Anti-Money Laundering, Combating of Terrorism and Combating of Proliferation of weapons of mass destruction Policy (AML/CFT/CFP Policy)

Table of Contents

ABBREVIATIONS	
AML	Anti-money laundering
CDD	Customer Due Diligence
CFT	Countering the financing of terrorism
EDD	Enhanced Due Diligence
FIU	Financial Investigation Unit Curacao
FATF	Financial Action Task Force
Guidance	AML-CFT Guidance for casino operators issued by Curacao Regulator
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
NOIS	National Ordinance on Identification of Clients when rendering Services
NORUT	National Ordinance on the Reporting of Unusual Transactions
PEP	Politically Exposed Person, family member of a PEP or known close associate of a PEP
PSP	Payment Services Provider
Regulator	Curacao Gaming Control Board
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
SOF	Source of Funds
SOW	Source of Wealth
The Regulations	NOIS and NORUT
UTR	Unusual Transaction Report

Disclaimer

1. Overview

1.1. Introduction

LBC ENTERPRISES B.V. is a limited liability company incorporated under the laws of Curaçao, with the company registration number 164426, having its registered office at Chuchubiweg 17, Willemstad, Curaçao (hereinafter – the Company).

To combat money laundering (ML) and the financing of terrorism (FT), we are required to implement measures to prevent and detect the use of proceeds of crime, terrorist financing and the proliferation of weapons of mass destruction (FP).

This policy sets out the information we consider, and the steps we take, to comply with our obligations in relation to to Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Counter-Proliferation Financing (CPF).

This policy applies to all employees and outsourced staff undertaking anti-money laundering, responsible gambling and anti-fraud procedures to the extent connected to their direct responsibilities, including Senior Management and the appointed Compliance Officer. To ensure that our systems and controls remain effective, we have identified a series of clear and proportionate risk indicators aligned with the risks faced by our business.These indicators are designed to deter potential money launderers from using our services, support the detection of suspicious activity, and assist in identifying problematic gambling behaviour.

1.2. The Money Laundering Compliance Officer and the Compliance Department

The Company has appointed a Money Laundering Compliance Officer (MLRO) as part of the art. 5g of the NOIS.

The MLRO is currently De-Anne Kelly.

Any employee appointed to act as MLRO must be registered with the FIU. Any change in MLRO shall be notified to the FIU.

The MLRO is the key individual responsible for the prevention of money laundering and the financing of terrorism. He/she has overall responsibility for ongoing regulatory compliance and creating anti-money laundering procedures.

The MLRO is fully engaged in defining and managing the processes needed to prevent money laundering and other fraudulent activity based on the following principles:

- The Company assumes that most customers are not money launderers. However, it identifies players since it requires the applicable regulations, using a risk-based approach.

- The Company monitors all transactions and activity.

- The Company continuously monitors its customers, as well as risks and processes.

The Company will ensure that all relevant employees are trained on AML and CTF policies and procedures and emphasize alerting these risks. Relevant employees will be required to pass competency tests on this topic.

1.3. Legal framework

- The Company's AML Policy and all related procedures were created subject to the relevant applicable legislation, in particular (but not limited to): The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- 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);
- 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 the 10th of July 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, of the 10th of July 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, of the 10th 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);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

These laws and regulations and any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law form the main legal basis for the Curaçao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons.

1.4. Definitions

Money laundering is the process of concealing, disguising, converting, transferring, or removing criminal property. In other words, it is the process of converting the proceeds of crime into assets with legal origin.

There are three stages of money laundering:

1. **Placement** – placement of funds generated from crime into financial system, either directly or indirectly (blending of funds, invoice fraud, smurfing).

2. **Layering** – the process of separating illicit proceeds from their source by creating complex “layers” of financial transaction designed to disguise the audit trail and provide anonymity (multiple bank transfers, investing in “cash” business).

3. **Integration** – the provision of apparent legitimacy to criminal derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system and appear to be legitimately earned or acquired funds (property dealing).

Money Laundering by a customer occurs either:

(a)where he/she tries to spend the proceeds of crime on gambling (known as 'criminal spend'),

or

(b)where he/she is using our services to try to disguise the source of their money (i.e., 'classic' money laundering whereby a criminal tries to turn their ill-gotten gains into ‘clean’ money by 'layering' it through a series of otherwise respectable transactions, so that they appear to have derived their wealth from legitimate activities).

It is important to remember that simple 'criminal spend' on its own is enough to constitute money laundering (i.e. the use of criminal proceeds to fund gambling as a leisure activity), regardless of whether it is accompanied by any 'classic' money laundering activities. Spending that is inconsistent with an individual's apparent legitimate income may indicate that they are gambling with the 'proceeds of crime'.

Most of the people think that money laundering refers to funds acquired with drugs trafficking, but there are many predicate offences for money laundering such as human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping and tax crimes.

One of the most common forms of money laundering in the gambling sector is by problem gamblers who steal money (often from their employers) to fund their habit.

Terrorist financing is the provision or collection of funds with the intention that they should be used (or in the knowledge that they are to be used) to carry out acts that support terrorists or terrorist organizations or to commit acts of terrorism.

The key differences between ML and TF are:

- For money laundering to occur, the funds involved must be the proceeds of criminal conduct.

- For terrorist financing to occur, the source of funds is irrelevant, i.e., the funds can be from a legitimate or illegitimate source.

However, they both involve money or other forms of value. They both involve the movement of money or value, for example, from one person to another, one account to another, one institution to another, one country to another, one asset class to another. They are both keen to disguise the source and destination of funds.

Financing of proliferation (FP) is the provision of funds 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.

LBC ENTERPRISES B.V. developed internal security measures to prevent money laundering and terrorist financing. The key features of these measures aim to stay aware of high-risk customers and detect suspicious activity, including the predicate offenses to money laundering and terrorist financing.

The Company recognizes that it may be subject to a wide range of regulatory and financial penalties if we fail to comply with our AML/CFT/CFP obligations. The Company may also be exposed to civil liability, and reputational and operational risk. When it comes to AML/CFT/CFP compliance, we therefore expect and encourage our employees to take their AML/CFT/CFP obligations very seriously.

Any employee who knows or suspects, or has reasonable grounds for knowing or suspecting, , that a customer is engaged in ML, FT or FP must report such knowledge or suspicion to our MLRO.

All employees should be aware that they may commit a criminal offence if they fail to escalate their suspicion of money laundering, terrorist financing or proliferation financing.

All employees should be aware that they may commit a criminal offence if they allow a person whom they know or suspect to be involved in money laundering or of providing financial assistance for terrorism to open an account with us or to use an existing account with us.

1.5. Data processing system

The Company operates its internal data processing system to detect high-risk scenarios, money laundering, and terrorist financing in day-to-day operations.

The Data processing system consist of the following mechanisms:

- identification of all users upon the business relationship is established;
- Politically Exposed Persons (PEP) and sanction list checks are performed by the relevant software;
- transaction monitoring is managed by trained staff;
- reporting of all suspected money laundering cases to the MLRO and the Curaçao FIU.

The Company will monitor trends and changes connected to ML/TF and will develop additional internal procedures to keep it up to date.

2. Business-Wide Risk Assesment

2.1. Purpose of the Risk Assessment

The Company shall conduct and maintain a Business-Wide AML/CFT Risk Assessment.

The purpose of the Business-Wide Risk Assessment is to identify, assess, understand, and mitigate the risks of money laundering (ML), terrorist financing (TF), and proliferation financing (PF) arising from the Company's activities, customers, products, services, delivery channels, and geographic exposure.

2.2. Scope of the Risk Assessment

The Business-Wide Risk Assessment shall identify the ways in which the Company's services and operations could be misused for money laundering, terrorist financing, or proliferation financing, and assess the likelihood and impact of such misuse.

All relevant risk factors shall be taken into account, with particular consideration given to:

- The type of customers
- The products and services offered
- The delivery channels used
- The geographical areas in which the Company operates or from which customers originate

The Company shall also consider and incorporate the outcomes and recommendations of the National Risk Assessment into its Business-Wide Risk Assessment, where applicable.

2.3. Risk Assessment Methodology

The Company shall apply a documented risk assessment methodology to identify and evaluate ML/TF/PF risks. The methodology shall:

- Identify inherent risks across all relevant risk categories
- Assess the effectiveness of existing mitigating controls
- Determine the residual risk after the application of controls

Each risk factor shall be classified as Low, Medium, or High, based on the likelihood and potential impact of the risk materialising.

The rationale for assigning each risk rating shall be clearly documented.

2.4. Risk Factors Considered

The Business-Wide Risk Assessment shall include, at a minimum, an assessment of the following risk categories:

2.4.1. Customer Risk

Including customer types, transaction behaviour, high-value players, politically exposed persons, and corporate customers.

2.4.2. Product and Service Risk

Including online gambling products, bonuses, promotions, and any features that may facilitate rapid movement of funds.

2.4.3. Delivery Channel Risk

Including non-face-to-face onboarding, remote access, and automated transaction processes.

2.4.4. Geographic Risk

Including customer residency, payment jurisdictions, and exposure to jurisdictions identified as high-risk, sanctioned or under increased monitoring by competent authorities.

2.5. Risk Appetite

Following the completion of the Business-Wide Risk Assessment, the Company shall define its risk appetite, determining the level of ML/TF/PF risk it is prepared to accept in the course of its business activities.

2.6. Monitoring and Effectiveness of Business-Wide Risk Assessment

The effectiveness of the AML/CFT policies, controls, and procedures implemented as a result of the Business-Wide Risk Assessment shall be monitored on an ongoing basis and improved where necessary.

2.7. Review and Update of the Risk Assessment

The Business-Wide Risk Assessment shall be:

- Reviewed whenever there are material changes to the Company's business or operating environment, including the introduction of new products, games, payment methods, markets, or regulatory changes; and
- Reviewed at least annually in the absence of such changes.

The review shall assess whether any amendments to the Business-Wide Risk Assessment are required.

2.8. Approval and Documentation

The Business-Wide Risk Assessment shall be documented in writing and submitted for approval by the Board of Directors.

The approved Business-Wide Risk Assessment shall be maintained as part of the Company's AML/CFT framework, and maade available to the Curaçao Gaming Authority upon request.

3. Customer Acceptance and Registration Policy

3.1. Purpose & scope

Before making a deposit or place real-money stakes, the customer must register a gaming account. Customers who do not register an account will not be able to play on the Company's website.

In case of Corporate Customers (B2B), additional checks will be conducted including background checks and full corporate due diligence.

The Customer Acceptance and Registration Policy defines the criteria by which the Company may or may not accept potential customers and describes the registration process.

3.2. Customer Acceptance

In order to deposit and play on the Company's website, a customer must first register on the site.

Registration is limited to individuals who are over eighteen (18) years of age.

Customers may only open one account in their name per site. Additional checks are run to block multiple accounts by email address, mobile number, device and certain other combinations of customer data. These checks are done in order to prevent customers opening multiple accounts in order to bypass the AML threshold.

Corporate customers, willing to resell the company's product, must provide the Company with extra due diligence which will be reviewed directly by the appointed 'day-to-day' AML officer.
Requirements are implemented directly by the Company's management and appointed Money Launder Reporting Officer, who oversees operations at corporate level.

Each corporate customer must be approved by the appointed day-to-day AML officer before the company can enter any business relationship with him/her. Due Diligence must be stored separately to those of standard (B2C) customers and needs to be easily accessible for the Company's Money Laundering Reporting Officer. Specific requirements for corporate customers can be found in Clause 4 of this AML policy.

3.3. Restrictions

- Individuals under 18 years of age are not permitted to register on the site.
- Individuals considered to be PEP, under Sanctions or listed in any blacklists, in particular: the Consolidated United Nations Security Council Sanctions List12, the Sanction Decree "Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s." (N.G. 2015, no. 29), the Ministerial Regulation "Libya" (N.G. 2015, 28), the Sanction Decree "Islamic Republic Iran 2015" (N.G. 2015, 27);, the Sanction Decree "Democratic People's Republic of Korea 2015" (N.G. 2015, 30), and the Ministerial Regulation "Yemen" (N.G. 2015, 65).
- Existing customers who have an existing exclusion on the site.
- Individuals with fraud red flags.
- Entities flagged by regulatory bodies.
- Entities directly or indirectly owned by any PEP.

- Entities listed on an active sanctions list.

Corporate entities may get rejected at the discretion of the AML Officer, MLRO or Senior Management if the company feels that the client does not implement sufficient AML practices.

If the AML Officer finds anything suspicious upon reviewing of the new corporate customer, they should report this immediately to the MLRO and the Senior Management. Jointly they will make a decision if the corporate customer can get accepted and if not, the MLRO should decide to file a SAR to the Local authorities with their findings regarding this rejected customer.

3.4. Information Entered on Registration

During the registration process and later on, the Company will request the following identifying information and contact details:

- First Name and Last Name,
- Date of Birth,
- Gender,
- Residential address and country of Residence,
- Email address and mobile phone number,

3.5. Username and Password.Terms Acceptance

During the registration process, the customer must also confirm acceptance of the website's general terms & conditions and its privacy policy.

3.6. Underage Customers

The system does not allow registration of customers who are underage. In order for the registration process to be successful, customers must be at least 18 years old or of legal age in their territory. Date of Birth will be cross checked with the provided ID upon Customer Due Diligence check.

3.7. Customer Due Diligence

To complete registration the customer must identify his/her personal data such as first name, last name, residential address, date of birth, email address, phone number. If the identification is failed at any point, the registration will be declined. Upon customer's first

withdrawal attempt the Company requests documents (such as ID, Proof of Address) in order to verify the identity of the player.

4. Customer Risk Scoring and Profiling

4.1. Purpose & scope

Within the risk-based framework, the Company will undertake risk profiling of all customers from the time of registration for potential money laundering/terrorism financing risks.

It is important to note that the Company's policies and procedures are based on the following:

- Actual regulatory and legal requirements;
- Guidance provided by GCB and Curaçao FIU;
- Internal evaluation of the Company's business risk assessment, and knowledge and experience about the customers.

4.2. Risk-based approach

The Company undertakes a risk-based approach to prevent and combat money laundering and terrorist financing. The Company's risk-based approach is covering the following areas:

- **risk identification and assessment** – identifying the money laundering risks the Company is facing, given its customers, products, and services profile and having regard to available information, and assessing the potential scale and impact of the risks
- **risk mitigation** – identifying and applying adequate measures to mitigate the material risks the Company is facing
- **risk monitoring** – putting in place management information systems (MIS) and keeping up to date with changes to the risk profile through changes to the business or to the threats, and
- **documentation** – documenting the risk assessment and strategy, having policies and procedures covering the above and achieving effective accountability from the Board of Directors and Senior Management.

4.3. Customer Risk Assessment

Based on the information supplied at registration (e.g. customer's full name, residential address, geo-location, age, PEP/sanctions status), the Company will make an initial risk assessment of each customer. Customers thus start their gambling history with the Company categorise them as either Low, Medium or High risk for ML/FT. This will determine decisions made at later points in how they are dealt with. Customer risk assessments are made regularly and when new information obtained.

The customer risk assessment is based on:

- individual status (PEP, under sanctions, adverse media, etc.)
- geographical location
- gambling and transactional behaviour
- payment methods used by the player
- fraud red flags a customer triggered

Customers who are considered High Risk will need to undergo EDD check.

4.3.1. Individual status

PEP

Politically Exposed Person means any person who has been entrusted with a high-ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level.

Any new or existing customer that is found to be a PEP or relative of such will have their account rejected or closed.

Sanctions lists

Governments and international authorities publish sanctions lists to combat persons engaged in illegal activities. Sanction lists include sanctioned people, organisations, or governments. Companies, individuals, organisations, or governments present on these lists as they may pose a higher risk.

Individuals and entities on these lists are subject to financial restrictions prohibiting counterterrorism regimes and money laundering worldwide.

Any new or existing customer that is found on the Sanctions database will have their account rejected or closed. Also, the MLRO must submit an STR to the Curaçao FIU.

Adverse media

Adverse Media or negative news is any bad and negative information about the customer or business discovered in various sources. This information can also expose someone being involved in a crime.

Any new or existing customer mentioned in adverse media can be a subject for EDD, but that depends on the finding. The Company may close the account or reject the registration depending on EDD results.

4.3.2. Geographical location

If the Company finds that the customer resides in a High-risk country, may be a subject for EDD.

High-risk countries are jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and proliferation financing. The Company defines the High-risk countries based on the FATF regulations (black and grey lists) and European Commission's list of high-risk third countries.

Link to the lists:

https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-international-level_en

The Company has implemented a geoblocking tool to limit access to its services from players located in certain geographic locations.

4.3.3. Gambling and transactional behaviour

Each player's gambling and transactional behaviour is constantly monitored. The Company both looks for behaviours that are considered markers of harm for problem gambling and behaviours that can indicate money laundering/financing terrorism.

Behaviours, if noticed, were given allocated scores that combined with other scored ML/FT red flags.

If any examples of ML/FT behaviour are observed, then EDD check must be undertaken immediately of the customer and, if necessary, the SAR process implemented.

4.3.4. Payment Methods

Payment methods that allow the Company to trace the origin of the funds (such as a bank account) and to pay back to the source of the funds are considered low risk.

Payment methods that are funded by cash (or quasi cash) and does not allow the Company to trace the source of the funds are considered high risk. For that reason, the Company does not accept cash deposits, and does not process withdrawals in cash under any circumstances.

Additionally, the Company does not accept not accept deposits paid or made by cheque or banker's draft.

Payment Method	**Risk Rating**
Bank transfers (Klarna, Trustly, Rapid, ApplePay), debit cards issued by banks	Low
EEA licensed e-wallets (Skrill, Neteller, Paysafecard)	Medium
Prepaid cards, Vouchers and Cryptocurrency	High
Cash deposits, Cash withdrawals, Deposits paid or made by cheque or banker's draft.	Prohibited

Manipulations with payment methods (e.g. deposits using one method, withdrawals using another) is also considered as a high-risk by the Company.

4.3.5. Fraud red flags

The Company has an anti-fraud risk management system to prevent bot attacks, fraudulent traffic, synthetic identities, account takeovers, identity thefts, credit card and CNP fraud, proxy users, multi-accounting, collusion etc. Some of the fraud red flags may also be connected to money laundering.

If the Company becomes aware a player triggered a fraud red flag, it will automatically be a subject for EDD.

4.3.6. Purpose and Intended Nature of the Business Relationship

Prior to establishing a business relationship, the Company shall obtain and document information regarding the **purpose and intended nature of the business relationship**

The purpose and intended nature information shall include, where applicable:

- The reason for the customer establishing a relationship with the Company
- The type of gambling products or services the customer intends to use
- The expected level of activity, including anticipated transaction frequency and value
- The expected source of funds used for gambling activity
- For corporate customers, the nature of the business, expected commercial activity, and rationale for using the Company's services

The Company shall monitor customer activity on an ongoing basis to ensure that transactions and behavior are consistent with the stated purpose and intended nature of the business relationship. Any material deviation from the expected activity profile shall be subject to further review and, where appropriate, escalation in accordance with the Company's Suspicious Activity Reporting procedures.

The purpose and intended nature of the business relationship shall be reviewed and updated periodically, and in any event where there is a change in the customer's risk profile, transaction behavior, or business circumstances.

4.4. Risk Score Calculation

Segment customers based on risk factors to detect potentially risky behaviour. Main factors include:

- **Geographical risk:** Customers from countries with high AML/CTF risks should be flagged. Know Your Country risk rating can be used. Please note that risk rating of countries is changing every 3 months. https://www.knowyourcountry.com/ratings-table/
- **Transaction behaviour:** Unusual deposit or withdrawal patterns (e.g., high-frequency, large sums). Deposit methods, Deposits VS Wager, Wagered last 12 months, Net hold last 12 months and Deposited amount last 12 months.
- **Gameplay patterns:** Identify players who exhibit irregular betting behaviour (e.g., high-risk betting, sudden spikes). Game type analysis (slots: low risk; roulette, BlackJack & live casino: high risk; sportsbook: medium risk).

Either of the categories implying a risk-based approach will provide an overall global risk score ultimately classifying whether the player is Low, Medium or High risk, which will then determine the actions need to be taken depending on that risk factor (*please see table below*). All scores are tallied up together and then divided by the number of triggers. For example if the player triggers deposit method as Skrill = 6, game type slots with score of 2, country Malta score of 4, deposit VS wager of 5x with a score of 6, deposit of 9,000 eur = 2, Net hold (NGR) of 3,000 eur = 1 and wagered 5 x 9000 score of 2 then the total score would be 23/7 = 3.28 or 3 to the closest whole number therefore the global risk score would be a 3 (low risk).

AML Risk Profile	1	2	3	4	5	6	7	8	9	10
Global Score										

Please note: if multiple payment methods are used by the player that need to be calculated separately. For example: if the player used Skrill, Sofort and Visa, then the Deposit method overall score will be: (6 + 6 + 4) / 3 = 5,33 (5, so medium risk).

Once the score is calculated, a risk level is assigned.

Not all factors can be automatically included in the CRA calculation due to technical or practical reasons, but the Company do monitor for these risks in other ways. For example, check for VPN usage or multi-accounting at the point of registration, there is a separate alert for players who use cards under a different name, and all withdrawals are checked before approval and payment.

4.5. Customer Due Diligence level

The level of Customer Due Diligence (CDD) conducted on a player will depend on the risk score assigned to the player as follows:

	Low	Med	High
Verify ID and address with docs	X	X	X
Collect additional personal details		X	X
Collect Source of Funds/ Wealth info		X	X (with documentation)
Ongoing monitoring	X	X	X (Enhanced)
Additional measures to address any other risk identified			X
Report suspected cases of ML/FT	X	X	X

4.6. Additional Details & Source of Funds/Wealth

A daily report will be sent to the Company's Key Compliance Officer. The report will include any player who is newly classified as medium or high risk, or who has moved from medium to high risk.

The AML manager will then:

1. Review all accounts in the report, including:

a. Checking what information the Company already have on them
b. Carry out open-source checks
c. Checking if they are in any way suspicious

2. Take appropriate action (if necessary):
    a. Block account if needed
    b. Apply appropriate Due Diligence measures
    c. Review the responses and the information provided by the player
3. If the player does not reply within 14 days, or the response is unsatisfactory, the account will be blocked. If documents are provided later, the AML manager should consider if the delay itself was suspicious, and act accordingly.

Accounts that have been assigned with medium or high risk, will require AML approval before any withdrawal request can be processed.

All decisions taken by the AML manager must be rectified and documented.

4.7. On-going Monitoring

The AML team will conduct on-going monitoring on accounts, on a risk sensitive basis. This includes:

- Obtain up to date identification documentation when existing documents have expired.
- Question the data and information about a player whenever inconsistencies are noticed.
- General review and update from time to time, based on customer's risk level.

4.8. Withdrawals

The terms and conditions relating to the depositing and withdrawal of monies are clearly highlighted for customers as part of the Company's Terms and Conditions. They are also clearly explained during the withdrawal process.

Withdrawal requests are reviewed and processed by the Anti-Fraud team at regular intervals each day. Under our Terms and Conditions, we reserve the right to request the customer to send us copies of documents to verify that they are the owner of any bank cards or other payment types which are being used to process deposits or withdrawals. Where we deem there to be a higher risk of fraud or money laundering, we reserve the right to require the customer to produce additional proof of identity and additional verification of their ownership of the method being used to withdraw funds.

If the Company receives notice of any chargeback, disputed deposit, or potential fraud, then the corresponding customer account will be frozen immediately. All reported chargebacks/fraudulent transactions will be investigated and challenged where possible and reported to the appropriate authorities.

Whenever possible the funds will be remitted back to their original source.

Where a customer wishes to withdraw funds from their account, our systems will identify the following information:

- whether this is the first withdrawal request by a customer
- whether the withdrawal method is the same as that used to deposit
- whether the total value of refunds on the account is less than €2,000 (the amount is configurable depending on payment method and jurisdiction)

If a withdrawal request is made on an account which meets all the above criteria, the refund will be processed automatically (although our Anti-Fraud team is able to monitor withdrawals as they take place and make an immediate stop to the withdrawal if deemed necessary).

If a withdrawal request does not meet all the above criteria, then it will be reviewed by the Anti-Fraud team.

5. Customer Due Diligence

5.1. Purpose & scope

The Company distinguishes between Customer Due Diligence (hereinafter – CDD) and Enhanced Customer Due Diligence (hereinafter – EDD).

The customer is obliged to cooperate concerning the fulfilment of the due diligence request. If the Company cannot successfully carry out the due diligence, the business relationship won't be established or continued, and no transaction will be carried out. In addition, the Company examines whether it is necessary to submit a SAR.

5.2. Standard Customer Due Diligence

The Company applies general (standard) customer due diligence (hereinafter – CDD) measures to the customers at the registration stage. The CDD process consists of:

- identification – establishing identity by collecting information from the customer.

- verification – proving a customer is who they claim to be by obtaining and validating documents or information which supports this claim of identity, which come from a reliable and independent source.

According to the above requirements, The Company collects the following information for identification and verification to prevent money laundering and terrorist financing:

a) First and Last Name
b) Date of birth
c) Residential address (street, no., ZIP code, city)
d) ID
e) Proof of Address (POA)

5.3. Documents acceptance

For acceptable ID documents, the Company require a government-issued document containing photographic evidence of the customer's identity. The following documents may be accepted for the verification purpose:

- current signed passport;
- driving license;
- identity card;
- another government issued document.

For POA verification the Company accepts:

- Utility bill for a service installed at the residence issued in the last 6 months;
- Correspondence or any other government-issued document from a central or local government authority, department or agency issued in the last 6 months;
- Lease agreement (Does not have to be issued in the last 6 months but must be currently valid.).

The main requirements to the documents provided by the customer are:

- the document must be valid and not expired.
- documents must be clear, legible and of good quality.
- Mobile phone bills not be accepted, as they are not tied to a residential address.

5.4. Ongoing monitoring

The general due diligence duties include the ongoing monitoring of the business relationship. This includes:

- Obtaining up to date identification documents when existing documents have expired.
- Questioning the data and information the Company hold about the player, whenever inconsistencies are noticed.
- General review and update from time to time, on a risk sensitive basis.
- Checking if transactions are matching with the information and documentation available at the Company about the customer.
- Updating the respective documents, data, or information at appropriate intervals, based ont he customer's risk level.

5.5. Enhanced Due Diligence

Enhanced Due Diligence measures shall be applied on a risk-based basis, and shall be commensurate with the higher risks identified, including risks identified through the Company's Business-Wide AML/CFT Risk Assessment.

The Company applies Enhanced Due Diligence measures (hereinafter – EDD) and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks.

EDD is applied in the following cases:

- in any case, identified by the Company or in the information provided by the authorities to the Company where there is a high risk of money laundering or terrorist financing;
- where a customer is resident in, or transactions involve, higher-risk jurisdictions, including countries identified by FATF or competent authorities;
- if the Company has doubts as to whether the information collected regarding the identity of the customer is not correct or not (or no longer) accurate;
- if the Company has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP;

- in any case where the Company discovers that a customer has provided false or stolen identification documentation or information, and the Company proposes to continue to deal with the customer;

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

- where new products, services, delivery channels or technologies, including crypto-assets, present increased ML/TF risk;

- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.

In cases where there is a higher risk, establishment of the business relationship or continuation of the business relationship (if the higher risk only arose later or was only recognised later) can happen only with the consent of the Key Compliance Officer.

If a customer has been deemed to be a high-risk or becomes one at any stage, the Company undertakes the EDD procedure, including any of the below (depending on the case):

- Re-verification of identity (repeated CDD).

- Establishing how the customer acquired his wealth to be satisfied that it is legitimate:

    - salary income or company profit (Certified Payslip / Certified employer letter / audited accounts if self-employed);

    - sale or liquidation of financial instruments (Certified shares/investments sale contracts or statements/ accountant letter);

    - sale of property (Certified copy of the contract of sale or letter from a solicitor or estate agent);

    - ○ inheritance (Certified copy of will including the value of heritage;

    - sale of the company (Certified contracts, media articles, certified letter from accountant or solicitor), etc.

- Establishing the customer’s source funds to be satisfied that they do not contains the proceeds of crime.

- Ensure that deposits originate from payment methods that belongs to the customer and do not allow anonymity by requesting copies of bank statements or account statements.

- Obtaining additional information on the purpose and intended nature of the business relationship, and assessing whether transactions are consistent with that purpose;
- Undertaking increased continuous monitoring of the business relationship.
- Any suspicious transaction must be investigated, and the business relationship underlying the transaction shall be monitored to assess the risk of money laundering and terrorist financing.

With EDD checks on transactions, the Company's fundamental aim is to ensure the transparency of payment flows. Accordingly, the origin and destination of the money used in a transaction shall be traceable back in each case to an account.

Definition of Source of Funds

The Source of Funds refers to the origin of the particular funds being used to deposit on the Company's website. This is not simply verifying which bank or financial institution the customer may have received the funds from. The information obtained should be substantive, relevant and establish the fund's origin and the method/circumstances under which the funds were acquired.

In higher-risk situations, source of funds information shall be requested periodically, even where no apparent change in transaction pattern or behaviour has occurred.

Definition of Source of Wealth

The Source of Wealth refers to the origin of the entire body of wealth (i.e. total assets) of the client. The information that the Company obtains should indicate the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired.

5.6. Politically Exposed Persons and Sanctions Screening

The Company uses a 3rd party KYC software to check all new customers at the registration stage against PEP and Sanctions databases. Customers screened against the following sanction lists:

- OFAC (Office of Foreign Assets Control);
- EU (European Union);
- OFSI (Office of Financial Sanctions Implementation);
- UN (United Nations); and
- Australian Governments Dept. of Foreign Affairs (DFAT).

Any new or existing customer found on the Sanctions database, or a PEP (or relative of such) will have their account rejected or closed.

In case of identifying a PEP, responsible staff will send a report to the MLRO who in turn will send a report to the Senior Management.

The MLRO will investigate each case to identify positive or false-positive PEP alert. The Company has a right to request additional documents from the customer for this purpose within the investigation.

If the PEP alert is true-positive, the MLRO will reject the registration or close the account and inform the Senior Management about the decision taken.

Politically Exposed Person means any person who has been entrusted with a high-ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level. In particular, politically exposed persons are:

- heads of state, heads of government, ministers, members of the European Commission, deputy ministers and assistant ministers,
- members of parliament and members of similar legislative organs,
- members of the governing bodies of political parties,
- members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are usually not subject to further appeal,
- members of the boards of courts of audit,
- members of the boards of central banks,
- ambassadors, chargés d'affaires and defence attachés,
- members of the administrative, management or supervisory bodies of state-owned enterprises,
- directors, deputy directors, members of the board or other managers with a comparable function in an international or European intergovernmental organisation.

Family member of PEP means a close relative, in particular

- the spouse or civil partner,
- a child and the child's spouse or civil partner and
- both parents.

5.7. Procedure for Account Closure

The Company may decide to close a customer's account on any of the below reasons:

- Fraud;
- Cheating;
- Bonus Abuse;
- Allowing a third person to use their account;
- Under-aged gambling;
- Problem gambler;
- Being abusive to staff;
- Commercial concerns;
- CDD/EDD failure;
- Terms and Conditions breach.

By law the Company must end the business relationship with the customer unless obtained appropriate consent for it to continue and even then, it is precautionary to close the account.

Due to the laws on Tipping Off, the Company cannot inform the customer that it has concerns regarding ML/FT, thus account closure must be done sensitively.

The MLRO will need to consider whether if a SAR should be submitted as part of the concern about the player's behaviour whether appropriate consent should have been requested.

Where the Company is unable to complete or apply the required CDD measures in relation to a particular customer at the point the CDD threshold for transactions is reached, and is accordingly required to cease transactions and terminate the business relationship with the customer.

5.8. Termination of the Business Relationship for AML/CFT reasons

Termination may occur where the customer fails to meet CDD or EDD requirements, or where the Company cannot adequately mitigate higher ML/TF/PF risk identified through EDD.

The Company shall document and retain records of all reasonable attempts made to obtain the required CDD information and documentation. Depending on the circumstances, the

Company may either close the customer's account or suspend and block the account in its entirety.

Where the customer provides the requested CDD information or documentation following the closure, suspension, or blocking of the account, the Company shall assess whether the delay in providing such information affects the money laundering, terrorist financing, or proliferation financing risk associated with the business relationship.

The Company shall assess whether there are grounds to suspect money laundering, terrorist financing, or proliferation financing. The failure or reluctance of a customer to provide CDD information shall not automatically be considered suspicious. All relevant facts and circumstances shall be taken into account when determining whether a Suspicious Activity Report should be submitted to the FIU.

Where there is no legal or regulatory reason to retain the customer's funds, any remaining funds shall be returned to the customer through the same payment method used to receive the funds.

All decisions relating to the termination, suspension, or continuation of a business relationship for AML/CFT reasons shall be approved by the MLRO and appropriately documented.

5.9.Corporate Customers (B2B) - Beneficial Ownership Identification and Verification

For corporate customers, the Company shall identify and verify the Beneficial Owner(s) prior to establishing a business relationship, in accordance with Regulation 11.2.2 of the Curaçao AML Regulations.At the minimum identification information, verification and evidence must be gathered for all persons holding 25% or more of the shares or voting rights or a person who otherwise exercises ultimate effective control of the customer. Where no individual meets the ownership threshold, the Company shall identify and verify the senior managing official(s) as the BO(s).

The Company applies a lower internal ownership threshold of 10% as a risk-mitigation measure, requiring Enhanced Due Diligence for individuals holding 10% or more of ownership or control.

Corporate customers are automatically considered as high risk and are subject to Enhanced Due Diligence.

The Company shall obtain sufficient information to identify and verify all Beneficial Owners and Directors, including but not limited to:

- Memorandum of Association
- The company's Excerpt of the Registrar / Chamber of Commerce
- Registry of Directors
- Registry of Shareholders
- Organisational and ownership structure charts
- Active Gaming License or Declaration with Business plan on the attempt to obtain a Gaming License
- AML/CFT Policy of the corporate customer

Beneficial Owners and Directors shall be subject to identity verification, sanctions and PEP screening, and, where applicable, source of funds and source of wealth assessment.

In cases where the Beneficial Owner cannot be satisfactorily identified or verified, the Company shall **not establish or shall terminate the business relationship**, and shall consider whether a Suspicious Activity Report is required.

In addition to this, the AML Officer may, at their discretion, request any of the required documents to be Notarized and/or Apostilled.

Beneficial Ownership information shall be **kept up to date** and reviewed on a **quarterly basis**, or earlier where changes in ownership, control, or risk profile are identified.

6. Funds Management Procedures

6.1. Player Account Balance

All funds deposited by the player or owed by the Company are credited to the player's corresponding account. The player can top up the funds in his/her account by depositing through the cashier on the Company's website and then use these funds to place bets. Bets are deducted from the account balance, and winnings are added to the account balance.

The player can withdraw withdrawals of available funds in the player's balance. The Company do not offer credit to players. A player may not transfer funds to another player.

6.2. Payment Methods

Payments shall only be accepted and made from accounts held with licenced financial institutions or through licenced payment providers.

No cash deposits/withdrawals will be affected between the Company and its players.

6.3. Player Deposits

After registering a gaming account, a player may then deposit funds into their account through the cashier on the site.

In order to facilitate these deposits, the company has integrated a number of gateways. All gateways are PCI DSS compliant, and the company does not hold any credit card data itself.

The company submits the transaction to the PSP and then waits for approval from the card acquirer/e-wallet. On approval, the deposit status is updated and the funds added to the player's balance.

6.4. Player Withdrawals

A player with an available balance will be able to request a withdrawal of the funds via the cashier on the site. The player will enter the amount they wish to withdraw and select their preferred payout method. The withdrawal amount is then deducted from the player's balance.

6.5. Withdrawal Payouts

In remitting funds to the player, the Company will, where possible, remit the funds directly into the account where the funds originated from, keeping a closed loop.

Provided that where this is not possible, the Company will remit the funds to the player in line with the requirements under AML legislation and to the lowest risk method possible.

7. Crypto payments

7.1. Compliance with regulatory requirements

LBC ENTERPRISES B.V. is committed to ensuring compliance with all applicable regulations governing Virtual Financial Assets (VFA). This includes adherence to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations, as well as other relevant financial regulations.

The Company will implement and maintain robust systems and controls to prevent the use of Virtual Assets for illicit activities. This includes conducting thorough due diligence, monitoring transactions, and reporting any unusual activities to the Curaçao Gaming Control Board (GCB) and Curaçao FIU. This part outlines the use and acceptance of VFAs, complying with applicable laws and regulatory standards, in particular, VFAs that involve the use of Distributed Ledger Technologies (DLT).

7.2. Risks with crypto payments

Cryptocurrency is decentralized digital money secured by cryptography and based on blockchain technology - that is, a distributed digital ledger that keeps a secure, transparent, and decentralized record of transactions.

Cryptocurrency is almost impossible to counterfeit or double-spend, so it might prove valuable to online gambling sites looking to become more secure and transparent.

However, their decentralized structure allows crypto to exist outside the control of governments and central authorities. Therefore, this new form of value is extremely unregulated.

Risks using cryptocurrency:

- Lack of legal framework;
- Volatility;
- Hacking concerns;

Cryptocurrency is an exciting, technology-powered form of value that promises to change many aspects of people's lives - including their gambling habits. However, while promising, this technology is still riddled with loopholes and issues that need to be addressed to protect consumers and the gambling industry as a whole.

Apart from focusing on all the benefits of digital currencies, LBC ENTERPRISES N.V. is aware of its potential risks and do its best to mitigate them.

7.3. Unhosted wallets

Unhosted wallets, defined as digital wallets that are not managed or hosted by a third-party service provider, are subject to stringent transparency requirements. The Company is aware that transparency regarding the owner and beneficiary of unhosted wallets is paramount for regulatory compliance and mitigating risks associated with Money Laundering (ML) and Terrorist Financing (TF).

LBC ENTERPRISES B.V. will ensure that players utilizing unhosted wallets for gaming transactions provide comprehensive information regarding their identity, including but not limited to, full name, address, and official identification documents. The Company will conduct thorough due diligence procedures to verify the identity of unhosted wallet owners, in line with established AML & CFT standards. Any unusual activity or transactions that raise concerns regarding the source or destination of funds will be promptly reported.

7.4. Custodial wallet services

Custodial wallet services, facilitating the exchange of Virtual Currencies (VC) to fiat, vice versa, or VC-to-VC transactions, are subject to rigorous monitoring and compliance measures to mitigate risks associated with money laundering and terrorist financing.

The Company when offering custodial wallet services through third-party Custodial Wallet Providers, will implement robust Customer Due Diligence (CDD) procedures to ascertain the source of funds (SOF) and verify the identity of users engaging in VC transactions, including minimum age requirements. Comprehensive KYC (Know Your Customer) protocols will be established to collect relevant information, including personal identification details and transaction histories, from customers. The Company will implement effective transaction monitoring systems to detect and prevent suspicious activities within custodial wallet services.

7.5. Volatility of VFAs

The values of VFAs relative to fiat currencies (e.g. EUR) may be subject to significant volatility and fluctuation. As a result, the value of VFAs may increase or decrease substantially over a short period of time. The Company hereby advises all players that VFAs are subject to significant fluctuations in value (vis-à-vis fiat currencies) due to market volatility. By engaging in transactions involving VFAs, all players acknowledge and accept the inherent risks associated with such volatility. Players are strongly encouraged to exercise caution and to consider these risks when making deposits, withdrawals, or any other financial transactions involving VFAs. All players acknowledge that due to the risks associated with the volatility of the value of VFAs relative to fiat currencies, that they may deposit or withdraw a sum which is higher or lower in value when compared to fiat currencies than anticipated.

8. Suspicious Activity Reporting

8.1. Reporting obligations

Every employee of the Company must report to the MLRO if there is a suspicion or knowledge of money laundering, funding of terrorism or if the funds being used on the Company's website are the proceeds of criminal activity.

The employees of the Company are required to detect and report either intended or completed unusual transactions.

The MLRO will consider each report and determine whether it gives grounds for knowledge or suspicion. If they do, then a SAR should be submitted to the FIU as soon as reasonably practicable.

Knowledge means that the person reporting knows the event to be a fact. Suspicion implies that the person reporting the incident may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial or financial sense.

A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report the activity then arises. Likewise, if concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and will need to be reported to the FIU.

The MLRO will assess all the circumstances related to the suspicion. Decision making will depend on what is already known about the customer and the transaction and how easy it is to make further enquiries.

8.2. Recognition of Unusual Transactions

An unusual transaction is a transaction inconsistent with the player's profile.

The employees if the Company must assess whether a customer's transaction qualifies as an unusual transaction.

All these unusual transactions must be reported to the MLRO 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 MLRO must keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU by the casino, the reasons therefore shall be adequately documented and signed off by the compliance officer and/or management.

The following transactions or intended transactions are deemed unusual:

a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
c. Transactions in the amount of XCG 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means.

This includes but is not limited to:

1. A cashless transaction in the amount of XCG 5,000 or more.
2. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
3. Accepting or releasing a deposit in the amount of XCG 5,000 or more at the request of the client;
4. Sale to a customer of chips in the amount of XCG 5,000 or more. "Chips" include but is not limited to tokens and credits.
5. A cash out in the amount of XCG 5,000 or more;

Note: A transaction may be a single transaction, but may also be 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.

Any transactions in the amount of EUR 2500 or more is deemed unusual transactions and directly reported to the FIU immediately as indicated above. The indicated examples are not limited, also credit card transactions and e-wallet transactions are to be reported to the FIU.

8.3. Red Flags/Indicators

Red flags are not intended to automatically result in filing a SAR with the FIU, however, are merely indicators that should lead the Company to question the customer's behaviour. If there is no reasonable explanation for the red flags, then an internal report must be made to the Key Compliance Officer.

The following is a list of possible red flags which should be considered:

- Customer does not cooperate in the carrying out of CDD/EDD.
- Customer attempts to register more than one account on a site.
- Customer makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well 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 belonging to the same gaming group.

- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the Customer's wealth, income or financial situation.

- Customer seeks to transfer funds to a bank account held in the name of a third party.

- Customer requests a withdrawal to an account he/she never deposited with.

- Customer opening an account and registering several different cards and making transfers between them.

- Customer depositing large sums, then places minimal bets, then withdrawing all their funds.

- Customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence.

If a customer refuses to provide CDD/EDD documentation, the Company won't immediately equate this on its own to suspicion of ML/FT.

The Company will consider all factors and information, including the payment method(s) used, game(s) played, playing trends and patterns, jurisdiction, and any open-source information.

If there are grounds to suspect ML/FT after considering all of these factors, then an SAR must be submitted.

8.4. Internal Suspicious Activity Report

All employees have a duty to report suspicious transactions / activity. If an employee has any suspicion about a customer's behaviour or transaction, it must be reported to the MLRO immediately.

Any suspicious transactions or activities must be reported by submitting an iSAR ticket or, alternatively, by emailing compliance@luckybet.co as soon as practicable following the process and accompanied by the relevant supporting documents.

The employee should still submit the report, even if their superiors are not in agreement. It will then be up to the MLRO to determine if the information available can be considered sufficient for a SAR to be filed to the FIU.

The following information is included in an Internal SAR:

- The customers details;
- The member of staff's statement about what gave them cause to make the report;
- All relevant documentation and information.

The MLRO will:

- Acknowledge receipt of the report, review and investigate further as required;
- Make an assessment based upon all the information and decide whether the matter needs to be reported externally to the FIU
- Make a record about the decision taken.

8.5. External report to FIU

Once the MLRO has received an Internal SAR, she/he will decide if a SAR should be submitted to the FIU.

When making this decision, the MLRO should consider that AML legislation is intended to address serious crime which usually either involves amounts that are not minimal or circumstances that show an intent to circumvent and abuse the safeguards in place to deter the use of the financial system for criminal purposes.

The MLRO considers whether an internal report gives rise to a suspicion of ML by taking into account all relevant information, including assessing whether there are common denominators between e.g., repeated suspicious behaviour, instances of chargebacks or identity fraud. For example, these may consist of common or related persons, common IP addresses etc.

The MLRO, in deciding to submit the SAR or not, should answer the following questions:

- Who is involved?

- How are they involved?
- What is the criminal/terrorist property?
- What is the value of the criminal/terrorist property (estimated as necessary)?
- Where is the criminal/terrorist property?
- When did the circumstances arise?
- When are the circumstances planned to happen?
- How did the circumstances arise?
- Why you are suspicious or have knowledge.

8.6. Reporting Procedure

The Company is obliged to submit a suspicious activity report to the FIU, by means of the goAML reporting portal, without due delay if there are indications that:

- the Company know, suspect, or has reasonable grounds for knowing or suspecting money laundering and/or terrorist financing,
- an asset related to a business relationship or transaction originates from a criminal offence that could constitute a predicate offence to money laundering,
- a business case, transaction, or asset is related to terrorist financing.

The reports and the submission of the thereto related information (all supporting documents) should be done in English.

The casino and its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting to the FIU.

8.7. Tipping-off or Prejudicing an Investigation

It is an offence to inform anyone that a SAR has been submitted or is being considered to be submitted.

The MLRO will consider whether it is necessary to report suspicious activities to the relevant authorities. If a SAR is made to the authorities, it is important that the relevant customer is not 'tipped off' about the fact that they are under investigation. This could prejudice the ability of the authorities to investigate them.

This means that employees of the Company shouldn't:

- at any time, inform a customer that a transaction is being delayed because a report is awaiting a defence (consent) from the FIU
- inform the customer that law enforcement is conducting an investigation.

It is therefore vitally important that the employees do not disclose to a customer that they have suspicions about them which may result in a report being made. This means it is possible to have an internal discussion about the customer, but in no way can the customer or their associates be given any indication that the customer may be under investigation.

It is an offence if you know or suspect that a disclosure of possible money laundering or of providing financial assistance for terrorism has been made by the MLRO to the relevant authorities, or that an investigation into money laundering is imminent or underway, and you disclose to any person not involved in the investigation - especially the customer(s) involved - that information (or any other matter that is likely to prejudice any such investigation).

However, it is still acceptable for the employees to make normal enquiries of a customer, conducted in a tactful manner, regarding the background of a transaction or activity that is inconsistent with the normal playing pattern of activity. We are required to make these enquiries, and simply making these enquiries in an ordinary manner should not give rise to the offence of tipping off or prejudicing against an investigation. Indeed, such customer enquiries are likely to be necessary not only in relation to money laundering but also in connection with our responsible gambling duties.

If there is a suspicion or actual knowledge or proof that a customer was involved in criminal conduct, then the employee must disclose it only to the MLRO immediately.

The issue must be escalated as soon as it becomes apparent to minimize the risk of delay. If there is pressure by the customer to honor his/her request/s, or to explain delays, the employee must escalate the issue for assistance, whilst taking great care to avoid making any statement that may constitute tipping off.

If in doubt, the employees consult the MLRO.

8.8. Record Keeping

The Companmy shall maintain, for at least five years, all necessary records on transactions (both domestic and international), to enable them to comply with information requests

from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

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 must be kept for at least five years after the business relationship is ended, or after the date of the occasional transaction.

The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority.

9. Internal Controls

9.1. Purpose & scope

The Company has a number of internal controls and general procedures which will be used on a day-to-day basis in respect of managing and running the daily operations of the business. The main purpose is the prevention of money laundering and terrorist financing.

9.2. Recordkeeping

The Company keeps all the documents and data collected or obtained within the scope of the due diligence, including:

- all data and information used to identify and verify customers (including type and number of the document, issuing authority, etc.);
- all records (receipts) relating to transactions, i.e., winnings paid out or refunds to customer accounts;
- all documents and records used for the preparation of the risk analysis, the risk analysis itself, including the results of the risk assessment, as well as the documentation on the appropriateness of the measures taken based on these results;
- the results of internal investigations, communication with FIU and regulators;
- documents collected within the scope of business partners due diligence;
- documents collected form the employees within the scope of the due diligence;
- documents regarding AML trainings (training materials, examination results, etc.);

The Company also keeps all documents created and processed in connection with a suspicion of money laundering or terrorist financing, including:

- all related internal and external correspondence, files and interview notes;
- the results of internal investigations and the measures taken, that can explain why the MLRO concluded and initiated the actions taken.

The retention period is five years and starts with the end of the calendar year in which the business relationship ends and in all other cases with the end of the calendar year in which the respective information was ascertained. Applicable legislation may provide for a more extended retention period. The Company destroys all the documents and data collected after retention period expiration unless other recordkeeping or retention obligations apply, but not less than 5 years.

9.3. Money Laundering Reporting Officer

The Company has appointed a Money Laundering Compliance Officer (MLRO) whose main responsibility is to review any internal suspicious transaction reports, and where necessary to submit a SAR with the FIU. The MLRO is the main contact point for the FIU.

In order to ensure that the MLRO is able to fulfil their role effectively, the Company guarantee that:

- MLRO acts independently, has been provided the necessary knowledge of the Company's activities and is able to decide independently as to whether internal reports are to be escalated to the FIU.
- MLRO has no conflicting responsibility which may pose a conflict of interest.
- MLRO has sufficient time, resources and information to fulfil their responsibilities.
- MLRO has a right to create work assignments to relevant employees and take decisions regarding ML/TF prevention.

The MLRO and their deputy carry out the following functions (including but not limited to):

- Creating and further developing the internal risk analysis, including a complete scope of risks connected to money laundering and terrorist financing.
- Developing and updating internal policies and procedures to prevent money laundering and terrorist financing.
- Creating unified reporting channels.

- Involvement in other internal organizational and work instructions creation and their further development, related to implementing the regulations on the prevention of money laundering or terrorist financing.

- Ensuring compliance with current AML regulations, and other relevant legislations.

- Ongoing monitoring of the Company's business activity to comply with the anti-money laundering regulations.

- Ensuring CDD/EDD is undertaken.

- Suspicious activity risk assessment.

- The submission of SARs in appropriate cases.

- Contributing to the content of staff's AML training.

- Maintaining a list of all inquiries received from law enforcement agencies and records relating to internal and external disclosures.

- Submitting a report to the management on MLRO activities on the risk situation of the Company and the measures taken and intended to implement the obligations under money laundering regulations.

The MLRO and their deputy are authorized, within the scope of their performance of their work:

- To perform their tasks independently and effectively.

- To submit the necessary legally binding declarations for the undertaking and represent it externally in relevant situations.

- To provide undertaking-specific instructions for all matters relating to the prevention of money laundering and terrorist financing.

- To carry out random checks without restriction.

9.4. Training

The Company will provide training to all staff directly or indirectly through a service provider upon joining the Company and after that annually.

Relevant training materials will be prepared for all teams based on Company policies, which is compiled according to the applicable legislation requirements and guidelines.

Training will be conducted as follows:

- Training material based on the finalised and approved Company policies, in the form of documents and presentations.
- Training will be provided to existing management and staff.
- Training will also be included in the induction of all new staff.
- Training will be followed up with a questionnaire to test everyone's understanding.
- Should the Company find that some parts of the training are unclear it will repeat the training focusing on the issues that were not understood.
- Regular refresher training will be given, which will include any updates and will focus on any shortfalls that arose during the previous period.
- Any update in the AML policy will be communicated in a group email and through ad-hoc training, and added to periodic training updates and material.

Staff training will focus on ensuring awareness of:

- all applicable legislations,
- the provisions of the money laundering and terrorist financing requirements,
- staff personal obligations under the money laundering and terrorist financing requirements,
- applicable internal reporting procedures,
- Company's policies and procedures to prevent money laundering and the financing of terrorism,
- Company's identification and verification procedures, record-keeping, and other procedures to prevent money laundering and the financing of terrorism,
- recognition and handling of suspicious transactions,
- staff personal liability for failure to report information or suspicions under the money laundering and terrorist financing requirements and the Company's internal procedures,
- new developments, including information on current techniques, methods, and trends in money laundering and the financing of terrorism,

- the money laundering and terrorist financing risks faced by the Company, and
- Data protection regulations.

Induction training sessions will be conducted for all employees and will include fraud prevention, detection and ancillary methods, as required by their role. Refresher training will also be provided, both on a regular basis and as needed, so as to keep employees up to date and informed of the Company's policies and procedures and any changes or improvements made. The MLRO keeps records of training delivered, showing details of the training has been provided, when and by whom, and the next training date. In case of any changes to the Company's policies and procedures or applicable legislation, all staff will get the relevant training.

9.5. Employees background check

Prior to engaging employees, the Company will carry out relevant integrity checks, in-line with their position, responsibilities and access levels. The Company will not employ any persons who are not deemed to be fit and proper.

For this purpose, the Company may request the following documents (in each case with due regard to data protection):

- a valid, original identity document,
- up to date CV,
- any other documents, as the Company deems necessary to request.

Once a person is employed, screening shall still be carried out on an ongoing basis as required. All employees of the Company must guarantee that they observe the provisions of applicable legislation and the associated due diligence obligations, report facts relevant to money laundering, and do not themselves participate actively or passively in dubious transactions.

For this purpose, Senior Management will regularly carry out checks on employees or whenever the Company feels the need to perform such inspections. In particular, such inspections shall be carried out when suspicion arises concerning the behaviour of specific employees. The Company may carry out these checks through surprise spot checks or other procedures that will enable such personnel to verify whether employees comply with the policies and procedures.

The frequency and extent of screening that shall be carried out, must be proportionate to the risk level posed by the employee. The risk level will be determined case by case depending on employee's position (e.g., head of department, senior, mid), the scope of duties and obligations, etc.

The Company will check all the employees at least once a year. The Company will use an employee performance sheet for this purpose.

9.6. Independent AML/CFT Audit Program and Regulatory Updates

The Company shall maintain an Independent AML/CFT Audit Program in accordance with Section V.5 of the CGA AML Regulations, designed to assess the adequacy, effectiveness, and compliance of the Company's AML/CFT policies, procedures, systems, and controls.

9.6.1. Independence of the Audit Function

The AML/CFT audit shall be conducted by individuals who are independent of the Company's AML compliance function and operational activities, and who possess sufficient qualifications, experience, and expertise in AML/CFT matters to ensure that audit findings and conclusions are reliable and objective.

9.6.2. Scope of the Audit

The independent AML/CFT audit shall include, at a minimum, an assessment of:

- The Company's AML/CFT policies, procedures, and manuals relating to money laundering, terrorist financing, and proliferation financing
- Compliance management and governance arrangements
- The effectiveness of transaction monitoring and **transaction testing**, including sampling of transactions on and beyond applicable thresholds
- The adequacy and effectiveness of AML/CFT training programs
- Compliance with applicable AML/CFT laws, regulations, and regulatory guidance
- The adequacy of the Company's record retention and data storage systems
- Interviews with employees responsible for handling customer transactions and their supervisors
- The Company's handling of unusual or suspicious transactions, including compliance with internal escalation and external reporting obligations

The audit shall also assess whether Senior Management and/or the Board have been responsive to findings and recommendations arising from previous AML/CFT audits.

9.6.3. Frequency of the Audit

The AML/CFT audit shall be conducted at least annually, or more frequently where required due to changes in the Company's risk profile, regulatory requirements, or following material AML/CFT incidents.

9.6.4. Documentation, Reporting, and Remediation

The scope, methodology, and results of the AML/CFT audit shall be fully documented. Any identified deficiencies or weaknesses shall be reported in writing to Senior Management and, where applicable, the Board of Supervisory Directors, as well as to the Key Compliance Officer.

The audit report shall include recommended corrective actions, clear remediation deadlines, and assignment of responsibility for implementation. These corrective actions could also include enhancement of controls and procedures.

9.6.5. Follow-Up and Record-keeping

The Company shall monitor the timely implementation of all corrective actions arising from the audit and retain audit reports, remediation plans, and follow-up evidence in accordance with applicable recordkeeping requirements.

9.7. Version Control

The Company is constantly improving its AML/CFT Policy in order to actively combat Money Laundering and the Financing of Terrorism. Therefore, it requires version control to keep track of said changes and approval by the Board of Director(s).

Version	Date	Author
1.0	29 May 2025	De-Anne Kelly
2.0	23 December 2025	De-Anne Kelly

LBC Enterprises B.V.

Curacao, 23 December 2025

_____

Capital Trust Corporation N.V.

Managing Director

D.Kelly
_____

De-Anne Kelly

Money Laundering Compliance Officer