

Anti-Money Laundering, Countering Financing of Terrorism and Combating Proliferation Financing Policy (AML/CFT/CPF).

Last updated: 02.08.2024

Version 1.3.

1. Introduction

Bets Entertainment N.V. (referred to as either "the Company", "Casino", "We" in this Policy) having its registered office at Abraham de Veerstraat 9, Curaçao, Company Registration number 155648, has developed a comprehensive risk-based Anti-Money Laundering, Countering Financing of Terrorism and Combating Proliferation Financing Policy ("the Policy", "the AML/CFT/CPF Policy") in an effort to maintain the highest possible compliance with applicable laws and regulations relating to anti-money laundering, countering financing of terrorism and combating proliferation financing.

The present AML/CFT/CPF Policy shall be regularly reviewed and, if necessary, revised to comply with applicable rules, regulations, policies, and best practices. The present AML/CFT/CPF Policy must be adhered to by the Company and Company's staff to mitigate reputational, regulatory, legal and financial loss risks.

2. Mission Statement

This document is intended to outline the Company's AML/CFT/CPF policies and procedures in order to ensure that:

- Statutory and regulatory obligations to prevent money laundering/financing of terrorism / financing of proliferation are met, taking positive action in order to minimize risk of the Company's services being used for the purpose of laundering the proceeds of criminal activity or terrorist financing.
- The Company does not engage with or continue established relationships with those whose conduct gives rise to suspicion of involvement with illegal activities. We will seek to terminate any relationship where conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities.
- Any such termination shall follow the reporting of the suspicions and thereafter shall be undertaken in conjunction with the relevant authorities and in accordance with the relevant regulations to avoid any risk to the Company.

- The Company complies with the obligations of relevant national and international legislation and regulation, adherence to Financial Action Task Force (FATF) recommendations, EU Directives and other applicable laws and regulations on the prevention of money laundering/financing of terrorism / financing of proliferation.
- The Money Laundering Reporting Officer (MLRO) will act as Key Official on behalf of the Company and is responsible for:
 - Receiving and assessing internal suspicion reports.
 - Taking reasonable steps to monitor and access any relevant “know your customer/business” information.
 - Making external reports to relevant national and international authorities.
 - Obtaining and using national and international findings concerning countries with inadequacies in their approach to money laundering prevention.
 - Taking reasonable steps to establish and maintain adequate arrangements for awareness and training.
 - Monitoring the day-to-day operation of the Company's Anti-Money Laundering, Countering Financing of Terrorism and Combating Proliferation Financing Policy.
 - Responding to relevant requests from regulators and law enforcement authorities.
 - Making compliance reports to the Company's senior management.

The Company is committed to high standards of anti-money laundering compliance and requires management and employees to adhere to these standards in preventing the use of its products and services for money laundering/financing of terrorism/financing of proliferation purposes.

3. Definitions of Money Laundering, Terrorist Financing and Proliferation Financing

According to Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (4th Money Laundering Directive), **Money Laundering** is defined as:

1. The conversion or transfer of property, knowing that such property is derived from criminal activity or from participation in such activity, 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 an activity to evade the legal consequences of that person's action.
2. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such activity.

3. The acquisition, possession or use of property, knowing, at the moment of receipt, that such property was derived from criminal activity or from an act of participation in such activity.
4. The participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to points 1, 2 and 3.

There are often three acknowledged phases of money laundering:

- **Placement** – the physical disposal of cash or other assets derived from criminal activity. During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses.
- **Layering** – the separation of the illicit proceeds from their source by layers of transactions intended to hide the origin of the funds. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities.
- **Integration** – supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appear to be personal transactions or normal business. However, even simple possession of criminal property may constitute an offence. Criminal property is defined as property which is, or represents, a person's benefit from criminal conduct, where the alleged offender knows or suspects that it is such.

Curacao Gaming Control Board (hereinafter – “GCB”) definition of money laundering:

- As provided in Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, May 2024: All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML).

Terrorist Financing is defined as:

The raising and processing of funds to supply terrorists with resources, the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 3 and 4 of Directive (EU)

2017/541 of the European Parliament and of the Council On Combating Terrorism. Terrorist financing entails soliciting, collecting, or providing funds with the intent of using them to support terrorist acts or organizations.

Curacao Gaming Control Board definition of terrorist financing (as provided in Regulations for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), August 2016): providing or collecting funds with the knowledge that they will be used in the commission of terrorist acts.

Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, May 2024:

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

Proliferation Financing is defined as:

The financial support for the proliferation of weapons of mass destruction, providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

The term „Proliferation Financing-related Targeted Financial Sanctions“ refers to specific sanctions outlined in European Union legal frameworks, aimed at preventing the spread of weapons of mass destruction.

Targeted Financial Sanctions are defined as:

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities. All natural and legal persons in Curaçao are required to freeze without delay and without prior notice, the funds or other assets of designated persons and entities. This is to comply with United Nations Security Council resolutions and the Common Foreign and Security Policy

of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. EU sanctions are binding for Curaçao on the basis of the Kingdom Sanctions Act.

4. Legal and Regulatory Framework

The Legal and Regulatory Framework is set by, without being limited:

EU Legislation:

- Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (4th EU Anti-Money Laundering Directive).
- Directive (EU) 2018/843 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (5th EU Anti-Money Laundering Directive).
- Commission Delegated Regulation (EU) 2018/1108 on Central Contact Points.
- Commission Delegated Regulation (EU) 2019/758 on Measures for Groups present in Certain Third Countries.
- Commission Delegated Regulation (EU) 2016/1675 on High Risk Third Countries.
- Regulation (EU) 2015/847 - Information accompanying transfers of funds. Regulation (EU) 2023/1113 - Regulation on information accompanying transfers of funds (recast).
- Regulation (EU) 2023/1114 - Regulation on Markets in Crypto-Assets.
- EU List of Prominent Public Functions (EUR-Lex - 52023XC00724). Prominent public functions at national level, at the level of International Organizations and at the level of the European Union Institutions and Bodies.
- Directive (EU) 2017/541 of the European Parliament and of the Council on Combating Terrorism.
- Payment card Industry (PCI) Data Security Standard V1.2 (October 2008).

FATF International Standards:

- FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems.
- FATF „Combating Proliferation Financing: A Status Report on Policy Development and Consultation“.

- FATF „Guidance on Counter Proliferation Financing“.
- FATF „Guidance on Proliferation Financing Risk Assessment and Mitigation“.
- EU Strategy Against the Proliferation of Weapons of Mass Destruction 15708/03.

Curacao Legislation:

- Sanctions National Ordinance (Sanctielandsverordening, PB 2014, no. 55).
- NOIS: the National Ordinance Identification for Services (Landsverordening identificatie bij dienstverlening, PB 2017, no. 92, GT).
- NOOGH: the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen, PB 1993, no. 63).
- Kingdom Sanction Act (N.G. 2016, no. 54).
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- NORUT: the National Ordinance on the Reporting of Unusual Transactions (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99).
- Appointment of the GCB as the AML/CFT supervisor for the LMOT for the gaming industry (no. 19/0283, Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector).
- National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector, LB van 28 januari 2019, no. 19/0282).
- Rules for reporting unusual transactions. (PB 2020, 157, Landsbesluit inzake regels voor melding ongebruikelijke transacties (Landsbesluit goAML meldportaal).
- Indicators for recognizing unusual transaction (PB 2015, 73, Regeling indicatoren ongebruikelijke transacties).
- Gaming Control Board. Regulations for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), August 2016.
- Caribbean Financial Action Task Force (CFATF) International Standards (Round Reports, Public Statements and Notifications).

- **Curacao Gaming Control Board:** Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, May 2024.

5. Regulatory Key Provisions

The 4th EU Anti-Money Laundering Directive contains the following provisions:

- Risk-based approach – all gambling operators are required to undertake customer due diligence on all transactions over 2,000 EUR: *for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.*
- Operators will have to develop, update and implement suitable written risk assessments, policies and procedures as well as processes for testing their effectiveness. Must be documented and made available to regulators and independent auditors.
- Staff must be fully screened and trained in AML/CFT.
- Must conduct enhanced due diligence where the risk profile of a customer indicates high risk and for domestic and foreign politically exposed persons (PEP). Simplified due diligence permitted for low-risk customers.
- Evidence of higher risk which are set out in Directive Annexes include size and frequency of transactions, customer residence in countries with significant corruption and crime and payments received from unknown parties.
- Records must be kept for a minimum of 5 years.

The 5th EU Anti-Money Laundering Directive addresses the following points:

- Cryptocurrencies are obliged to comply with the AML Regulations applied to financial institutions.
- Extension of sectors that are now “obliged entities” and in scope of the updated money laundering regulations. Includes: Crypto assets exchange providers – entities that either exchange virtual assets to money or to other virtual assets, or vice versa; Custodian Wallet Providers – entities that provide services to safeguard, hold, store and administer virtual assets on behalf of its customers. All newly obliged entities will require a full suite of policies, controls and procedures designed to meet their new regulatory obligations and designed for their specific business.
- Obligated entities need to be confident that they are using correct PEP definitions

and that PEP data they rely upon is accurate and up to date. As such, PEP lists (commercial or independently generated), need to be reviewed constantly to make sure the data is up to date and contains secondary identifiers such as date of birth, sex, nationality, photo and where possible, date appointed to office. Enhanced due diligence measures are still required if a PEP is identified.

- Obtaining beneficial owner information can be a huge challenge for obliged entities. Many registries around the world do not publish beneficial owner information, or else the information is partial and incomplete. Often organization structures are complex and include offshore entities. As a result, unpacking ownership structures and correctly identifying beneficial owners is a specialist skill requiring experienced and highly trained staff, particularly as these are the types of organization that are most likely to be used by financial criminals. It is advisable for obliged entities to work with an experienced provider in order to assist with this process.

Regulation (EU) 2023/1114 - Regulation on markets in crypto-asset contains the following provisions:

Crypto-asset service providers will have to conduct the money laundering and terrorist financing risk assessment, develop, update and implement suitable general policies and procedures related thereto. Legal persons or other undertakings that intend to offer to the public or seek the admission to trading of asset-referenced tokens shall submit their application for an authorization to the competent authority and provide a description of their internal control mechanisms and procedures to ensure compliance with the obligations in relation to the prevention of money laundering and terrorist financing under applicable EU regulations.

FATF Customer Profile Risk Indicators of the potential breach, non-implementation, or evasion of Countering Proliferation Financing measures:

- During on-boarding, a customer provides vague or incomplete information about their proposed activities. Customer is reluctant to provide additional information about their activities when queried.
- During subsequent stages of due diligence, a customer, particularly a trade entity, its owners or senior managers, appear in sanctioned lists or negative news, e.g., past ML schemes, fraud, other criminal activities, or ongoing or past investigations or convictions, including appearing on a list of denied persons for the purposes of export control regimes.
- The customer is a person connected with a country of proliferation or diversion concern, e.g., through business or trade relations – this information may be obtained from the national risk assessment process or relevant national CPF authorities.

- The customer is a person dealing with dual-use goods or goods subject to export control goods or complex equipment for which he/she lacks technical background, or which is incongruent with their stated line of activity.
- A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile established at onboarding.
- A customer affiliated with a university or research institution is involved in the trading of dual-use goods or goods subject to export control.
- A customer or counterparty, declared to be a commercial business, conducts transactions that suggest that they are acting as a money-remittance business or a pay-through account. These accounts involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons. In some cases, the activity associated with originators appear to be entities who may connected a state-sponsored proliferation program (such as shell companies operating near countries of proliferation or diversion concern), and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls.

6. Risk Based Approach

The risk-based approach recognizes that the AML/CFT/CPF risks faced by each sector and each subject person are different and allows for resources to be invested and applied where they are most required. The risk-based approach envisages the application of checks that are proportionate to the assessed risk. The cornerstone of the risk-based approach is the risk assessment which must be carried out at different stages of a subject person's activities. This assessment allows the subject person to identify its AML/CFT/CPF vulnerabilities and the AML/CFT/CPF risks it is exposed to. On this basis, the subject person will be able to draw up, adopt and implement AML/CFT/CPF measures, policies, controls and procedures that address any identified risks.

Applying Risk-based Approach means that a casino has to:

- Assess the risks that money laundering or terrorist financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Document their risk assessments, including everything that has been done and the reason for this being done.

The risk assessment considers all relevant risk factors, including the player, countries

or geographic areas, products and services (types of games of chance) that the casino offers and delivery channels, before determining what the level of overall risk is. Based on the risk assessment, the appropriate level and type of mitigation to be applied is determined. Casinos should also take notice of the outcomes of the National Risk Assessment (NRA) of the jurisdictions where they operate and take these outcomes into account when conducting their risk assessment. The risk assessment should also be made available to the GCB upon request.

Business Risk Assessment (BRA):

All factors that may have an impact on the risks of money laundering, financing of terrorism and financing of proliferation must be taken into account in the risk assessment, but special consideration must be given to the type of customers, products and services offered, delivery channels and geographical risk factors. Once the business risk has been assessed, the casino can set a risk appetite: it decides how much risk he is prepared to accept.

This risk assessment has to be documented and approved by the Board of directors of the casino. It should also be made available to the GCB upon request. All aspects of the Business Risk Assessment should be covered, including:

- The methodology adapted;
- The reasons for considering a risk factor as presenting a low, medium or high risk;
- The outcome of the BRA;
- Any information sources used.

Customer Risk Assessment (CRA):

The customer specific risk assessment has to be carried out either prior to the carrying out of an occasional transaction, or during establishing a business relationship. It is possible that this initial customer specific risk assessment will have to be revised at a later stage of the business relationship and this may result in a customer's risk rating having to be adjusted.

The Customer Risk Assessment will assess the particular risks the casino will be exposed to when providing its services or products to players. The information collected to draw up the CRA will formulate the customer's risk profile. On the basis of the CRA, the proper level of CDD can then be applied as stipulated in the Customer Acceptance Policy (CAP).

7. Risk factors specific to the Gambling Sector

1. Customer risk

The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. 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 (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Casual customers like locals, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (junket operators monitor player activity and issues and collect credit).

2. Geographical risk

The geographical risk is the risk posed to the casino by the geographical location of the player and the source of wealth of the business relationship. The nationality, residence and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered as high risk:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

3. Product, service and transaction risk

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being

more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by casinos of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
- Anonymous payment methods such as pre-paid cards and virtual assets;
- Use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
- Types of specific games (e.g. roulette, craps → even bets);
- Peer to peer gaming;
- The use by customer of accounts held or cards issued in the name of third parties;
- The transfer of funds from one gaming account to another;
- Multiple casino accounts or wallets (internet operator may own and control multiple web sites);
- Changes to financial institution accounts to fund casino account;
- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- Using cash to fund a pre-paid card poses similar risks as cash;
- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling.

4. Distribution channels risk

The channels through which a casino establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction:

- Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;
- While situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes unless the casino adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;
- Where there is the involvement of a third party in the interactions between the customer and the casino, there is also an increase of risk. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations.

8. KYC Procedure

Know Your Customer Procedures are followed to achieve the following objectives:

- Allowing only legitimate customers to register an account (i.e., to exclude from registration the following categories: Minors, Sanctioned Persons or Players from Sanctioned countries are not allowed to register a gaming account).
- Build the risk profile associated with the customer.
- Confirming that customers are who they say they are.
- Monitoring customer accounts and transactions for illegal activities.
- Blocking duplicate accounts.
- Identifying possible PEP & customers from countries identified as having significant levels of corruption or other criminal activity.

Identification refers to the collection of personal details of the player to establish the identity of the player. Verification on the other hand consists in confirming the personal details collected for identification purposes using reliable, independent source documents, data or information. The personal information required and extent of verification to be carried out, will vary depending on risk.

The Company has to make sure that customers are registering an account to play and transact exclusively on their behalf.

8.1. Registration:

Before being able to play on the website a customer needs to first register an account. On the registration page the customers are asked for the following details:

- Email address. In order to validate the email address of the player, an email with a link to validate the email address will be sent to the email address listed in the registration. A player will not be allowed withdraw funds unless his/her email address is validated.
- Full name
- Date of Birth
- Residence Address

Once the above information is received the fraud department will screen the information for any false or suspicious signs, possible duplicate/Self-Excluded accounts, Politically Exposed Persons and Sanction Lists.

Sanction Lists:

□ **U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List** Specially Designated Nationals And Blocked Persons List: <https://sanctionslist.ofac.treas.gov/Home/SdnList>

□ **EU Sanctions List:** <http://www.sanctionsmap.eu/#/main>

For PEP status screening the Company can rely on internet search or consult reports and databases on corruption risk, like the Transparency International Corruption Perceptions Index or on www.knowyourcountry.com

The IP address from where the traffic originated is tracked by the Company's back-office software. Should traffic originate from countries which are on the list of restricted countries, the account will be blocked.

Should the checks (manual or automatically done by the system) indicate that a duplicate account has been registered, the account is suspended until further checks are made. Further checks are aimed to determine whether this is indeed a duplicate account registered intentionally with the detrimental or offensive purpose.

Identification:

When identifying the player, at a minimum the following information must be collected:

- i. full name;
- ii. permanent residential address;
- iii. date of birth;
- iv. place of birth;
- v. nationality; and
- vi. identity number.

However, in low-risk scenarios the Company may limit identification to the three personal details set out in (i) to (iii) above. On the other hand, in high-risk situations, it is possible that a licensee considers the collection of additional personal details as necessary to mitigate the higher risk of ML/FT.

At this stage, a provisional risk rating will be assigned based on the initially collected information.

8.2. Age Verification

No customers under the age of 18 can register an account. The system does not allow persons under 18 to register an account. The Company reserves the right to request proof of age documents from persons intending to participate or participating in the gaming opportunities offered by the Company at any time. Acceptable proof of age documents includes valid government-issued photo IDs.

The Company takes all reasonable steps to prevent underage gamblers from accessing and using the Company's services, including the use of identity verification services to ensure that all users are eligible to play.

8.3. Verification

Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources. Verification is carried out for the casino to determine to its own satisfaction that the player is who he declared himself to be. What is important is that documents are clear, legible and of good quality. Verification of evidence of identity implies a check whether the document presented is legitimate and that it has not been stolen from the true owner. If the casino obtains foreign documentation, extra care should be taken with regard to verifying its authenticity, particularly where the type of document is unfamiliar.

Verification of identity has to be carried out by making reference to an unexpired government-issued document containing photographic evidence of the customer's identity (e.g. passport, identity card). Where such a document does not allow verification of the player's residential address, the casino can obtain other documents like a bank statement, utility bill, letter from a public authority or rental agreement, which should not be more than six months old to verify the residential address. The casino can also contact the player by letter, e-mail or telephone to verify the information supplied. It can also send a verification code to the e-mail address to verify that the address is current and genuine. Verification can also be done by checking social media, telephone directories, companies registries or media and news sources.

Where the casino does not have sufficient comfort that it knows its player, it is expected that it will take additional measures to do so. Some of these measures include requesting additional identification documents, asking the player to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

8.4. Standard Customer Due Diligence (CDD).

The Company collects, verifies, and authenticates KYC Due Diligence information regarding the customers. Standard KYC Due Diligence requires submission of the following documents:

- *Scan of identification document e.g., ID card or Passport.*
- *Valid proof of address e.g., utility bill (not older than 3 months).*
- *Proof of payment method ownership.*

In case the customer doesn't have an opportunity to provide the documents in Latin or Cyrillic alphabet, the Company reserves the right to demand video verification where the customer shows his/her documents.

The following events will trigger the Standard Due Diligence procedures:

- *Accumulated transactions of the customer (Deposits and/or Withdrawals) are equal to or above 2,000 Euro.*
- *The Company has doubts about the accuracy or adequacy of previously obtained customer identification data.*
- *Customer's activity raise suspicion, even if Customer's accumulated transactions are less than 2,000 Euro.*
- *Customer requests to change account details like address, email, any other profile details provided earlier by customer to the Company.*

Note: 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 2,000 Euro.

In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the casino obtains any necessary information from the customer concerned. However If the 2,000 Euro threshold is reached, the player cannot deposit funds into the account or withdraw funds from the account. Besides that, if the requested information and documentation is not received within 30 days from the moment the 2,000 Euro threshold was met in order for the casino to complete CDD, the casino has to terminate the relationship with the player and report the transaction to the FIU.

8.5. Enhanced Due Diligence (EDD)

In cases where players, products or transaction are deemed to be of higher risk, Enhanced Due Diligence (EDD) procedures should apply. The following events should trigger the EDD procedures:

- *Player is a PEP (Politically Exposed Person) or becomes a PEP after establishing business relationship with the Company.*
- *Duplicate IPs.*
- *IP shifting.*
- *Country of origin associated with higher credit card fraud.*
- *Attempts to create multiple accounts.*
- *Attempting to withdraw funds without using the funds to play (withdrawal without making any bets or starting any game session).*
- *Sudden changes in account activity.*
- *The registered country is not part of the FATF whitelist, or the registered country is any other country that appears associated with higher risk of money laundering, terrorist and*

proliferation financing, as well as countries identified as having significant levels of corruption or other criminal activity.

- *Noticeable changes in the gaming patterns of customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he/she normally carries out.*
- *Customer carries out transactions which seem to be disproportionate to their wealth, known income or financial situation.*
- *Size and frequency of transactions raise suspicions. Sudden changes in account activity e.g., the volume of transaction increases suddenly.*
- *The Company has doubts about the accuracy or adequacy of previously obtained customer identification data.*

For every account deemed as High Risk an Enhanced Ongoing Monitoring of the business relationship will be conducted.

In situations where EDD check is required the customer must submit also:

- *Bank statement (not older than 3 months).*
- *Proof of the source of funds.*
- *Payment method confirmation (if required).*

If the customer does not send these documents within 30 days, the gaming account will be blocked from all transactions. The account also can be suspended (access to account temporarily restricted) until provision of the requested documents depending on relevant risk level.

Other EDD measures applied by the Company depending on the risk level defined:

- Obtaining additional information on the customer (e.g., occupation, volume and assets, information available through public databases, internet etc.) and updating more regularly the identification data of customer.
- Obtaining necessarily detailed information and explanations on the source of funds or source of wealth of the customer. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal ruling.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence, terminate or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In situations presenting a higher risk of ML/TF, source of funds information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

8.6. Ongoing Due Diligence

The Company performs ongoing and regular monitoring of potentially risk placement of funds by customers. In case of suspicious placement of funds, customer's account and funds are suspended and enhanced due diligence is conducted.

The Company shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, their risk profile, including where necessary the source of funds.

The Company shall ensure that documents, data, and information collected through the Standard and/or Enhanced Due Diligence (KYC) measures are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers.

Ongoing monitoring of identity:

In conducting ongoing due diligence on the business relationship the casino should hold accurate and up to date identification data of its customers. Since identity may change due to circumstances, the casino should be able to show that if identification information changes, it will be detected and re-evidenced. This means that the casino should consider to obtain evidence of identity periodically to detect any changes, refresh the data on key events (i.e. change of payment instrument) or should consider tracking expiry dates on evidence of identity and refreshing it as it expires. Casinos should determine on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

Ongoing monitoring of transactions:

Transaction monitoring is executed to prevent involvement of the casino with ML/TF and to safeguard the reputation of the casino. While in conducting ongoing scrutiny of transactions a casino notices that a customer's transactions are not consistent with what it knows or expects from the customer, the casino has to question this unusual activity and, where necessary, establish the source of the funds used for that transaction. Source of funds refers to how the funds for a particular transaction were obtained by the player. The reason for inconsistency may lie in inconsistency, amongst others, with the source of funds or average profile or account activity noted to date). The casino has to understand what the reason for this deviation is and obtain sufficient information and documentation with regard to the transaction. It is also one of the situations in which the risk profile of the customer may have to be revised. After receiving this information the casino has to decide whether the transaction is an unusual transaction and need to be reported to the FIU.

8.7. Duplicate accounts

Customers are only allowed to hold one account. When a player registers, the details are checked for possible duplicate accounts. Should the checks indicate that a duplicate

account has been registered; the account is suspended until further checks are made to determine whether or not this is indeed a duplicate account.

Should the fraud management department have any doubts about any of the information submitted at registration stage or have any doubts whatsoever, further identification verification should be carried by requesting supplementary documents from the player. The documents requested are:

- scan of identification document e.g., ID card or passport
- scan of credit card, other payment method confirmation (if required)
- valid proof of address e.g., utility bill (not older than 3 months)

Should the fraud department still not be satisfied, they should ask for further documents. If in doubt, the MLRO should be informed and consulted for further steps, decisions and reporting.

8.8. Record Keeping

The Company keeps for at least 5 (five) years all records obtained through Standard and/or Enhanced Due Diligence (KYC) measures and documentation regarding relations with customers and customers' transactions, as well as correspondence with the customers.

The Company will keep the following records:

- transaction documents
- due diligence information
- information relating to suspicious transactions
- MLRO reports
- training in relation to AML matters, and
- policies and procedures
- records obtained through Standard and/or Enhanced Due Diligence (KYC) measures
- all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence.

This information could be required on a timely basis by regulatory authorities. The documents as outlined should be kept for 5 years from the date of the transaction or the date of completion of any related transaction. Customer due diligence information, or copies thereof, must also be kept for a minimum of 5 years from the date the person concerned ceases to be a registered customer or from the date of the customers most recent activity. These records can be kept in documentary or electronic format.

8.9. Politically Exposed Persons (PEPs)

A Politically Exposed Person is someone who has been entrusted with a prominent public function, such as a senior political figure. Individuals who are closely related to this person, for instance, immediate family members and close associates, are also considered as PEPs. PEPs are classified as a money laundering risk since they may be exposed to property that has been generated by corruption and bribery because of their position.

Screening for PEP status has to be carried out before establishing the business relationship or conducting the occasional transaction.

As a general rule, within the daily work flow every client that has been identified as of high-risk, EDD measures will be applied, and also additional checks are made to identify if the client is a PEP. EDD measures are applied to the customer identified as a PEP and the close associates, in compliance with the applicable EU directives.

The current PEP lists are consulted in order to identify a customer as PEP. Once established as PEP, the following steps are taken:

- Obtain the approval from risk management to maintain and continue the business relationship.
- EDD measures are applied.
- Take reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the player's spending pattern matches his legal source of funds. The casino requests a statement from the player about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources. When public sources cannot, or can insufficiently verify the received information, the casino can request the customer to provide documents
- Ongoing monitoring of the customer's / business partner activity.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

As such, PEP lists (commercial or independently generated) and customer profiles, need to be reviewed constantly to make sure the data is up to date and to identify the situations when person becomes a PEP after establishing business relationship with the Company.

8.10. The termination of the business relationship with the Customer

In case the obligations arising from the customer due diligence cannot be met within 30 calendar days, the casino cannot establish the business relation or perform the transaction or he is obliged to terminate the business relationship with the customer. The casino must also keep a record of all the attempts made to get the necessary information and documentation. To this end, a casino may decide to either close the account or to keep it blocked and suspended in its entirety.

In the event that the customer makes the requested information and/or documentation available to the casino following the closure or the suspension and blocking of the gaming account, the casino has to consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.

The casino is to consider whether there are any grounds giving rise to suspicion of ML/TF/FP. The reluctance of the customer to provide CDD on its own should not be automatically equated to a suspicion of ML/TF/FP. The casino should consider all factors and information it has at his disposal to decide whether there are grounds to suspect ML/FT/FP. If, however the presumption of ML/FT/FP exist the casino should submit an unusual transaction report to the FIU with regard to this player.

Where there is no reason for the retention of funds, the funds are to be remitted back to the player. This has to be done through the same channels used to receive the funds.

9. Monitoring Transactions for Signs of Money Laundering, Terrorist Financing and Proliferation Financing

9.1. Risk Profiles

The Company develops and maintains risk profiles (low, medium and high) to determine the customer categories which expose the Company to higher risk.

9.2. Suspicious and Unusual Transactions (STR and UTR) and reporting to FIU

There is a number of events which might raise suspicions of money laundering, and which require further scrutiny. The following are listed below (but not limited to):

- Customer does not cooperate in the carrying of customer due diligence.
- Customer attempts to register more than one account with the same website.
- Customer deposits considerable amounts during a single session by means of multiple payment methods.
- Customer deposit funds well in excess of what is required to sustain their usual betting patterns.
- Customer makes small wagers even though he/she has significant amounts deposits, followed by a request to withdraw in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.

- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he/she normally carries out.
- Customer enquiries about the possibility of moving funds between accounts (websites) belonging to the same gaming license.
- Customer carries out transactions which seem to be disproportionate to their wealth, known income or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- Customer displays suspicious behavior in playing games that are considered as high risk.
- Artificially splitting a withdrawal to remain “below the radar”.
- Unexplained or unclear source of wealth e.g., student playing large volumes of money the source of which cannot immediately be ascertained.
- Sudden changes in account activity e.g., the volume of transaction increases suddenly.

Any suspicions of Money Laundering should be reported internally to the MLRO. These reports should be documented by means of an Internal Suspicious Transaction Report. The MLRO will then investigate the report and decide if it is necessary to escalate the report to the responsible authorities, restrict access to customer's account and perform other necessary measures.

All unusual transactions must be reported to the compliance officer in the format approved by management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements. The compliance officer must keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU by the casino, the reason shall be adequately documented and signed off by the compliance officer (MLRO) and/or management.

Any unusual/suspicious behavior needs to be reported to the FIU (The Financial Intelligence Unit Curaçao) at **goAML reporting portal**. The MLRO must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The casino shall report to the FIU the details of the transactions by means of the goAML reporting portal. The reports and the submission of the thereto related information (all supporting documents) should be done in English.

If FIU Curaçao, after proper analysis of an unusual transaction, concludes that there is a suspicion of money laundering and/or terrorism financing, this transaction will be reported to the Public Prosecutor's Office as a suspicious transaction.

9.3. Tipping Off

It is extremely important that at no point is the customer to be informed that he/she is

being investigated or that any transactions he/she made were flagged for suspicious activity. Such an action would qualify as “tipping off”. Tipping off could unnecessarily alarm the customer if following investigations, it turns out that there is no suspicious activity going on, but more importantly it could forewarn anybody conducting criminal activity of the investigations and could prejudice investigations. If forewarned of an impending investigation a criminal could destroy evidence incriminating them. Tipping off is a criminal offence. No unnecessary staff should be informed of the suspicions; it is sufficient to initially inform the MLRO. It is also important not to take any action which might indicate to the person being investigated of the suspicions e.g., suspending account for no immediate apparent reason without proper explanation.

The casino, their directors, officers and employees are prohibited to disclose the fact that an UTR is being reported to the FIU. A risk exists that players could be unintentionally tipped off when the casino is seeking to perform its CDD obligations in these circumstances. Therefore, if the casino has a suspicion that transactions relate to ML or TF, casino should take into account the risk of tipping-off when performing the CDD process. If the casino reasonably believes that performing the CDD process will tip-off the player, it may choose not to pursue that process, and should file an UTR/STR to the FIU.

9.4. Suspected Fraud/Money Laundering Involving Employees.

ML/FT activity and/or fraud can also be conducted by employees of the Company. Should any activities of the Company employees raise suspicions of ML/FT or fraud, the same procedure should as with customer transactions should apply. The suspicious activity should be reported to the MLRO by means of an Internal Suspicious Transaction Report whilst avoiding tipping off and involving any unnecessary employees.

9.5. Failure to Report.

One should always keep in mind that failure to report a suspicious transaction when there are reasonable grounds to suspect ML/FT activities is also a criminal offence.

10. Employee Training and Screening

10.1. Training

It is imperative that staff receive appropriate and regular training as to their responsibilities with regard to:

- customer due diligence measures.
- record-keeping procedures.
- internal reporting procedures.
- policies and procedures on internal control, risk assessment, risk management, compliance management and communications that are adequate and appropriate to prevent the carrying out of operations that may be related to money laundering or the funding of terrorism/proliferation.

- relevant regulation in each jurisdiction where a license is held; and
- the recognition, handling and monitoring of transactions which might raise suspicions of money laundering and terrorist financing, and which require further scrutiny.

Records are kept of all training given to staff together with confirmation that they have reached the necessary level of understanding and competence, as well as position-specific training level. All documentation related to AML/CTF/CPF training including materials, tests, results, attendance and date are maintained. In addition, the Company's compliance training program is updated as necessary to reflect current laws and regulations.

Each employee segment should be trained on topics and issues that are relevant to them:

- **New employees.** A general training of the nature and process of money laundering and terrorist financing, and the need to report any unusual transactions to the appropriate designated officer must be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority.
- **Dealers, cashiers and slot department personnel.** They need some additional training on how money launderers might use gambling companies to launder money. They also need some training on the organization's procedures in order for them to know what they must do if they recognize potential money laundering. Personnel involved with account opening must also understand the need to verify the identity of the customer.
- **Audit staff.** Those charged with overseeing, monitoring and testing money laundering controls should also be trained about changes in regulation, money laundering methods and enforcement, and their impact on the organization.
- **AML Compliance staff.** They will need specialized training to be able to stay on top of new trends or changes that impact the organization and the way it manages risk
- **Supervisors and Managers.** A higher level of instruction covering all aspects of money laundering, terrorist financing policies, procedures and regulations must be provided to those with the responsibility to supervise or manage the staff.
- **Senior Management and the board of directors.** Money laundering issues and dangers should be regularly and thoroughly communicated to the board.

Refreshment training must be arranged at regular intervals to ensure that staff members are kept informed of current and new developments regarding money laundering and terrorist financing techniques, methods and trends. To demonstrate compliance with aforementioned staff training guidelines, the casino shall maintain records that include:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

10.2. Employee Screening

Staff who are dishonest present a fraud and business risk to the Company. The Company ensures that there is in place appropriate procedures for due diligence when hiring employees. The Company shall ensure that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. The Company shall screen all employees for criminal records.

This could include reference checks, credit record checks and other vetting measures including verification of information given during the recruitment phase, and confirmation of identity.

To summarize, employees should:

- be identified and verified.
- be screened to ensure their probity.
- receive appropriate training.

11. Know Your Business (KYB)

The Company applies KYB procedures in order to verify the identity of the vendors, suppliers and any contractors (referred to as "Business Partner"). This includes checks on background of the Business Partner, its directors and the beneficial owners (and all individuals/entities in a holding structure of the Business Partner), with whom the Company contracts or intends to contract.

The purposes of KYB:

- to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner of the Business Partner. For legal persons this should include understanding the ownership and control structure of the Business Partner.
- to conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the Business Partner, their business and risk profile, including, where necessary, the source of funds.

The Company requests from suppliers, providers and contractors within the KYB procedure:

- Company corporate ownership chart indicating all companies in the shareholding structure up to UBO/UBOs. If ownership is exercised through one or more companies, it is necessary to provide company certificates for each company up to UBO/UBOs.

- Extract from Register of equivalent document (corporate certificates) indicating directors, shareholders, registered address.
- Memorandum and Articles of Association of the companies in the corporate structure.
- Passport copies in regard to all UBOs and Directors indicated in the corporate structure,
- Utility bills or other evidence of residential address not older than 3 months in regard to all UBOs and Directors indicated in the corporate structure.

The Company reserves the right to request further documentation and information that the MLRO considers necessary to identify background of the suppliers, providers and contractors.

12. Designated Money Laundering Reporting Officer (MLRO)

The appointed Money Laundering Reporting Officer is responsible to ensure that, when appropriate, the information or other matter leading to knowledge or suspicions, or reasonable grounds for knowledge or suspicion of money laundering/ financing of terrorism/ financing of proliferation is properly disclosed to the relevant authority. The MLRO will liaise with the relevant law enforcement agencies on the issues of whether to proceed with a transaction or what information may be disclosed to customers or third parties.

The MLRO acts independently (independent from the games operations).

The MLRO is assigned at the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money

laundering and terrorist financing and to make suggestions to management for improvements; and

- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

Any member of staff that has a suspicion that a customer is engaged in money laundering/ financing of terrorism/ financing of proliferation should report the matter to MLRO whose task is to decide whether it should be reported to authorities, which can also provide guidance on how to deal with suspicious customers. These reports will be delivered via an internal form, which will be kept on record even though the MLRO decides to not take the reported activity further.

The MLRO will also be responsible for ensuring this Policy is implemented and that risk assessment is regularly updated. The MLRO shall prepare regular reports covering operation and effectiveness of the Company' policies and procedures to overcome the threat of ML/TF/PF. The MLRO should respond promptly to any reasonable requests for information made by applicable regulator or law enforcement authorities.

APPENDIX A: SUSPICIOUS/UNUSUAL TRANSACTION REPORT

INTERNAL STR/UTR FORM	
Brand/Product	
Company Name	
MLRO Name	
Date of STR	
Is Company currently refraining from carrying out a transaction because of this STR?	
Approximate aggregate amount of funds involved in Euro	
Is there a particular crime you deem relevant to this STR?	
Please provide, in chronological order, a brief explanation of the circumstances which gave rise to this STR, including reference to sanctions lists/ open-source information/ intelligence databases, transaction activity, customer behavior, where applicable	

Details of person involved in STR	
Name	
Title	
Gender	
Date of birth	
Country of birth	
Nationality	
Identification document type	
Identification document number	
Expiration date of identification document	
Residential address	
Country of residence	
PEP or not?	
Listed on a sanction list? Provide links and attach soft copy of information obtained	
Subject of a criminal investigation? If yes, please indicate which country, if known	
Business relationship information with person involved in STR	
Current status of business relationship	Active/ never initiated/ terminated/ termination in process/ suspended
Date when established business relationship	
Date when discontinued business relationship	
Account information	
Account number	
Balance	
Date suspended or blocked	
Additional comments/ Information regarding customer, suspicious transaction, customers' behavior	
Measures taken by the Company with the date	

indicated	
-----------	--