

ANTI-MONEY LAUNDERING, COUNTER-
TERRORISM FINANCING, AND COUNTER-
PROLIFERATION FINANCING
(AML, CTF AND CPF) POLICY

CONFIDENTIAL

Table of Contents

1	DEFINITIONS	4
2	PREFACE	6
2.1	COMPLIANCE STATEMENT	6
2.2	APPLICABLE LEGISLATION	6
2.3	DOCUMENT MAINTENANCE AND REVIEW	7
2.4	CONSEQUENCE OF NON-COMPLIANCE	8
3	THE RISK-BASED APPROACH	8
3.1	EXPLANATION OF THE RISK-BASED APPROACH	8
3.2	BUSINESS RISK ASSESSMENT	8
4	CUSTOMER DUE DILIGENCE (CDD)	10
4.1	CUSTOMER ACCEPTANCE POLICY	10
4.1.1	<i>Customer Risk Assessment</i>	10
4.1.2	<i>Prohibited Accounts</i>	12
4.2	CDD MEASURES	12
4.3	ENHANCED DUE DILIGENCE	14
4.3.1	<i>Source of Wealth</i>	14
4.4	SIMPLIFIED DUE DILIGENCE	16
4.5	SANCTIONS SCREENING	16
4.6	POLITICALLY EXPOSED PERSONS (PEPs)	17
4.6.1	<i>CDD Measures Specific to PEPs</i>	17
4.7	ONGOING MONITORING	18
4.7.1	<i>Ongoing Customer Profile Monitoring</i>	18
4.7.2	<i>Ongoing Transaction Monitoring</i>	19
4.8	BUSINESS AFFILIATE AND SUPPLIER DILIGENCE	20
5	REPORTING UNUSUAL TRANSACTIONS	20
5.1	REPORTING OBLIGATIONS	20
5.2	RECOGNITION OF UNUSUAL TRANSACTIONS	21
5.3	PROHIBITION OF DISCLOSURE	22
5.4	RECORD KEEPING	23
6	ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	23
6.1	APPOINTMENT OF A MONEY LAUNDERING COMPLIANCE OFFICER	23
6.1.1	<i>Duties of the Compliance Officer</i>	24
6.2	EMPLOYEE SCREENING AND TRAINING PROGRAMS	24
6.2.1	<i>Employee Due Diligence</i>	24
6.2.2	<i>Training</i>	25
6.3	INDEPENDENT AUDIT FUNCTION	26
7	APPENDIX I: COUNTRY RISK LIST	27
8	APPENDIX II: INTERNAL UNUSUAL ACTIVITY REPORT	29

Document Information

Approval	Managing Director
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	June 17, 2026
Next Review Date	June 17, 2027

Version History

Date	Ver.	Author	Summary Changes	Approved by Director
September 2024	1.0	Paloma Media B.V.	Document creation as part of AML Program review	
May 2025	2.0	Paloma Media B.V.	Document update as part of AML Program review	
June 2026	2.1	Paloma Media B.V.	Document update as part of AML Program review	

1 Definitions

Casino means Paloma Media B.V. with Certificate of Operation under application number OGL/2024/677/0722 from the Curaçao Gaming Control Board.

CFATF means The Caribbean Financial Action Taskforce, an organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.

Compliance Officer means a senior officer at management level and independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.

FATF means The Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

FATF Recommendations means A framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;

Financial Transactions include the purchase or cashing in of casino chips or tokens, the opening of an account, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that include only casino chips or tokens. Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

Financing of proliferation (PF) 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.

FIU means The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.

CGA means the Curaçao Gaming Authority.

Kingdom Sanctions Act means The National Ordinance also known as the "Rijkssanctiewet", published under N.G. 2016 no. 54.

Money laundering (ML) is the process of concealing the true origins of illegally obtained funds, making them appear to originate from legitimate sources. ML encompasses a broad range of activities, including attempts to turn criminally obtained money into 'clean' money, transferring the benefits of crimes like theft or fraud, and facilitating the laundering of criminal or terrorist property. This process typically occurs in three stages – placement, layering and integration.

NOIS means National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).

Politically Exposed Persons (PEPs) means Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Sanctions National Ordinance means The National Ordinance also known as the “Sanctielandsverordening”, published under N.G. 2014 no. 55.

Source of Funds Refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.

Source of Wealth is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.

Targeted financial sanctions are measures imposed by governments or international bodies to restrict the financial activities of specific individuals or entities linked to unlawful activities, such as terrorism or money laundering. These sanctions aim to prevent these parties from accessing the financial system. Unlike general sanctions that apply broadly to entire countries, targeted sanctions focus on specific individuals or entities. This approach minimizes the impact on the wider population while addressing particular risks. Targeted financial sanctions apply to individuals or entities listed on sanctions lists maintained by organizations like the United Nations or the European Union.

Terrorism Financing (TF) refers to the provision of funds or financial support for terrorist acts, individuals, or organizations, and is characterized by the intent to intimidate populations or compel governments and international bodies to act or refrain from acting. Unlike ML, which always involves proceeds from illegal activities, terrorist financing may not necessarily derive from illicit sources; instead, it often utilizes legitimate funds from charitable donations, business profits, or foreign government sponsorships. While both terrorism financing and money laundering may employ similar methods – such as cash smuggling, structuring, wire transfers,

and the use of debit and credit cards – the primary concern of TF is to obscure the intended use or end recipient of the funds rather than their origin. Additionally, funding for terrorist activities does not always require large sums of money, as it can accumulate over time through simple transactions.

Unusual transaction A transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.

(Ultimate) beneficial ownership (UBO) Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

2 Preface

2.1 Compliance Statement

Paloma Media B.V. (the Company), being established in and governed by the laws of Curaçao, is committed to implementing robust policies to prevent money laundering (ML), terrorism financing (TF), and proliferation financing (PF). In light thereof, the Company has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (AML, CTF AND CPF) policy. Adherence to this Policy is obligatory and vital for guaranteeing that the Company remains in full compliance with relevant laws and regulations pertaining to AML, CTF AND CPF. As a responsible gaming enterprise operating in Curaçao, we acknowledge the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

2.2 Applicable Legislation

The local authorities in charge of the supervision of AML/CFT/CFP matters for the gaming sector are the Curaçao Gaming Control Board (GCB) and the Curaçao Financial Intelligence Unit (FIU). The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- 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);

- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282)
- National Decree supervisor unusual transactions gaming sector (L.B, 28.01.2019, no. 19/0283)
- 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 Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- 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 10 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 10 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 Decree prohibition of import, export, and transit of Venezuelan Gold (N.G. 2019, no. 82).
- National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no.74) as amended by (N.G. 2014, no. 90).
- GCB's Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

The Company's operations are guided by collaboration with international regulatory bodies, including the Financial Action Taskforce (FATF) and the Caribbean Financial Action Task Force (CFATF), strengthening our compliance with global standards.

2.3 Document Maintenance and Review

This AML, CTF AND CPF policy is designed to meet the legal requirements as outlined by the Curaçao Gaming Authority and to foster a culture of compliance within our organization.

Regular reviews and updates will be conducted to adapt to evolving regulations and business needs. The maintenance and review of this document will take place annually.

2.4 Consequence of Non-Compliance

Violations of this policy may result in severe consequences, including disciplinary actions up to and including termination of employment for staff members found in breach of these regulations. Additionally, non-compliance can expose the casino to significant legal implications, including fines, sanctions, and potential criminal charges, which could severely impact our reputation and operational viability. Furthermore, failure to adhere to AML regulations may lead to increased scrutiny from regulatory authorities, loss of licenses, and damage to our business relationships.

3 The Risk-Based Approach

3.1 Explanation of the Risk-Based Approach

The Company adopts a risk-based approach in our AML compliance program, as recommended by FATF guidelines. This approach is essential for identifying and mitigating ML/TF risks specific to the online gaming industry. When developing its AML compliance program, the Company assesses risks in such a way that higher risks necessitate more robust measures to mitigate them. Conversely, for lower-risk scenarios, the Company may employ simplified measures.

To effectively apply the risk-based approach, the Company conducts a preliminary assessment of the risks associated with money laundering and terrorist financing within the organization, and based thereon develops and implements suitable policies, procedures, and controls to manage and mitigate these identified risks, including the present Policy.

The Company shall continuously monitor and enhance the effectiveness of these policies, procedures, and controls, ensuring that it maintains thorough documentation of its risk assessments, detailing all actions taken and the rationale behind them. The Company shall also assess and manage risks associated with emerging technologies and new gaming products that may facilitate ML/TF/PF activities.

3.2 Business Risk Assessment

The Business Risk Assessment (BRA) framework is an essential element of the Company's AML/CFT/CPF compliance program. It offers a systematic risk-based approach to identifying, assessing, and mitigating the risks associated with money laundering, terrorist financing, and proliferation financing within the Company's operations.

The Company conducts comprehensive BRAs and evaluates potential risk factors related to customers, products, services, geographic locations, and delivery channels. Each identified risk

factor is assessed using a structured methodology based on its likelihood and potential impact, utilizing both quantitative and qualitative data.

For each risk factor, the following elements are assessed:

- Likelihood – the probability that the identified risk could materialize, taking into account factors such as transaction volumes, customer behavior patterns, accessibility of products, cross-border exposure, and historical incidents;
- Impact – the potential regulatory, financial, operational, and reputational consequences to the Company should the risk materialize, including exposure to sanctions breaches, regulatory enforcement, license impact, and financial loss.

Each risk factor is assigned a rating of Low, Medium or High based on a combined assessment of likelihood and impact.

Tailored controls and measures are then implemented to address the identified risks, tailored to the specific level and nature of the threat. Residual risk is evaluated to determine whether it falls within the Company's defined risk appetite. Where residual risk exceeds acceptable levels, additional mitigating measures must be implemented or the activity, product, customer segment, or geographic exposure must be restricted or discontinued.

The Company distinguishes between:

- Inherent risk: the level of risk present before the application of mitigating controls; and
- Residual risk: the level of risk remaining after the application of controls such as CDD, EDD, transaction monitoring, sanctions screening, customer limits, product restrictions, and reporting procedures.

All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities. The Board of Directors shall formally approve the BRA and risk appetite.

BRAs are conducted regularly to ensure that the Company's risk profile stays current and accurate, with a comprehensive assessment performed annually. Additional assessments may be prompted by significant events, such as the launch of new products, changes in regulations, or substantial shifts in the business landscape. The Company does not accept customers or business relationships that fall outside of the defined risk appetite, including those involving sanctioned jurisdictions or anonymity-enhancing products.

4 Customer Due Diligence (CDD)

4.1 Customer Acceptance Policy

4.1.1 Customer Risk Assessment

The Customer Risk Assessment procedure is a key component of the Company's internal AML, CTF and CPF framework. It is designed to identify, assess, and manage the specific ML/TF/PF risks associated with establishing and maintaining a business relationship with a customer.

The assessment begins when a new customer applies for an account. Based on the information collected during registration, verification, screening, and transaction monitoring, the Company develops an initial customer risk profile and assigns a Customer Risk Rating. This rating determines the level of due diligence, intensity of ongoing monitoring, and frequency of review applicable to the customer. Higher-risk customers are subject to more frequent and rigorous monitoring, enhanced due diligence, and additional approval requirements where applicable.

The Customer Risk Assessment considers, at a minimum, the following risk factors:

- **Customer Risk:** This includes an assessment of the customer's background, occupation or business activity, expected account activity, source of funds where relevant, transaction patterns, and any other information known to the Company. Higher-risk customer categories may include politically exposed persons, high spenders, disproportionate spenders whose gaming activity does not appear consistent with their known or expected financial profile, customers with multiple or irregular income sources, customers using third parties, and customers whose activity may indicate attempts to circumvent customer due diligence measures.
- **Product and Service Risk:** This includes an assessment of the risks associated with the Company's gaming products, services, account functionality, and payment methods. Higher-risk factors may include products that allow customers to influence outcomes, peer-to-peer gaming, unusual account usage, multiple accounts or wallets, anonymous or difficult-to-trace payment methods, virtual assets, prepaid cards, unlicensed electronic wallets, and indicators of identity fraud.
- **Geographic Risk:** This includes an assessment of the customer's nationality, residence, place of birth, IP location, payment location, and any other relevant geographic connection. Higher-risk jurisdictions include countries with weak AML/CFT controls, high levels of corruption, sanctions exposure, terrorism financing concerns, or other financial crime risks. Relevant sources may include the FATF list of high-risk jurisdictions subject to a call for action, the FATF list of jurisdictions under increased monitoring, CFATF public statements, OFAC sanctions lists, Kingdom Sanction Act Decrees, and other credible risk

indices. The Company maintains and regularly updates an internal High-Risk Country List.

- **Delivery Channel Risk:** This includes an assessment of the method by which the business relationship is established and transactions are conducted. Non-face-to-face onboarding, remote verification, use of intermediaries, use of technologies that may increase anonymity, and channels that limit the Company's ability to verify customer identity or activity may present increased risk. The Company applies reasonable controls to mitigate these risks.

Following the assessment, customers are classified as low, medium, or high risk. The level of due diligence and ongoing monitoring applied must correspond to the customer's risk classification.

For customers assessed as **low risk**, Simplified Due Diligence may be applied, provided that no risk-enhancing factors are present and the customer's transactions remain below the applicable CDD threshold of Cg. 4,000.

For customers assessed as **medium risk**, the Company must obtain additional information and documentation as required by its policies and procedures. This may include further information on the customer's expected activity, payment methods, occupation, or source of funds where relevant.

For customers assessed as **high risk**, the Company must apply Enhanced Due Diligence. High-risk customers include, but are not limited to, politically exposed persons, customers connected to high-risk jurisdictions, customers with complex or unusual activity, customers whose actual account activity materially exceeds their expected profile, customers with disproportionate spending, and customers whose financial background cannot be reasonably understood based on the information already available.

Accounts classified as high risk or displaying unusual or potentially suspicious behaviour must be escalated to the Compliance Officer for further investigation. The Compliance Officer must determine whether the customer's risk rating remains appropriate, whether additional EDD measures are required, whether activity should be restricted pending review, and whether an unusual transaction report must be submitted to FIU Curaçao.

Certain high-risk customer categories, including politically exposed persons and any other customer category identified in this Policy, require approval from the Compliance Officer and, where required, senior management before the Company may establish or continue the business relationship, increase account limits, process significant transactions, or permit continued activity that exceeds the customer's expected profile.

This structured approach ensures that the Company identifies, assesses, documents, and mitigates customer-related ML/TF/PF risks in a risk-based and proportionate manner, in line with applicable AML, CTF and CPF requirements.

4.1.2 Prohibited Accounts

The Company's customer acceptance policy is formulated in accordance with legal requirements and aligns with the Company's risk appetite as well as the BRA. Therefore, certain categories of individuals are prohibited from being accepted as customers, either by preventing them from registering or by blocking their access to our site, as necessary:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by UN, EU or OFAC.
- Individuals for whom there are reasonable grounds to suspect involvement in ML/TF/PF or any other form of criminal activity.
- Self-excluded customers who are barred from our websites or included in any national self-exclusion registers as stipulated by licensing conditions.
- Individuals who have submitted documents or information that the Company has reasonable grounds to suspect are fraudulent or falsified.
- Customers for whom an elevated risk level in their profile has led the Company to terminate the customer relationship for any reason.

4.2 CDD Measures

The Company has an obligation to undertake CDD measures when:

- players engage in financial transactions equal to or above Cg. 4,000.00;
- carrying out occasional transactions above the monetary equivalent of Cg. 4,000.00;
- there is a suspicion of money laundering or terrorist financing; or
- the casino has doubts about the veracity or adequacy of previously obtained customer identification data.

The CDD measures to be taken are as follows:

- *Identifying* the player and *verifying* that customer's identity using reliable, independent source documents, data or information;
- *Identifying the beneficial owner* and taking reasonable measures to *verify the identity of the beneficial owner*, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the *purpose and intended nature of the business relationship*;
- Conducting *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 casino's knowledge of the player, its business and risk profile, including, where necessary, the source of funds.

The Company's CDD procedures require prospective customers to create a full profile at the point of registration. Mandatory information required at registration stage includes:

- Full name;
- Date of birth;
- Permanent residential address;
- Unique and verified email address;
- Phone number;
- Unique nickname; and
- Password.

To complete the required customer identification and verification process, the Company asks its customers to upload a copy of valid identification documents. This request is sent to the customer's registered email address. If needed, the customer may also receive a phone call to help with the verification process. If the documents are in a different language, the Company will take necessary steps to ensure that the documents adequately prove the customer's identity, such as obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation.

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. Documents issued by the government that lack a photograph can be used to confirm the customer's current address, provided the address is included in the document.

If a document submitted by a potential customer does not meet the verification standards, the compliance officer or designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance.

Once a non-compliant document is identified, the customer must be informed without delay. If the customer cannot provide compliant documents within 30 days from the moment the Cg. 4,000.00 threshold is reached; the Company shall terminate the relationship with the customer and report the transaction to the FIU.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

4.3 Enhanced Due Diligence

Enhanced Due Diligence (EDD) will be implemented for customers identified as higher risk, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. Enhanced Due Diligence has to be conducted where the risks of money laundering or terrorist financing are higher. In any case, the following scenarios are subject to EDD:

- Residents of higher risk geographic areas;
- Politically Exposed Persons (PEP's);
- Products or transactions that might favor anonymity;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. They should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of EDD measures include but are not limited to:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

4.3.1 Source of Wealth

As part of the Company's EDD measures, source of wealth information must be obtained and, where appropriate, verified for customers who are identified as high-risk following the Company's comprehensive customer risk assessment. This includes, but is not limited to, politically exposed persons, customers connected to high-risk jurisdictions, customers with complex or unusual activity, customers whose actual account activity materially exceeds their expected profile, or customers whose financial background cannot be reasonably understood based on the information already available.

Source of wealth refers to the origin of the customer's overall wealth or net worth, rather than the specific funds used for an individual transaction. The purpose of obtaining sources of wealth information is to assess whether the customer's expected and actual level of account activity is

reasonable and proportionate when compared with their apparent financial position, occupation, business activity, income level, or other known background information.

For high-risk customers, the Company must obtain sufficient information to understand how the customer accumulated their wealth. Possible sources of wealth may include, but are not limited to, employment income, business ownership or profits, dividends, investments, sale of assets, inheritance, gifts, property ownership, rental income, pension income, insurance payouts, legal settlements, cryptocurrency holdings or gains, gambling winnings, trust distributions, or other legitimate and verifiable sources of wealth.

Depending on the circumstances and the customer's risk profile, acceptable supporting documentation may include recent tax returns, salary slips, employment contracts, audited financial statements, company ownership documents, dividend statements, bank statements, investment portfolio statements, sale and purchase agreements, notarial deeds, property records, inheritance documents, gift letters supported by evidence of the donor's financial capacity, trust documents, loan agreements, pension statements, insurance payout confirmations, crypto exchange records, wallet transaction history, or other reliable documents evidencing how the customer accumulated their wealth.

The documentation obtained must be sufficiently recent, complete, credible, and relevant to support the customer's explanation. The Company must verify, to the extent reasonably possible, that the information and documentation are genuine, consistent with the customer's profile, and sufficient to explain the customer's level of wealth and expected account activity. Self-declarations, screenshots, unverifiable statements, or incomplete documents should not be accepted as sufficient evidence in high-risk cases unless supported by additional independent and reliable information.

Where source of wealth information is required, the matter must be escalated to the Compliance Officer. The Compliance Officer must review the customer's risk assessment, source of wealth explanation, supporting documentation, transaction history, expected and actual account activity, jurisdictional risk, screening results, and any other relevant information. The Compliance Officer must determine whether the source of wealth has been satisfactorily established, whether the customer's risk rating remains appropriate, whether additional EDD measures are required, and whether any mitigating measures should be applied.

For PEPs and other high-risk customers, approval from the Compliance Officer is required before the Company may establish or continues the business relationship, increase account limits, process significant transactions, or permit continued activity that exceeds the customer's expected profile. Where the risk is significant, unresolved, or outside the Company's risk appetite, senior management approval must also be obtained.

All source of wealth requests, customer responses, documents received, verification steps, internal assessments, escalation decisions, approvals, mitigating measures, and related reporting decisions must be documented and retained in accordance with the Company's record-keeping obligations.

4.4 Simplified Due Diligence

In low-risk scenarios, where the risks of ML/TF/PF are lower, simplified due diligence measures may be applicable, balancing the need for compliance with operational efficiency. Such measures include but are not limited to:

- *Not collecting specific information:* If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the casino to obtain the player's identity.
- Verifying the identity of the customer and the beneficial owner *after* the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the Company can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low-risk situations, the Company has to verify the basic identification details, while the verification of any other personal details is upon the Company, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of ongoing monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply, or when the customer reaches the threshold prescribed above of Cg. 4,000.00.

4.5 Sanctions Screening

We are committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with these sanctions. The Company shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.

The Company shall perform perpetual sanctions screening on customers and also perform trigger-based sanctions screening of customers at least in the following scenarios:

- At the moment of registration;
- At the moment of withdrawal request;
- At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered, the Company shall immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and the Compliance Officer shall immediately file a report with the FIU. Once the true match is confirmed by the supervisory authority, the Company shall terminate services and keep the frozen assets until further instruction from the supervisory authority.

4.6 Politically Exposed Persons (PEPs)

A PEP is an individual who is entrusted with prominent public functions, other than middle ranking or more junior officials, including the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers,
- members of parliament or of similar legislative bodies,
- members of the governing bodies of political parties,
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances,
- members of courts of auditors or of the boards of central banks,
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces,
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organization.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.

4.6.1 CDD Measures Specific to PEPs

The Company implements appropriate risk management systems to identify whether a customer or beneficial owner is a PEP, or a relative or close associate of one. This includes, at first instance, conducting comprehensive screening against reliable databases and lists to determine the PEP status of new customers during the onboarding process.

No business relationship shall be established or continued with a PEP before obtaining senior management¹ approval to service the PEP. This applies to new customers, ongoing relationships, and any occasional transactions.

In addition, the Company takes reasonable measures to ascertain the source of wealth and source of funds of the PEP. This involves:

- Requesting a statement from the PEP regarding their Source of Wealth.
- Verifying the statement through independent and reliable sources. Public sources will be consulted first, and if insufficient, additional documentation may be requested from the customer.

Additionally, the Company shall conduct enhanced ongoing monitoring of the business relationship, including analysis of the PEP's spending patterns to ensure they align with their declared legal sources of funds and the information on file.

In accordance with the risk-based approach that the Company employs, measures are tailored to the risk of the PEP, where the following are taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

PEP status screening will be conducted regularly throughout the business relationship. If a player who was not identified as a PEP at onboarding later becomes one, the Company is required to implement the enhanced due diligence measures outlined above within a thirty-day window of this determination. Failure to implement the required measures for newly identified PEPs within the specified timeframe will result in the termination of the relationship with that customer.

4.7 Ongoing Monitoring

4.7.1 Ongoing Customer Profile Monitoring

During the periodic review of a customer, the Company verifies and confirms that the CDD information about the client, nature and purpose of the business relationship, and SOF is still accurate and up to date, evaluate if there are external signals (bad press/adverse news, incidents) that could give rise to a change in the business risk profile of the customer and ensure to perform screening against sanctions lists and PEP lists. The periodic review also includes an overall review of the transaction behavior of the client to determine if unusual activities have taken place, for instance in case of transactions which normally would not be expected.

¹ Senior management refers to individuals responsible for day-to-day operations or their immediate subordinates. Approval may also be sought from the Compliance Department manager.

The periodical review of the customer is based on the risk profile of the customer:

- For high-risk customers – once per year;
- For medium risk customers – once every 2 years;
- For low-risk customers – once every 3 years.

4.7.2 Ongoing Transaction Monitoring

The Company performs both real-time monitoring of transactions, as well as post-event monitoring, to ensure that such transactions and activity are consistent with the Company's knowledge of the client, declared or expected source of funds, and anticipated betting and transactional behaviour. More attention is paid to high amounts, high-risk clients and high-risk jurisdictions.

Where transactions or activity are inconsistent with the Company's knowledge of the customer, the Company must take reasonable steps to establish and verify the source of funds used for the relevant transaction or activity. Source of funds refers to how the specific funds used by the customer were obtained. Possible sources of funds may include, but are not limited to:

- Salary, wages, bonuses, or other employment income
- Business profits, dividends, or shareholder distributions
- Savings or accumulated personal funds
- Sale of property, vehicles, shares, or other assets
- Investment returns, including interest, dividends, or capital gains
- Loan proceeds from regulated financial institutions or private lenders
- Inheritance or gifts
- Pension payments or retirement benefits
- Insurance payouts or legal settlements
- Rental income or other passive income
- Cryptocurrency trading, mining, staking, or digital asset sales
- Gambling winnings or other lawful gaming proceeds
- Trust distributions or family office transfers
- Any other legitimate and verifiable source of funds

Depending on the circumstances, acceptable documentation may include, where relevant, recent bank statements, payslips, employment contracts, tax returns, audited financial statements, sale agreements, loan agreements, inheritance documents, proof of business income, crypto exchange records, wallet transaction history, or other reliable documents evidencing the origin of the funds.

The documentation obtained must be sufficiently recent, complete, and credible to explain the transaction or activity under review. The Company must verify, to the extent reasonably possible,

that the documents are genuine, consistent with the customer's profile, and support the customer's explanation. Screenshots, self-declarations, or incomplete documents should not be accepted as sufficient evidence unless supported by additional reliable information. Any inconsistencies, unexplained gaps, or concerns regarding the authenticity or adequacy of the documentation must be resolved before the activity may be treated as satisfactorily explained.

For high-risk customers, politically exposed persons, transactions involving high-risk jurisdictions, or cases where the source of funds explanation is complex, incomplete, or raises concern, approval from the Compliance Officer is required before the Company may continue the business relationship or allow further relevant transactions. Where the risk is significant, unresolved, or outside the Company's risk appetite, senior management approval must also be obtained in accordance with the EDD measures applicable under this Policy.

All source of funds requests, customer responses, documents received, verification steps, internal assessments, escalation decisions, approvals, and reporting decisions must be documented and retained in accordance with the Company's record-keeping obligations.

4.8 Business Affiliate and Supplier Diligence

The Company recognizes that when contracting or outsourcing specific functions, there is a risk of increased AML exposure if the third parties involved are not properly vetted and their relevant processes are not assessed. Prior to entering into any service agreements that fall under this Policy, the Company performs due diligence to verify the legitimacy of the potential partners.

This due diligence includes, at a minimum, obtaining the following documents:

- Certificate of Incorporation and Memorandum & Articles of Association
- Identification of Directors and/or Shareholders
- Declaration of Beneficial Ownership
- KYC documentation for signatories, as applicable.

Additionally, potential third-party suppliers are required to submit a copy of their AML/CTF policies and procedures, where applicable. The Compliance Officer will review these documents for their accuracy and completeness prior to entering into any agreements.

5 Reporting Unusual Transactions

5.1 Reporting Obligations

All unusual activities and transactions, including attempted transactions, are initially reported internally. The officers responsible for transaction monitoring must immediately report any unusual activities to the Compliance Officer upon identification, providing a brief description of

the specific mitigating measures taken. The Company confirms that it is duly registered with the FIU Curaçao's goAML platform for the submission of unusual transaction reports.

All employees who engage with customers or have access to customer information receive anti-money laundering training. This training prepares them to identify actions by customers that may reasonably raise suspicions of money laundering or terrorism financing. Staff members are expected to recognize and understand any gaming or transaction behaviors that might indicate customer involvement in money laundering or terrorism financing. If they know, suspect, or have reasonable grounds to believe they are dealing with the proceeds of crime, they must submit an Internal Unusual Activity Report to the Compliance Officer (CO) in accordance with the Reporting Procedure. This ensures that the employee's legal obligation to report is fulfilled. Please see [Appendix II](#) for the Report form.

Employees are required to report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed, using the Internal Unusual Activity Report form. If a more in-depth investigation is necessary, the Compliance Officer will complete this within ten (10) business days. During this time, the Compliance Officer may request additional information from relevant departments.

If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU Curaçao regarding any unusual monetary operations or transactions within 48 hours. In any cases whereby the report is made under one of the objective indicators, as defined below, the report must be made to the FIU Curacao no later than 48 hours after the transaction has been executed.

5.2 Recognition of Unusual Transactions

Staff will be trained to recognize unusual transactions based on customer profiles and specific indicators. Reporting procedures to the compliance officer will be established.

According to NORUT, the Company is observing both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. All such transactions must be reported to the compliance officer in a format approved by management. Additionally, any supporting documentation, such as copies of identification, cash-out slips, and other relevant records, must also be submitted as supplements.

The Compliance Officer is tasked with maintaining an organized filing system for these records. If the casino fails to report internally identified transactions to the Financial Intelligence Unit (FIU), the rationale for this decision must be thoroughly documented and signed by the compliance officer and/or management. In accordance with the FATF Recommendations, the Company and its employees pay particular attention to all complex or unusually large

transactions, as well as any unusual transaction patterns that lack a clear economic or legitimate purpose.

The following transactions or intended transactions are deemed unusual:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Cg. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 1. A cashless transaction in the amount of Cg. 5,000.00 or more.
 2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of Cg. 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as “objective indicators”, while (d) is referred to as “subjective indicator”. While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

5.3 Prohibition of Disclosure

All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

The Company has implemented a system of measures to ensure that employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the Financial Intelligence Unit Curaçao are safeguarded from threats or hostile actions by other employees, members of the management body, or customers. Additionally, they are protected from adverse or discriminatory employment actions.

5.4 Record Keeping

The casino retains all necessary records of transactions, both domestic and international, for a minimum of five (5) years to ensure compliance with information requests from regulatory authorities. These records must be detailed enough to allow for the reconstruction of individual transactions, including the amounts and types of currency involved, if applicable, to provide evidence for potential criminal prosecutions.

All records gathered through CDD measures, such as copies of official identification documents, account files, and business correspondence, will be stored for at least five (5) years after the business relationship has ended or after the date of an occasional transaction.

Records shall be stored in a manner that ensures their integrity, confidentiality, and accessibility. Electronic records shall be stored in secure, encrypted databases with access controls to prevent unauthorized access. Physical records shall be stored in locked, fireproof cabinets within secure areas of the office. Access is restricted to authorized personnel only. Regular backups of electronic records shall be conducted and stored in a separate, secure location to prevent data loss.

After the retention period, records shall be disposed of securely to prevent unauthorized access or disclosure. Electronic records must be permanently deleted using secure deletion software that ensures data cannot be recovered. Physical records must be shredded using cross-cut shredders or incinerated to ensure complete destruction.

When properly ordered to do so by any enactment, rule of law or court order, the Company shall provide a document, customer due diligence information, or enhanced due diligence information and the Company will maintain a register of the documents and information provided, and will keep a copy of the same.

6 Anti-Money Laundering Compliance Program

6.1 Appointment of a Money Laundering Compliance Officer

Curleigh Cochrane has been appointed as the Compliance Officer, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML/CTF compliance officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

The Compliance Officer can be contacted at cc@aimcompliance.io

6.1.1 Duties of the Compliance Officer

The Compliance Officer shall be assigned at least 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.

6.2 Employee Screening and Training Programs

6.2.1 Employee Due Diligence

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing the Company's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors.

The employee due diligence process is informed by the Company's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate money laundering, or terrorism financing must undergo screening. This requirement applies to:

- Prospective employees prior to their hiring for such roles.
- Current employees before they are transferred or promoted to such positions.

To screen both current and potential employees, the Company should:

- Identify the individuals.
- Verify their identity.
- Confirm their employment history, such as through references.

- Determine their suitability for the position and assess whether they pose any risk to the Company.

The Company will consider the knowledge and qualifications required for the responsibilities and authorities associated with each role.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. The Company must evaluate whether:

- The employee has a criminal record, which may be verified through a police check.
- The employee is or has been subject to regulatory, court, or legal actions.
- The employee has leveraged bankruptcy laws for personal gain.
- The employee has resided in high-risk countries or regions.

Regular updates and re-evaluations are essential for maintaining an effective compliance program against money laundering, terrorism financing, and proliferation financing. This process includes conducting periodic reviews of all employees, with a particular emphasis on those in high-risk roles, to ensure their risk profiles are accurate and current. Additionally, reviews triggered by significant changes in an employee's job responsibilities, promotions, or external alerts that may influence their risk status are also initiated.

6.2.2 Training

In delivering AML, CTF and CPF training to the designated categories of employees, the Company will consider the necessary knowledge and qualifications required for their duties, responsibilities, and authorizations. As part of the training framework, the Company will outline the AML, CTF and CPF requirements and provide comprehensive information on the measures and activities that staff are expected to undertake within their roles.

The Company will ensure that documentation of the training provided to staff is maintained, capturing the following information:

- 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.

The Company will regularly update the training programs to reflect any changes in internal and external regulations, as well as developments in the availability of training programs in the market for external training. Furthermore, extraordinary training in AML, CTF and CPF matters will be provided in specific situations, including:

- The introduction of new internal and external regulations related to AML, CTF and CPF that apply to the Company's staff.
- The launch of new products or services that alter the AML, CTF and CPF risk exposure.
- Instances where an employee breaches internal or external AML, CTF and CPF regulations due to a lack of knowledge during the performance of their duties.

6.3 Independent Audit Function

An independent audit function will be established for the annual evaluation of the AML program, ensuring audit personnel are qualified and findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate the Company's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

7 Appendix I: Country Risk List

Please note that the following list of high-risk and low-risk countries is subject to continuous review. Any changes in geographical risk will be reflected promptly to ensure the list remains current and accurate at the time of drafting.

High-risk countries include:

1. Afghanistan
2. Algeria
3. Angola
4. Belarus
5. Bulgaria
6. Burkina Faso
7. Burma (Myanmar)
8. Cameroon
9. Central African Republic
10. China
11. Côte d'Ivoire
12. Croatia
13. Cuba
14. Democratic People's Republic of Korea
15. Democratic Republic of the Congo
16. Ethiopia
17. Gibraltar
18. Haiti
19. Iran
20. Iraq
21. Kenya
22. Lebanon
23. Libya
24. Mali
25. Monaco
26. Mozambique
27. Namibia
28. Nicaragua
29. Nigeria
30. Panama
31. Philippines
32. Russia
33. Somalia

34. South Africa
35. South Sudan
36. Syria
37. Tanzania
38. Uganda
39. United Arab Emirates
40. Vanuatu
41. Venezuela
42. Vietnam
43. Yemen

Low-risk countries include:

1. Antigua and Barbuda
2. Aruba, Kingdom of the Netherlands
3. Belize
4. Bermuda
5. Cayman Islands
6. Denmark
7. Dominica
8. Finland
9. Grenada
10. Guyana
11. Montserrat
12. New Zealand
13. Norway
14. Saint Kitts and Nevis
15. Saint Lucia
16. Saint Vincent & the Grenadines
17. Singapore
18. Sint Maarten Kingdom of the Netherlands
19. Suriname
20. Sweden
21. Turks and Caicos Islands

Excluded markets include, but are not limited to:

1. Aruba
2. Australia
3. Austria
4. Belgium
5. Bonaire
6. Czech Republic
7. Curacao
8. France
9. Germany
10. Greece
11. Lithuania
12. Saba
13. Sint Eustatius
14. Spain
15. The Netherlands
16. United States of America

CONFIDENTIAL

8 Appendix II: Internal Unusual Activity Report

Internal Unusual Activity Report		
Date of report:		
Client full name:		
Client ID:		
Risk rating:		
Account status (Active/Suspended/Blocked):		
Account balance:		
Date of account registration:		
Client details: E-mail:		
Client details: Phone number:		
Client details: Brand registration:		
Date of birth:		
Nationality/Country of registration:		
Address:		
Due diligence documents held:		
Reason for reporting: explain what activity / transaction gave rise to the report. If necessary, please use the additional information section:		
Date of suspected criminal activity/transaction:		
Provide details (e.g. dates and amounts) of any known intended or pending transactions:		
Name (reporting employee):	Signature:	Date:

PALOMA MEDIA B.V. AML, CTF & CPF POLICY

Upon completion, please forward the form to the department responsible as soon as possible.		
Action taken by the responsible department		
Confirmation of receipt of the MLRO: I confirm that I have received this form from the person(s) named above.	Signature:	Date: