESSMENT

5.1. For the purpose of identification, assessment and analysis of risks of money laundering and terrorist financing related to their activities, Omega Entertainment N.V. conducts a risk assessment. Steps are taken to identify, assess and analyze risks that are proportionate to the nature and level of complexity of the economic and professional activities of Omega Entertainment N.V. The following are considered of at least the following risk categories:

5.1.1. risks relating to customers.

5.1.2. risks relating to countries, geographic areas or jurisdictions.

5.1.3. risks relating to products, services or transactions.

5.1.4. risk relating to communication, mediation or products, services, transactions or delivery channels between Omega Entertainment N.V. and customers.

5.2. The steps taken to identify, assess and analyze risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of Omega Entertainment N.V. and/or the players.

5.3. AML screening is conducted on existing or potential customers to assess their risk. When conducting screenings, Omega Entertainment N.V. seeks to achieve the following objectives:

- conduct a risk assessment
- avoid violating sanctions
- protect from regulatory fines

Omega Entertainment N.V. performs AML screening of its customers upon account opening and/or upon their first withdrawal requests and/or when customers engage in financial transactions equal to or above Naf. 4,000 (or prior thereto) and/or when risk levels of customers change. With AML screening, Omega Entertainment N.V. ensures that existing or potential customers are not present on any of the sanction's lists, banned or wanted lists, are not classified as PEPs and do not have any adverse media data on file. To perform AML screening, Omega Entertainment N.V. first obtains the full name, date of birth, address and contact details of the customer. PEPs and sanctioned individuals are not allowed as customers. Further, Omega Entertainment N.V. does not allow anonymously gambling.

5.4. As a result of the risk assessment, Omega Entertainment N.V. maintains the following risk classification:

5.3.1. Low risk. Players who are classified as Low risk and are subjected to Standard Due Diligence procedures related to the request for KYC documentation as per the process described above and constant monitoring of activities on account.

5.3.2. Medium risk. Players who fail to provide the requested documentation at a stage where this is required (for example, where it has been requested due to defined triggers, PEPs, increase in volume of transactions), the account will be under increased monitoring.

5.3.3. High risk. Player's activity is the determining factor for the classification of a Player as High Risk. Any Player of which an automated alert has been generated, or an inappropriate

activity has been detected, will be categorized as High Risk for which an Enhanced Due diligence procedure is applied. The instances in which a High-risk classification is assigned includes but are not limited, to those instances as mentioned in the section below.

5.4. The Customer Acceptance Policy of Omega Entertainment N.V. is based on what is required under applicable legislation. The following people are not accepted as customers:

- Under 18
- PEPs
- Individuals on FAFT, UN, EU, UK or OFAC sanctions lists
- Residents in countries classified and/or prohibited as high risk by the applicable competent authorities
- Individuals suspected of ML/ TF involvement or other types of criminal activity
- Self-excluded customers
- Individuals who have submitted documentation or information which we have reasonable grounds to suspect is fake or fraudulent

5.5. Categories of customers whose activities may indicate a higher risk include:

- customers who have multiple sources of income
- customers with irregular income streams
- PEPs
- high spenders
- disproportionate spenders
- casual customers like locals or tourists especially when spending pattern changes
- improper use of third parties
- customers using multiple casino player rating accounts

5.6. Omega Entertainment N.V. also takes into consideration geographical risks which are assessed by the location of the player and the source of wealth in the business relationship. Nationality, residence and place of birth of the player are taken into account.

6. POLITICALLY EXPOSED PERSONS

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

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

6.2. Omega Entertainment N.V. pays more attention when the customer originates from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards.

6.3. In order to effectively manage such risks, Omega Entertainment N.V. assesses the countries of origin of their client in order to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the 40+9 requirements of the Financial Action Task Force.

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

7. CUSTOMER DUE DILIGENCE & VERIFICATION

Customers must be identified, and their identity may be verified.

Omega Entertainment is obligated to conduct a Customer Due Diligence when:

- customers engage in financial transactions equal to or above Naf. 4,000;
- carrying out occasional transactions above the monetary equivalent of Naf. 4,000;

- there is suspicion of money laundering and/or terrorist financing and/or illegal activities; or
- there are doubts about the veracity or adequacy of previously obtained customer identification data.

A transaction may be a single transaction but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of Naf. 4,000.

7.1. Standard Due Diligence. OMEGA ENTERTAINMENT N.V. requests identification and verification of the identity of the Customer (as set forth in paragraph 7).

7.2. Standard Due Diligence is conducted in the following cases:

7.2.1. anytime during the Customer onboarding;

7.2.2. upon a request for withdrawal; and/or

7.2.3. in accordance with applicable laws and regulations that may be required from time to time;

7.2.4. anytime at the discretion of Omega Entertainment N.V.

7.3. OMEGA ENTERTAINMENT N.V. further reserves the right to conduct a phone verification of the Customer Account to verify details provided by the Customer at the time of registration or at any other time requested by Omega Entertainment N.V. The adequate timeframe for completion of standard due diligence may vary depending on several factors, such as the volume of documentation provided, the complexity of the verification process, and the workload of the operator's verification team. In general, OMEGA ENTERTAINMENT N.V. aims to complete standard due diligence within a reasonable time frame, which can range from a few hours to a few business days. It's important to note that OMEGA ENTERTAINMENT N.V. is required to comply with regulatory requirements for customer identification and verification, which may affect the time frame for completion of the process. If you have any concerns or questions about the time frame for completion of due diligence, it's recommended to contact the customer support team for clarification.

7.4. OMEGA ENTERTAINMENT N.V. further reserves the right to conduct a phone verification of the Customer Account to verify details provided by the Customer at the time of registration or at any other time requested by OMEGA ENTERTAINMENT N.V.

7.5. Enhanced Due Diligence. In certain specific instances Omega Entertainment N.V. will conduct Enhanced Due Diligence by requesting the following KYC information (additionally notwithstanding requirements set forth in paragraph 7):

7.5.1. A selfie of the Customer holding the identification document.

7.5.2. A recently issued utility bill or bank statement.

7.5.3. A bank statement showing the initial deposit.

7.5.4. A bank statement not older than 6 months from the bank to which a withdrawn amount should be deposited.

7.5.5. Information regarding the source of wealth. Source of wealth is the origin of all the money a person has accumulated over their lifetime to include (but not limited to) employment income, inheritance, investments, business ownership interests.

7.6. There are also following Enhanced due diligence measures applicable:

7.6.1. receiving and verifying the information about the residential address of the customer.

7.6.2. continuous monitoring of the customer account activity, including tracking transactions conducted during a relationship, regular checking of the data used to identify the person, updating relevant documents, data, and information, and, if necessary, identifying the source and origin of the funds used in the transaction.

7.7. Enhanced Due Diligence is applied as soon as a Customer is classified as a High risk including but not limited to the following situations and as further discussed in the section 'Monitoring of Account Holder activities:

7.7.1. when there are doubts about the veracity or authenticity of the previously obtained identification data of the Customer.

7.7.2. in any other case, when there are suspicions that the act of money laundering and/or terrorist financing is, has been or will be carried out.

7.7.3. upon suspicion of a Customer attempting to or having created multiple Customer Accounts in multiple different names.

7.7.4. upon suspicion of Customer(s) being part of a syndicate of Customers colluding to gain an advantage over Omega Entertainment N.V.

7.7.5. upon suspicion of the Customer being a politically exposed person (PEP)

7.7.6. at the detection of any irregular, suspicious, inappropriate or fraudulent activity

7.7.7. for customers located in a high-risk location.

7.8. Omega Entertainment N.V. will process Enhanced Due Diligence within a reasonable timeframe, as specified by Omega Entertainment N.V. This timeframe may vary depending on the nature of the information requested and other factors.

7.9. If Omega Entertainment N.V. is not able to verify the identity of the Customer based on the provided documentation and further efforts, Omega Entertainment N.V. reserves the right to put the Customer Account on hold pending the provision of verification information, or to terminate the account if it finds the information contained in the Customer Account to be false or misleading.

7.10. OMEGA ENTERTAINMENT N.V. employees shall be prohibited from establishing or continuing any relationships and carrying out transactions when it is not possible to fulfil the due diligence requirements established in this procedure:

7.10.1. where, in the cases established by this procedure, the Customer fails to submit the data confirming his identity and his residential address, or where he submits incomplete data;

7.10.2. where the data are incorrect, or where the Customer avoids submitting the information required for establishing his identity or the submitted data are insufficient for that purpose.

7.11. OMEGA ENTERTAINMENT N.V. shall be prohibited from establishing or continue any relationships without requesting the Customer to submit data confirming his identity as per section 6.1., or where there is a substantiated suspicion that the data recorded in these documents are false or falsified.

7.12. In the period of cooperation with the customer OMEGA ENTERTAINMENT N.V. must in all cases:

7.12.1. carry out the ongoing monitoring of the Customer's activity on his account, used payment methods for refilling his balance and withdrawal transactions, including scrutiny of transactions undertaken throughout the course of such relationships, to ensure that the transactions being conducted are consistent with OMEGA ENTERTAINMENT N.V. knowledge of the customer, risk profile as well as the source of funds. Source of funds refers to how funds for a particular transaction were obtained by the player such as personal savings, pension release, property sales, share sales and dividends.

7.12.2. to ensure that the documents, data or information submitted by the Customer during due diligence are appropriate, relevant, regularly reviewed and kept up to date.

7.13. Customers under 18 are not allowed to register. The system prevents minors from registering by checking on the date for birth. The system does not allow the registered USA residents.

7.14. For verification of payment methods used by the customers to add funds to their accounts OMEGA ENTERTAINMENT N.V. may ask:

7.14.1. photo of a credit card(s) used to make the deposit (the front side with the first 6 digits and the 4 last digits, the expiry date, and the name of the card owner all visible, rear side with the CVV covered).

7.14.2. bank statement of the account from which the deposit was made for a period of the last 6 months displaying the name of the account holder.

7.14.3. a screenshot from the personal account of the customer in the payment system displaying the transfer of the funds in favor of OMEGA ENTERTAINMENT N.V. (in case when e-wallet is used for making deposits).

7.14.4. if the Customer's preferred method of adding the funds to his account is through his e-wallet, where funds can be added only by wire transfer or credit card, OMEGA ENTERTAINMENT N.V. may additionally ask to provide an account statement of the credit institution confirming the origin of the deposit.

7.14.5. if the Customer is adding funds to his account using other payment, OMEGA ENTERTAINMENT N.V. may ask to prove of the legitimacy of funds used for the deposit.

7.14.6. OMEGA ENTERTAINMENT N.V. may ask for a screenshot from a personal e-wallet account to confirm the name of the account holder.

7.15. OMEGA ENTERTAINMENT N.V. may, in accordance with internal policies and internal control procedures, refuse to execute the monetary operations or transactions and terminate the transactions or relationship with the Customer, where the customer avoids submitting, or refuses to submit, additional information to an OMEGA ENTERTAINMENT N.V., at its request and within the specified time limits.

7.16. **Ongoing Due Diligence.** Continuous monitoring is conducted by Omega Entertainment N.V. where customer behavior and/or activities and/or transaction(s) are deemed to be or suspected to be unusual according to applicable laws and regulations, in which case further investigation are undertaken and/ or shall be subject to periodical review, in the following instances (but not limited to):

- inactivity period followed by intense activity
- game type behavior and amounts played
- withdrawals amongst against deposits amounts
- transaction behavior
- payment method use

7.17. During the period of cooperation, Omega Entertainment N.V. is obliged in all cases to

- carry out the ongoing monitoring of the Customer's activity, used payment methods, including scrutiny of transactions undertaken throughout the course of such relationships, to ensure that the transactions being conducted are consistent with Omega Entertainment N.V. knowledge of the Customer, risk profile as well as the source of funds;
- ensure that the documents, data or information submitted by the Customer during due diligence are appropriate, relevant, regularly reviewed and kept up to date;
- pay attention to any activity which they regard as likely, by its nature, to be related to money laundering and/or terrorist financing, and in particular to complex or unusually large transactions, and relationships or deposits/withdrawals with Customers from third countries in which, based on the information officially published by international intergovernmental organizations, money laundering and/or terrorist financing prevention measures are insufficient or do not correspond to international standards.

8. IDENTIFICATION

8.1. OMEGA ENTERTAINMENT N.V. identifies the Customer and retains the following data prior to account opening:

8.1.1. first name, surname.

8.1.2. personal identification code

8.1.3. date of birth, place of birth

8.1.4. a residential address

8.1.5. nationality

8.2. OMEGA ENTERTAINMENT N.V. verifies the identification data specified in clauses 8.1.1. and 8.1.2 based on a valid official identity document which includes a photograph of the holder:

8.2.1. driving license.

8.2.2. identity card.

8.2.3. travel-document or passport.

8.2.4. any other document designated by an official governmental authority.

8.3. The verification of the residential address may be carried out based on the following documents:

8.3.1. valid official identity document.

8.3.2. recent utility bill.

8.3.3. recent account statement or reference letter issued by a credit institution/financial institution.

8.3.4. correspondence from a central or local government authority, department or agency.

8.3.5. any other documents issued by independent agency.

8.4. In case the employees of Omega Entertainment N.V. have suspicions about the Customer's identity document specified in section 8.2., they may ask to provide the copy of the identity document authenticated by a notary or certified by a notary.

9. REPORTING OF UNUSUAL MONETARY OPERATIONS OR TRANSACTIONS

9.1. Omega Entertainment N.V. is required to abide by the National Ordinance for Identification of Services and also required to detect and report either intended or completed unusual transactions. OMEGA ENTERTAINMENT N.V. pays attention to any activity which they regard as likely, by its nature, to be related to money laundering and/or terrorist financing, and in particular to complex or unusually large transactions, and all unusual patterns of transactions which have no apparent economic or visible lawful purpose, and any relationships or monetary operations with customers from third countries in which, based on the information officially published by international intergovernmental organizations, money laundering and/or terrorist financing prevention measures are insufficient or do not correspond to international standards. OMEGA ENTERTAINMENT N.V. examines the basis for and purpose of execution of such operations or transactions and the results of the investigation that must be recorded in writing.

9.2. MLCO must report to the Financial Intelligence Unit Curaçao any suspicious or unusual monetary operations or transactions. Omega Entertainment N.V. and its employees and/or representatives and/or the person who acted on their behalf are not liable for damage caused to a person or customer participating in a transaction made in economic or professional activities, in performing a professional act on the provision of a professional service

9.2.1. upon performance of duties and obligations arising from AML and TF regulations in good faith, from failing to make the transaction or from failing to make the transaction within the prescribed time limit.

9.2.2. in connection with the performance of the duty to report in good faith.

9.3. The following transactions or intended transactions are deemed unusual:

9.3.1. cases where it is aware of, obtains information concerning, has suspicions or has substantial grounds to suspect that money laundering and/or terrorist financing was, is, or will be performed, or it has been attempted.

9.3.2. cases where they have suspicion or sufficient grounds to suspect that the customer's funds have been obtained from criminal activity.

9.3.3. cases where they have a suspicion or sufficient grounds to suspect that the transactions or activities are related to terrorist financing.

9.3.4. transactions by or on behalf of a person who is named on a list adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55).

9.3.5. transactions in the amount of Naf. 5,000 or more (such a transaction may be a single transaction or a series, combination or pattern of transactions involving a total amount of the monetary equivalent of Naf. 5,000 or more and is considered per gaming day).

9.4. There are indicators helping to identify unusual transactions. Indicators describe when a transaction (executed or intended) is to be labeled as unusual and thus must be reported to the Financial Intelligence Unit Curaçao without delay. The term "without delay" is interpreted as follows:

9.4.1. MLCO should send unusual transaction reports within 48 hours after the transaction has been executed, or after there has been an intention of a transaction.

9.4.2. In individual cases the reporting to Financial Intelligence Unit Curaçao might be extended to a maximum of 5 working days. A request for extended reporting should be directed in writing to the Financial Intelligence Unit Curaçao, stating the reasons for the extension.

9.4.3. The Financial Intelligence Unit Curaçao will inform the respective reporting entity in writing of its decision within 24 hours.

9.4.4. The time period between the execution of the transaction (or the intention to execute a transaction) and the moment the MLCO receives the report, should not exceed 24 hours.

9.4.5. As of the moment that the MLCO receives the transaction report, he must complete the relevant research with regard to a possible Money Laundering/Terrorism Financing within 10 working days.

9.4.6. If after the research period (maximum of 10 working days), there is a suspicion of Money Laundering/Terrorism Financing, the MLCO must report the transaction within 48 hours to the Financial Intelligence Unit.

9.4.7. In the case it is not possible to comply with the above-mentioned time periods, the MLCO shall send a request for reporting extension in writing to the Financial Intelligence Unit Curaçao, stating the reasons for this extension.

9.4.8. The Financial Intelligence Unit Curaçao will evaluate objective grounds and inform the reporting entity on its decision in writing within 48 hours upon receiving the request.

9.5. There are two kinds of indicators: objective and subjective:

9.5.1. in case of an objective indicator (see the Annex 1), it describes mandatory under which circumstances a transaction is to be considered as unusual.

9.5.2. in case of a subjective indicator (see the Annex 1), the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, and any other circumstance that may be relevant) has reasonable indications to presume that a transaction is related to money laundering or terrorism financing. For subjective indicators, red flags can be suggested by the supervisors and/or the FIU Curaçao that indicate such possible presumptions.

9.6. A report to the FIU is submitted via GoAML reporting portal (link to register in GoAML - <http://mot.cw/Web/MOTWeb/MOTWeb.nsf/web/goaml%20the%20new%20portal%20for%20fiu%20curacao>)

9.7. The structural unit of OMEGA ENTERTAINMENT N.V., a member of a management body and an employee are prohibited to inform a person about a report submitted on them to the Financial Intelligence Unit, a plan to submit such a report or the occurrence of reporting as well as about any precept made by the Financial Intelligence Unit or about the commencement of criminal proceedings.

9.8. The prohibition provided for in section 8.9. is not applied upon submission of information to competent supervisory authorities and law enforcement agencies.

9.9. OMEGA ENTERTAINMENT N.V. shall establish a system of measures ensuring that the employees and representatives of the entity reporting of a suspicion of money laundering or terrorist financing to the Financial Intelligence Unit are protected from being exposed to threats or hostile action by other employees, management body members or customers of OMEGA ENTERTAINMENT N.V., in particular from adverse or discriminatory employment actions.

10. STORAGE OF INFORMATION

10.1. OMEGA ENTERTAINMENT N.V. must keep a register of reports of unusual monetary operations and transactions specified in section 8.3. of this procedure.

10.2. OMEGA ENTERTAINMENT N.V. must keep a register of the customers with whom transactions or relationships were terminated under the circumstances specified in section 6.6. of this procedure or under any other circumstances related to violations of the procedure for the prevention of money laundering and/or terrorist financing.

10.3. Register data, correspondence with customers and all necessary records on transactions (both domestic and international) are stored in paper or electronic format by Omega Entertainment N.V. for at least five years from the date of termination of transactions or relationships with the customer, in order for Omega Entertainment N.V. to comply with applicable legislation and as well with information requests from competent authorities.

10.4. Copies of the identity documents of the customer, other data received at the time of establishing the identity of the customer must be stored for five years from the date of termination of transactions or relationships with the customer.

10.5. Time limits for storage may be additionally extended upon receipt of a reasonable request from a competent institution.

10.6. OMEGA ENTERTAINMENT N.V. must store the personal data of staff referred to in section 10.4. of this procedure for five years upon termination of employment.

11. TRAINING

11.1. In providing the specified categories of employees with the AML/CTF training, OMEGA ENTERTAINMENT N.V. takes into consideration the knowledge and qualifications necessary for the duties, responsibilities and authorization of staff. OMEGA ENTERTAINMENT N.V., within the framework of the training, explains to staff the AML/CTF requirements and provide detailed information on the measures and activities the staff are expected to conduct within the framework of their responsibilities.

11.2. OMEGA ENTERTAINMENT N.V. develops and documents s staff training plan which contains at least the following programs:

11.2.1. an internal training program for staff, which uses internal training resources (hereinafter referred to as the “internal training”).

11.2.2. a training program for new employees (employees who have just started to perform their duties or changed position at OMEGA ENTERTAINMENT N.V. (hereinafter referred to as the “new staff training”).

11.3. In addition to the internal training program referred to in subsection 11.2.1. of the present Regulations, OMEGA ENTERTAINMENT N.V. shall ensure extraordinary staff training in the cases referred to in section 11.6. of this procedure.

11.4. OMEGA ENTERTAINMENT N.V. shall ensure that the information on the staff training conducted is saved by documenting the following data:

11.4.1. name of the training.

11.4.2. personal data of the trained employee.

11.4.3. position and structural unit of the trained employee.

11.4.4. training venue.

11.4.5. head and organizer of the training.

11.4.6. time of training.

11.4.7. duration of the training.

11.4.8. result of knowledge tests and certificate obtained, if any.

11.5. OMEGA ENTERTAINMENT N.V. ensures that, in addition to the internal and external training, any employee may obtain the necessary advice from senior employees involved in the AML/CTF risk management.

11.6. In addition to the internal training, OMEGA ENTERTAINMENT N.V. ensures extraordinary staff training in AML/CTF issues at least in the following cases:

11.6.1. new internal and external regulations governing the AML/CTF have come into force and are applicable to the staff of OMEGA ENTERTAINMENT N.V.

11.6.2. new services have been introduced which cause changes in AML/CTF risk exposure.

11.6.3. during the performance of his/her duties an employee violates the internal and external regulations governing the AML/CTF due to insufficient knowledge.

12. INTERNATIONAL SANCTIONS

12.1 Omega Entertainment N.V. is prohibited from engaging in any actions that are banned under the international sanctions imposed in Curacao. Omega Entertainment N.V. is also prohibited from accepting transactions the execution of which would conflict with international sanctions implemented in the Curaçao.

12.2. Prospecting Customers from countries that pose high ML/TF risks which lie outside of the business risk appetite shall be blocked from registration and/or login. The Compliance department reviews the list of accepted countries on a regular basis, in line with certified and credible sources of information regarding the level of ML/TF risks, corruption, political

unrest, and countries subject to sanctions (see Appendix A for the compiled list of banned countries), embargos or similar measures, countries with no or little AML Regulations and monitoring by FATF, or countries providing funding and/or support for terrorism.

Annex 1

PROVIDERS OF INTERNET GAMING AND GAMBLING

Objective indicators

A. A transaction which is reported to the police or judicial authorities

Indicator	Definition
G0000111	A transaction which is reported to the police or judicial authorities in connection with money laundering or financing or terrorism.

B. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance.

G0000114	An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions National Ordinance.
----------	---

C. A transaction amounting to NAF (ANG) 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner; This comprises in any case the following situations:

G0000135	1. A giro-based transaction amounting to NAF (ANG) 5,000.00 or more: A giro-based transaction is a transfer from a bank account of the service provider to a local or international bank accounts carried out at the request of the client addressed to the service provider. 2. The taking into deposit or the releasing out of deposit of an amount of NAF(ANG) 5,000.00 or more at the request of the client. 3. Sale of tokens to a client in the amount of NAF (ANG) 5,000.00 or more. The term "tokens" includes at least chips and credits.
----------	--

4. Pay-out of prizes in the amount of NAF (ANG) 5.000,-- or more.

5. All other cases.

NB In case of Indicator G0000135: please indicate the applicable sub-indicator (1,2,3,4 or 5) when reporting a transaction. In case of sub-indicator 5, please always provide a description of the situation.

Subjective indicator Suspected money laundering transactions or financing of terrorism.

Indicator	Definition
G0000211	A transaction giving cause to assume that it may be connected with money laundering or terrorist financing.

The following applies for all indicators in these annexes:

- for all amounts mentioned in NAF (ANG): this encompasses both the amount in NAF (ANG) as well as the equivalent thereof in foreign currency;
- the transaction concept encompasses both realized and intended transactions.



(SMES) Solutions for Management Employment Support N.V.

Managing Director

17.08.2026