

INTERNAL AML POLICY OF ONLINE BETTING COMPANY/ONLINE CASINO

of CUPWIN B.V. - revision #3 dated 05.09.2024

SECTION 1. INTRODUCTION.....	1
SECTION 2. ANTI-MONEY LAUNDERING AND TRANSACTION FRAUD.....	1
SECTION 3. SECURITY AND MONITORING.....	2
SECTION 4. RESPONSIBLE RELATIONSHIPS WITH CUSTOMERS AND BUSINESSES.....	2
SECTION 5. AML RULES OF THE ACCOUNT USE.....	3
SECTION 6. FINANCIAL CONTROL.....	3
SECTION 7. ANTI-FRAUD POLICY.....	4
SECTION 8. MONEY LAUNDERING CONTROLS.....	4
SECTION 9. POLITICALLY EXPOSED PERSON IDENTIFICATION.....	5
SECTION 10. PROHIBITED COUNTRIES AND SANCTIONS.....	7
SECTION 11. CLIENTS IDENTIFICATION.....	10
SECTION 12. CUSTOMER DUE DILIGENCE.....	13
SECTION 13. ENHANCED CUSTOMER DUE DILIGENCE.....	14
SECTION 14. SIMPLIFIED CUSTOMER DUE DILIGENCE.....	15
SECTION 15. REPORTING OF UNUSUAL TRANSACTIONS.....	16
SECTION 16. RECORD KEEPING.....	17
SECTION 17. EMPLOYEE TRAINING.....	18
SECTION 18. RISK SCORING.....	19
SECTION 19. TRANSACTIONS AND ONGOING MONITORING.....	20

SECTION 1. INTRODUCTION

1.1. CUPWIN B.V. registration number 164533, a company organized and existing under the laws of Curacao, whose registered office is at Abraham Mendez Chumaceiro Boulevard 03, Willemstad, Curacao, (hereinafter — «Company») has experience in securing gaming businesses against criminal misuse and implementing wide-ranging anti-fraud and anti-money laundering processes, procedures, and extensive staff training programs. The company has experience in securing gaming businesses against criminal misuse and implementing wide-ranging anti-fraud and anti-money laundering processes, procedures, and extensive staff training programs.

1.2. The Company is not a financial institution and thus should not be treated as such. A client's account will not bear any interest. The Company is not an exchange and therefore does not execute any conversion between any currencies. For the execution of the payment functions under the agency agreement, the Company coordinates its actions and policies with the principal or the gaming operator (hereinafter — «Operator») and acts on behalf of the Operator to fulfill the payment obligations with customers and businesses.

1.3. Underpinning programs will be knowledge of the Proceeds of Crime Act and Money Laundering indicators usually detected in a gaming environment, particularly in a Card Not Present transactional environment.

1.4. The Company is fully aware of all aspects of the Proceeds of Crime Act and its responsibilities and is well placed to impart knowledge of Anti—Money Laundering measures and requirements having secured major remote and non-remote gaming businesses in this field.

SECTION 2. ANTI-MONEY LAUNDERING AND TRANSACTION FRAUD

2.1. Gaming environments are often targeted by those wishing to launder money. The speed of transactions and the use of multiple payment processing options make gaming businesses especially vulnerable to this activity.

2.2. As a result, many of the initial trading and procedural decisions are either directly aimed at combating this threat, or protections are enhanced as a by-product of the overall commercial and trading approach/strategy taken by the business.

2.3. ALL staff will be given training in Money Laundering indicators such as (but not limited to):

- Unusual Betting Patterns;
- Suspicious deposit and withdrawal patterns (size and frequency);
- Reliability of Card Data;
- Customer verification issues and Identity Theft;
- Account linkage/multiple accounting;

2.4. All instances of suspected Money Laundering attempts must be reported to the MLRO but that suspicion must not be conveyed to the customer and further actions must await consent. The

MLRO is then responsible for liaising with, submitting Suspicious Activity Reports. He will also ensure that appropriate registers are kept for all related reporting.

SECTION 3. SECURITY AND MONITORING

3.1 . It is essential to implement adequate monitoring procedures in any gaming business across premises, equipment, people, communications, and transactions. The Company will implement a range of measures and procedures to ensure security and safety in these areas.

3.2. The Company has installed Call recording technology. This has multiple benefits that include:

- Staff Training;
- Ensuring accuracy of bet (timing and placement) and transaction data;
- Customer and Brand Reputation Protection;
- Implementation of robust and frequent monitoring procedures that will guard against and deter collusion between staff and customers;

3.3. The protection of data and the security of software and hardware generally are of prime concern for any business where transactions and data are recorded in a Non-Face to Face environment. Consequently, the Company will implement an overarching policy of 'Encrypt whatever can be Encrypted'. Access to Shared Drives will be strictly limited and monitored and where appropriate, password protected. Data Storage and Back-Up solutions/procedures exist to ensure that Customer Data is not accessible to outside parties and reliably prevents loss of data.

SECTION 4. RESPONSIBLE RELATIONSHIPS WITH CUSTOMERS AND BUSINESSES

4.1. The published policies will make specific reference to fraudulent activity, prior knowledge of a result of the likely result of an event, and matters relating to match-fixing and suspicious events. It will detail the actions we may take where cheating is suspected or identified and will detail the extent to which we will co-operate with regulators and sports governing bodies to tackle these matters. This will in general allow a transparent communication process with customers in these instances.

4.2. However, the Company is acknowledged that if serious criminal activity is suspected or identified, it is also incumbent on them and staff that those suspected of this activity are not 'tipped off' as to those suspicions and subsequent investigations and that in some instances, alternative approaches will be required. Appropriate staff training and escalation procedures will be in place.

4.3. The Company will take all necessary measures to ensure the propriety of its relationships with other businesses. This will entail a standardized due diligence approach often accompanied by Non-Disclosure Agreements where appropriate. This will require default disclosure of ownership and management structures, company incorporation details, address, and contact details. Details of these investigations will be templated, and records kept.

SECTION 5. AML RULES OF THE ACCOUNT USE

5.1 . In order to be able to use the website, a client must first register and open an account.

5.2. One client can open only one (1) account. Only one account for each household, IP, PC is allowed. If a client attempts to open more than one account, all accounts may be blocked or closed and any bets may be voided. Also, any returns, deposits, winnings, or bonuses which a client has gained or accrued during such time as the duplicate account was active will be forfeited by a client and maybe reclaimed by us, and a client will return to the Company on demand any such funds which have been withdrawn from the duplicate account. If a client wishes to open another account, a client may do so by contacting support of the Operator. If a new account is opened, the old account will be closed.

5.3. For transaction security, the Company uses SSL encryption. All customer data will be treated as confidential and will not be sold to third parties.

5.4. A client is not allowed to transfer funds from his/her account to other players or to receive funds from other players into the client's account, or to transfer, sell and/or acquire user accounts.

5.5. The Company reserves the right to retain payments if suspicion or evidence exists of manipulation of the casino system. Criminal charges will be brought against any user or any other person(s), who has/have manipulated the casino system or attempted to do so. The Operator reserves the right to terminate and/or change any games or events being offered on the website.

SECTION 6. FINANCIAL CONTROL

6.1. A client may only participate in games if they have sufficient funds on account for such participation.

6.2. Deposited amounts are available on the account within a reasonable amount of time after the confirmation of the deposit. Before a withdrawal can be made, all previous deposits need to be confirmed.

6.3. A client may only use your own personal credit/debit card or another payment method to fund his/her account. The name appearing on the credit cards, or registered on the payment accounts used for deposits or payouts must correspond to the name registered on the account.

6.4. Cardholders' responsibility is to know the laws concerning online gambling in their country of domicile.

6.5. Participation of minors in the activity offered on this website is prohibited.

6.6. For the execution of the Company's payment functions the Operator reserves the right to carry out verification procedures for each client at first withdrawal. Such verifications may for example include copies of a player's passport, national Identity Card, copies of a player's utility bills, and/or copies of the debit/credit cards used to deposit.

6.7. It's the responsibility of the player to ensure that all documents as a part of the KYC process are genuine. Faked or fraudulent documents provided may result in a confiscation of deposits and potential winnings of the player.

6.8. To make a withdrawal, a player must play through active deposited amounts at least once before the withdrawal. This procedure is in line with anti-money laundering practices.

6.9. The Operator reserves the right to use additional procedures and means to verify a client's identity (Know Your Client) When effecting deposits into the account. This could include (but is not limited to) a selfie with a document or form of identification. To verify a player's account casino management require documents (ID, payment systems, utility bills etc.) in Latin or Cyrillic alphabet. In case the player doesn't have an opportunity to provide documents in the above-mentioned alphabets casino reserves the right to demand video verification where the player shows his/her documents.

6.10. The Operator reserves the right to make a phone call to the number provided in the client's account, which can be a necessary part of the KYC procedure. Until the account is fully verified, no payouts will be processed.

SECTION 7. ANTI-FRAUD POLICY

7.1. If the player is suspected of fraudulent actions including, but not limited to participating in any type of collusion with other players' fraudulent actions against other online casinos or payment provider' chargeback transactions with a credit card or denial of some payments made creating two or more accounts other types of cheating or becomes bankrupt in the country of their residence, the Operator reserves the right to terminate such account and the Company suspends all payouts to the player. This decision is at the sole discretion of the Operator and the player will not be notified or informed about the reasons for such actions.

7.2. Should the Operator become aware of any user who has accepted the bonus or a promotion with the sole purpose of creating a positive expected value on bonus return by using known practices aimed at securing a payout of said bonus by Company or at any way try to take advantage of bonuses received by Operator, then the immediate confiscation of winnings and closure of the account with the right to withhold any further withdrawals will be enforced. An example of advantage play would be delaying any game round in any game, including free spins features and bonus features, to a later time when a client has no more wagering requirement and/or performing new deposit(s) while having free spins features or bonus features still available in a game, the Company reserves the right to withhold any withdrawals and/or confiscate all winnings.

SECTION 8. MONEY LAUNDERING CONTROLS

8.1. In addition, the Company has developed an agreed set of internal procedures about anti-money laundering include:

- Identifying their customers (including their age) and checking their information in detail;
- For protection against identity theft, confidential customer information submitted at any point in time shall be protected from unauthorized or unnecessary disclosure;
- Customer credit card numbers stored on the system shall be secured from unauthorized use;

- Making use of the watch lists containing known or suspected members of terrorist organizations, to try to ensure that they do not hold accounts;
- Monitoring the gaming and in-payment/pay-out behavior of customers;
- Limiting deposits (to a variable extent, since some firms do not have limits but rather monitor carefully those few gamblers who make large online deposits);
- Prohibiting direct payments between customers;
- Prohibiting cash payments;
- Automatic blocking of payments from countries that are not the same as the registered home country of the customer
- After identifying an attempt to launder money, reporting the information to the Financial Intelligence Unit and — depending on the jurisdiction and 'tipping off' rules — blocking the account/ending the commercial relationship.

SECTION 9. POLITICALLY EXPOSED PERSON IDENTIFICATION

9.1. "Politically Exposed Person" means a natural person who is or who has been entrusted with prominent public functions in the Republic or in another country, an immediate close relative of such person as well as a person known to be a close associate of such person:

- (a) heads of State, heads of government, ministers and deputy or assistant ministers;
- (b) members of parliament or of similar legislative bodies;
- (c) members of the governing bodies of political parties;
- (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
- (e) members of courts of auditors or of the boards of central banks;
- (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- (g) members of the administrative, management or supervisory bodies of State-owned enterprises;
- (h) directors, deputy directors and members of the board or equivalent function of an international organisation;
- (i) mayor.

Provided further that no public function referred to in points (a) to (i) shall be understood as covering middle-ranking or more junior officials; Provided furthermore that 'close relatives of a politically exposed person' includes the following:

- (a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

(b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;

(c) the parents of a politically exposed person;

9.2. In a situation where an economic or professional transaction or a participant in the performance of an official act, the customer or their actual beneficial owner is a politically exposed person of national level, a member of the family of a politically exposed person of national level, or a person who is a close associate of a politically exposed person of national level, then the obliged person applies the following customer due diligence measures:

A. receives approval from senior management to establish a partnership or to continue business relationships with that person;

B. applies methods of customer due diligence measures to establish the origin of the material wealth and the sources of funds that are used in partnerships or that are used for the transaction;

C. monitors these partnerships in an enhanced manner of customer due diligence and conducts regular enhanced monitoring, except cases specified in legal acts.

9.3. If a politically exposed person of state-level no longer fulfills the public duties entrusted to him or her, then the obliged entity, for at least 12 months, must take into account the risks that have been associated with the person in question and apply the necessary and risk-based methods until it is sure that the risks inherent in a politically exposed person of a national level no longer arise.

9.4. The Company entity may not apply the methods of customer due diligence described in this part to a politically exposed person of national level, to members of his or her family, and to persons who are considered his or her close associates, if no other circumstances are indicating the presence of other, higher than usual risks.

9.5. The Company should establish the internal procedural rules based on which the decision shall be made whether the potential customer or the actual beneficial owner of the customer is a politically exposed person of state level, a politically exposed person of the local level of a county which is the contracting state of the European Economic Area Agreement or a third country or who performs or performed the public duties assigned to him or her in international organizations. The Company should establish the close associates of a politically exposed person of state-level and members of his or her family only if their connection with the executor of important public duties is known to the public or when the obliged entity has reason to believe that such a relationship exists.

9.6. The Company must apply the enhanced customer due diligence measures in addition to the necessary methods of customer due diligence with regard to a politically exposed person of state-level including the following methods:

A. require the additional information from the customer, as well as to apply all necessary methods to establish sources of wealth and money that are used to establish business relationships or when conducting a transaction;

B. verify data or make inquiries to the relevant databases or open databases or make inquiries or verify data concerning the customer, or to the appropriate supervisory authorities at the

customer's location or on official websites of government agencies. The following data should be checked primarily:

C. a politically exposed person can be identified using the NameScan database: <https://namescan.io/FreePEPCheck.aspx> HYPERLINK

"<https://namescan.io/FreePEPCheck.aspx>", which has a free access, or in any paid database (for example, Thomson Reuters, WorldCheck and others);

D. while checking a politically exposed person of local level, as well as a politically exposed person of national level, it is necessary to perform an additional check up using Google, and also using local search systems in the country of origin of the customer, by entering the customer's name and date of birth both in Latin letters and using the local language.

9.7. The decision to establish a business relationship with a politically exposed person of national level must be taken by the management board of the Company, the responsible member of the management board or the contact person. If a business relationship is established with the customer that will become later on or later it will become known that he or she or actual beneficial owner has become a politically important person of state level in the understanding of this guidance, then it is necessary to inform the man.

9.8. The Company proceeds with PePs screening of clients once a week.

SECTION 10. PROHIBITED COUNTRIES AND SANCTIONS

10.1. The prohibited country is the third country which, on the basis of the OFAC Sanctions Programs, OFSI Sanctions Programs, United Nations Sanctions, Directive (EU) 2015/849 of the European Parliament and of the Council, that regulates the counteraction to money laundering and the financing of terrorism of the financial system and which amends the Resolution (EU) 648/2012 of the European Parliament and of the Council and recognizes invalid, and the Directive (EU) 2005/60/EU of the European Parliament and of the Council and Commission Directive (EU) 2006/70/EU (EU page 141, 05.06.2015, pages 73-117), section 9 part 2, high-risk countries are listed (Annex 14) on the basis of these adopted acts.

10.2. Prohibited countries are listed in Appendix №1, which is an integral part of this policy. If the Company in the commercial or professional activity in the course of a transaction or in the performance of an official act interacts with the participating entity, with a customer, in whose respect an official action is carried out, or with a customer from a sanctioned third country, then any activity should be prohibited.

10.3. Sanctions are imposed by the EU, the United Nations and governments and include a range of financial or trading restrictions, such as freezes on the assets of and travel restrictions on nominated individuals, bans on financing of state-owned enterprises, prohibitions on the supply of technical, financial and other assistance and outright prohibitions on trade. In its business activities, the Company has due regard to relevant applicable sanction programs.

10.4. EU Sanctions

The EU imposes sanctions within the framework of the Common Foreign and Security Policy, either on an autonomous EU-basis, typically imposed through Council Regulations that have immediate legal effect in member states, or by implementing binding resolutions of the United Nations Security Council. Sanctions imposed by the EU may target governments of third countries or non-member state entities and individuals, such as terrorist groups and individual terrorists. The EU maintains and publishes lists of targeted countries, entities, groups or individuals (EU Sanctions Lists). New kind of sanctions may prohibit any type of financing or funding of entities under sanctions, including entities that are listed on regulated markets in the EU.

Sanctions requirements imposed by the EU have to be followed by all persons and entities doing business in the EU, including nationals of non-EU countries, and also by EU nationals AML and Sanctions policy Detailed requirements and entities incorporated or constituted under the law of an EU member state when doing business outside the EU.

For more information about these sanctions, see the following European Commission website: http://ec.europa.eu/external_relations/cfsp/sanctions/index_en.htm

10.5. US Sanctions

In the US, the Office of Foreign Asset Control of the US Treasury Department ("OFAC") administers and enforces US-based economic and trade sanctions programs against targeted foreign countries, terrorists, international narcotics traffickers and those engaged in activities related to the proliferation of weapons of mass destruction and other threats to the national security, foreign policy or economy of the US. These sanctions programs are based on US foreign policy and national security goals, as well as on United Nations and other international mandates.

OFAC also publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. Additionally, OFAC lists individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country specific. Collectively, such individuals and companies are called Specially Designated Nationals ("SDNs") (US Sanction lists). New kind of sanctions prohibit any type of financing or funding of entities under sanctions, including entities that are listed on regulated markets in the EU. OFAC maintains and publishes lists of these targeted countries, entities, groups or individuals, referred to generally as sanctions and SDNs lists. A US person is prohibited by OFAC from engaging in a wide range of transactions with any individual, group, entity or country on these lists. For more information about these sanctions, see the following US Treasury Department website: <http://www.ustreas.gov/offices/enforcement/ofac/>

10.6. UN Sanctions

The UN sanctions list is maintained by UN member states and organizations to eliminate terrorism, weapons proliferation, human rights violations, money laundering, deliberate destabilization of sovereign countries, and drug trafficking, etc. Depending on the situation, sanctions are applied to economic, cultural, trading, or diplomatic relationships with targeted countries.

The United Nations Security Council (UNSC) has primary responsibility for the maintenance of international peace and security. It has 15 members (5 permanent members with veto

powers—China, Russia, the US, France, and the UK—and 10 non-permanent members), and each member has one vote. Under the Charter of the United Nations, all member states are obligated to comply with Security Council decisions, including sanctions imposed by the body.

For more information about these sanctions see the following website:

<https://www.un.org/securitycouncil/sanctions/information>

10.7. UK Sanctions

Sanctions are restrictive measures that can be put in place to fulfil a range of purposes. In the UK, these include complying with UN and other international obligations, supporting foreign policy and national security objectives, as well as maintaining international peace and security, and preventing terrorism.

The UK implements a range of sanctions regimes through regulations made under the Sanctions and Anti-Money Laundering Act 2018 (the Sanctions Act). The Sanctions Act provides the main legal basis for the UK to impose, update and lift sanctions.

UK sanctions Regulations made under the Sanctions Act apply in the whole of the UK, including in Northern Ireland. The prohibitions and requirements in these Regulations apply to conduct by UK persons. This includes anyone in the UK (including its territorial waters), UK nationals outside of the UK, and bodies incorporated or constituted under the law of any part of the UK. It is government policy for UK sanctions measures to be given effect in the British Overseas Territories and Crown Dependencies to make sanctions as effective as possible.

HM Treasury implements and enforces financial sanctions, through its Office of Financial Sanctions Implementation (OFSI). OFSI helps to ensure that financial sanctions are properly understood, implemented and enforced in the UK.

Financial sanctions include restrictions on designated persons, such as freezing their financial assets, as well as wider restrictions on investment and financial services.

OFSI helps companies understand their financial sanctions obligations, monitors compliance and assesses suspected breaches. OFSI can also issue licences to allow for an activity that would otherwise be prohibited by financial sanctions regulations, under certain circumstances.

For more information about these sanctions, see the following OFSI website: <https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation>

10.8. The Company screens clients manually against sanctions lists and has due regard to any linkages with this every day. Such linkages will be considered as a risk factor in determining the appropriate level of customer due diligence to be applied and the Company will not undertake any business activities that are not allowed under sanctions.

SECTION 11. CLIENTS IDENTIFICATION

11.1. Clients' identification is a player verification procedure.

The main aim of it is to ensure that the holder of the account is the real person and the money going into the casino account is his own (and not a result of criminal activity). Also, it helps to

know for sure that withdrawals are headed towards legitimate bank account, owned by him and not anyone else. It is required if the player's deposits / payments have reached limits, also if the player's account is suspicious. The player must upload the documents by himself.

List of required documents:

- Photo of ID or passport.
- Photo or screenshot of the payment system.
- Photo or screenshot of the document confirming the current address (not older than 6 months old)
- Selfie with ID.
- Source of wealth/funds (bank statements, tax declaration, etc. not older than 6 months old)
- Selfie with a special note (example: Hello 'casino name') and/or other special conditions (blinking eye, head/hand turning etc.)

11.2. Screening - Sanctions & Politically Exposed Person: sanction lists typically contain those involved with organized crime, financial crime, and terrorism or are blocked for political reasons. The main aim of applying additional scrutiny to customers who are classed as a PEP is to mitigate the risk that the proceeds of bribery and corruption may be laundered, or are assets stripped from their country of origin. While screening the customer attention should be paid to the following:

- match by name and surname (need to consider features of transliteration of name and surname in different countries);
- date of birth (if available);
- gender (male/female);
- primary country;
- appearance.

11.3. Additionally, the obtained information must be checked in open sources (Internet search).

While searching for information in open sources, attention should be paid to the following:

- official sources (e.g. government bodies' websites - for the Minister of Finance this will be the website of the Ministry of Finance);
- social networks (Facebook, LinkedIn, Twitter, etc.);
- other sources, which can help to confirm the PEP status of the customer.

11.4. The decision of classifying a customer as PEP, their family member, or close associate should be based on available data, assessment of this data, rational and analytical thinking, logic, and available official guidelines.

11.5 Risk Assessment - based on geographic location (ID issuing country & residence) / Social Media presence and Other Online Footprints/ I.P (& efforts to mask I.P)

How to verify documents:

- Photo of ID document: all data (name, date of birth, citizenship) should be completely coincide with the data in Player's details tab. The document should be valid, the photo of the holder, date of birth, date of issue/expire are a must. For example, passport, ID, driver's license are suitable for identification.
- Photo or screenshot of the payment system: all data should be completely coincides with the data in Payment systems debts tab. Necessary data for cards - first 6 and last 4 digits, name of card holder (same as in Player's details tab), card validity period should be clearly seen. The player has the right to hide other data. Scanned copies are not accepted as PS verification.
- A photo or a screenshot of a document confirming the current address: the data (name, address + date of issue of the document) should be coincides with the data in Player's details tab. Acceptable documents: utility bill / bank statement / payment for mobile services. A photo of registration details in passport is acceptable for the players from the CIS. The document must be no older than 90 days (3 months).
- Selfie with ID: it should be visible the player holds the ID in his hands, a thorough check for editing / photoshop should be made. Optionally, a selfie with ID + a sheet of paper on which the name of the casino and the current date are written can be requested.
- Proof of wealth: a document confirming the welfare of the player. Refers to the origin of the entire net wealth (i.e. total assets). The information that should be obtained should give an indication as to the volume of wealth the player would reasonably be expected to have and provide a picture of how it was acquired. Such information is possible to gather using online footprints and proof by an Enhanced Source of Wealth Declaration.
- Proof of funds: a document confirming the flow of funds to the payment system. Easier to establish than source of wealth but this should not simply be restricted to knowing from which bank or financial institution the funds may have been received. The information obtained should be substantive, relevant and be able to establish the fund's origin and the method/circumstances under which the funds were acquired. Source of funds can be obtained by detailed bank statements showing debits and credits as deposits and remitted amounts and to which recipients.
- Screening - Sanctions & Politically Exposed Person: a sanction lists typically contain those involved with organised crime, financial crime, terrorism or are blocked due to political reasons. Transacting with persons or entities on the list can bring heavy fines and restrictions. The main aim of applying additional scrutiny to customers who are classed a PEP is to mitigate the risk that the proceeds of bribery and corruption may be laundered, or are assets stripped from their country of origin. While screening the customer in OFAC Sanction List Search, we must pay attention to the following: -match by name and surname

(need to consider features of transliteration of name and surname in different countries); date of birth (if available); -gender (male/female); -primary country; -appearance. Additionally, we must check the obtained information in open sources (Internet search). While searching information in open sources, we should pay attention to the: -official sources (e.g. government bodies' websites - for the Minister of Finance this will be the website of the Ministry of Finance); -social networks (Facebook, LinkedIn, Twitter, etc.); other sources, which can help to confirm PEP status of the customer. The decision of classifying a customer as PEP, their family member or close associate should be based on available data, assessment of this data, rational and analytical thinking, logic and available official guidelines.

- Risk Assessment - based on geographic location (ID issuing country & residence) / Social Media presence and Other Online Footprints/ I.P (& efforts to mask I.P): the information about the country where the document was issued and the player's place of residence is investigated. Some countries may be associated with an increased risk in the gambling industry or financial crimes. The purpose of having the ability to search for information on the Internet using various online footprints is to focus on adverse news or negative information that may be associated with the player, found across different news sources and social media platforms. Checking for adverse information can reveal links to money laundering, financial fraud, drug trafficking, financial threats, organized crime, financial terrorism, and other crimes. These links pose a serious threat to the reputation of organizations and can lead to legal consequences. Suspicious IPs are analysed during standard verification or any other investigation, particularly in cases where an account has been dormant or inactive for a significant period. The analysis focuses on examining the connections between IP addresses used to access the account and their frequent changes. If suspicious links are detected, such as unusual or unexpected combinations of IP addresses, it may indicate potential security breaches or unauthorized access to the account.

SECTION 12. CUSTOMER DUE DILIGENCE

The Company undertakes CDD measures in the following circumstances:

- Players engage in financial transactions equal to or exceeding NAf. 4,000.
- Players carry out occasional transactions exceeding the monetary equivalent of NAf. 4,000, whether as a single transaction or a series of related transactions.
- There is a suspicion of money laundering (ML) or terrorist financing (TF).
- The Company has doubts about the veracity or adequacy of previously obtained customer identification data.

12.1 CDD Measures to Be Taken

Identifying the Customer:

- Verify the customer's identity.

Identifying the Beneficial Owner:

- Take reasonable measures to verify the identity of the beneficial owner.

Understanding the Business Relationship:

- Obtain information on the purpose and intended nature of the business relationship.

Ongoing Due Diligence:

- Conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure transactions are consistent with the institution's knowledge of the customer, business, and risk profile, including, where necessary, the source of funds.

12.2 Timing of CDD Measures:

- CDD measures (1-3) must be completed at the time the NAf. 4,000 threshold is reached.
- Casinos are required to apply a minimum level of CDD measures when entering a business relationship (e.g., opening an account).
- At least personal details must be collected, and sanctions screening must be conducted when opening an account.
- Players may be allowed to use their gaming account while carrying out CDD measures. However, if the NAf. 4,000 threshold is reached, players are not allowed to deposit funds into or withdraw funds from the account.

Additional Measures:

- The threshold must be calculated on a daily basis, taking all deposits and withdrawals into account since the establishment of the business relationship, including peer-to-peer transfers.
- If documentation is not received within 30 days of reaching the threshold, the casino must terminate the business relationship and report the transaction to the Financial Intelligence Unit (FIU) if there is a presumption of ML.
- Conducting CDD at the earliest possible opportunity can limit situations in which ill-gotten funds are received.

12.3 Inability to Complete Customer Due Diligence (CDD)

In instances where the Company is unable to complete the required CDD measures, the following actions must be taken:

Account and Business Relationship Initiation:

- The casino operator must refrain from opening the account, commencing the business relationship, or performing the transaction if CDD requirements cannot be met.

Termination of Existing Business Relationships:

- If a business relationship is already established and the casino operator is unable to complete the necessary CDD measures, the operator must terminate the business relationship promptly.

Reporting Obligations:

- The Company is required to submit an unusual transaction report to the Financial Intelligence Unit (FIU) if there is a presumption of money laundering (ML), terrorist financing (TF), or proliferation financing (PF).

SECTION 13. ENHANCED CUSTOMER DUE DILIGENCE

In circumstances where the risk of money laundering (ML) or terrorist financing (TF) is heightened, enhanced Customer Due Diligence (CDD) measures must be implemented to mitigate the increased risk. Enhanced CDD is required in the following scenarios:

- Politically Exposed Persons (PEPs): This includes both international and domestic PEPs, who pose a higher risk due to their prominent public positions.
- New Technologies: Emerging technologies that may present increased risks due to their anonymity or potential misuse.
- Higher-Risk Countries: Transactions or relationships involving countries known for higher risks of ML or TF.
- Other Higher-Risk Situations: Any other situations that present a heightened risk of ML or TF.

13.1 Enhanced CDD Measures:

In high-risk situations, the Company operator should consider the following enhanced measures to effectively mitigate risk:

Additional Information Collection:

- Obtain further details about the player, such as occupation and volume of assets. This can be achieved through public databases, internet searches, and other available sources.

Frequent Data Updates:

- Regularly update the player's identification data to ensure its accuracy and relevance.

Source of Funds (SoF) and Source of Wealth (SoW):

- Gather information regarding the source of funds or source of wealth of the player to verify legitimacy.

Transaction Information:

- Obtain detailed information on the reasons for intended or performed transactions to assess their legitimacy.

Senior Management Approval:

- Secure approval from senior management before commencing or continuing the business relationship in high-risk cases.

Enhanced Monitoring:

- Conduct more rigorous monitoring of the business relationship by increasing the frequency and depth of controls and examining transaction patterns for unusual activity.

Initial Payment Requirement:

- Require that the first payment be made through an account in the player's name at a bank that adheres to similar CDD standards.

SECTION 14. SIMPLIFIED CUSTOMER DUE DILIGENCE

When the risk of money laundering (ML) or terrorist financing (TF) is assessed to be lower, simplified Customer Due Diligence (CDD) measures may be implemented. These measures are designed to reflect the lower risk and should be proportionate to the nature of the lower risk involved.

14.1 Simplified CDD Measures

In scenarios where simplified CDD is appropriate, the following measures may be considered:

Delayed Verification:

- Verify the identity of the player and the beneficial owner (BO) after the establishment of the business relationship, rather than before.

Reduced Frequency of Updates:

- Implement less frequent updates of customer identification data, recognizing the lower level of risk.

Minimized Ongoing Monitoring:

- Reduce the degree of ongoing monitoring and transaction scrutiny, based on a reasonable monetary threshold that reflects the lower risk profile.

Infer Purpose and Nature:

- Simplify the process of understanding the purpose and intended nature of the business relationship by inferring these aspects from the type of transactions or the nature of the established relationship, rather than requiring extensive specific information.

14.2 Limitations of Simplified CDD

Simplified CDD measures are not permissible in the following situations:

- Suspicion of ML or TF: Simplified measures cannot be applied if there is any suspicion of money laundering or terrorist financing.
- Higher-Risk Scenarios: Simplified CDD is not acceptable in higher-risk scenarios or where there are concerns related to heightened risk factors.

SECTION 15. REPORTING OF UNUSUAL TRANSACTIONS

The Company are required to report unusual transactions or intended transactions to the Financial Intelligence Unit (FIU) to support the prevention and detection of money laundering (ML) and terrorist financing (TF). The reporting procedure is essential for maintaining the integrity of financial operations and ensuring compliance with regulatory standards.

15.1. Definition of Unusual Transactions:

An unusual transaction is defined as a transaction or series of transactions that is inconsistent with the player's known profile. To determine whether a transaction is unusual, both objective and subjective indicators are used.

15.2. Objective Indicators:

Objective indicators of unusual transactions include:

- Transactions reported to police or judicial authorities.
- An intended transaction involving a natural or legal person listed on a UN or EU sanctions list.
- Transactions equal to or exceeding NAf. 5,000, including bank transactions, sales of chips or credits, and payments of prizes.
- Transactions where there is reason to assume possible connections to ML or TF.

15.3. Procedure for Reporting

Submission via goAML Portal:

- Reports must be submitted through the goAML portal at <https://portal.fiucuracao.cw>. Companies must register to gain access to this portal, and all reports should be submitted in English.

Reporting Timeline:

Objective Indicators:

- Reports of transactions that meet objective indicators must be submitted within 48 hours of the transaction occurring.

Subjective Indicators:

- Report internally to the Compliance Officer (CO) within 24 hours.
- The CO has 10 working days to conduct the relevant research.

FIU Reporting: If a presumption of ML or TF exists, the CO must report to the FIU within 48 hours.

Examples of Situations Possibly Related to ML or TF

- Betting Accounts: Setting up multiple betting accounts with deposits just below the reporting threshold, followed by rapid withdrawals.

- Cash Transactions: Regularly depositing or transacting similar amounts of cash, or funding accounts with credit/debit cards, prepaid cards, checks, and cryptocurrency and then requesting payouts.
- Inconsistent Income: Unexplained income that is inconsistent with the player's financial situation or profile.
- Machine Credits: Claiming machine credits or payouts without a corresponding jackpot.
- Multiple Accounts: Associating with multiple accounts under different names.
- Threshold Patterns: Frequent betting transactions or cash deposits/withdrawals just below the reporting threshold.
- Parallel Betting: Betting against associates or intentionally losing to facilitate the receipt of casino-issued checks or wire transfers of legitimate winnings.
- Currency Exchanges: Multiple or unusual currency exchanges, particularly those involving low denomination bills being exchanged for high denomination bills, or exchanges with minimal gambling activity.
- Wire Transfers: Frequent wire transfers or currency exchanges just below thresholds, or 'cash out' transactions without corresponding 'buy in' transactions.

SECTION 16. RECORD KEEPING

16.1. The Company must retain the following records and information for a period of five years after the end of a business relationship with a client or after the date an occasional transaction was completed:

(a) Copies and information for compliance with the Client Identification process covered in section 11.

(b) Evidence and records of transactions both domestic and international

(c) Correspondence documents with clients

(d) Suspicious Transaction Reports and/or Suspicious Activity Reports performed by staff members including the examination performed by the CO, the corresponding findings and any subsequent communication with FUI Curacao.

(e) Player risk profile

16.2. Records and information retained must be visible, legible and of sufficient content and quality, to permit reconstruction of transactions so as to provide, if needed, evidence for prosecution of criminal activity. It is highlighted that processes should be established, for the retrieval of records and information retained, which must be accessed timely and without due delays. In cases where it is reasonably justified, the Company should retain records and information for five additional years, bringing the total retention period to a maximum of ten years after the end of a business relationship with a client or after the date an occasional transaction was completed. Reasonable justification

refers to the prevention, detection and investigation of Money Laundering and Terrorist Financing in relation to ongoing criminal proceedings or suspicions.

SECTION 17. EMPLOYEE TRAINING

17.1. The Company ensures that its employees, agents or other individuals authorized to act on the Company behalf are adequately trained and informed about the requirements set out in the Company policies and procedures. The Company also ensures that the daily duties of its employees are executed in accordance with the Company regulations and technical instructions specified in the Company ANTI-MONEY LAUNDERING POLICY. Any employee, who violates ANTI-MONEY LAUNDERING POLICY regulatory documents or acts illegally in the course of performance of his/her duties, shall be subject to disciplinary sanctions and liability as provided for in the regulatory enactments of Curacao.

17.2. The Company establishes a system of tailored training for its employees (employees, who have contact with clients such as front-line staff or agents; employees who are involved in client transaction activities and handle client's funds; employees who are responsible for implementing or overseeing the compliance program (such as senior management, information technology staff or internal auditors), etc.) so that they understand their obligations under the Regulator, how the Company business or their particular profession could be vulnerable to ML/TPF activities, the Company compliance policies and procedures and their roles in detecting and deterring ML/TPF activities.

17.3. The training program shall include at a minimum:

- ML/TF concepts, definitions of ML/TF, why criminals choose to launder money and how the process for ML/TF usually works;
- the Company compliance policies and procedures for preventing and detecting ML/TF, including reporting, client identification, know-your-client, client due diligence and record keeping obligations;
- Responsibilities of the Company employees, agents or anyone else acting on the Company behalf when dealing with suspicious transactions.

17.4. Compliance training is comprised of two key elements:

Induction training – Compliance Officer is responsible for identifying relevant new staff that is required to undergo induction training within 30 days after commencement of employment relationship. The training is conducted by the AML and Compliance Department and/or Compliance Officer or the Compliance Officer may engage an external service provider. Until a new member of staff has been signed off as competent, no client servicing activities are allowed; Refresh training - all relevant staff must undergo refresh training on a semi-annual basis. The training is conducted by the AML and Compliance Department and/or Compliance Officer or the Compliance Officer may engage an external service provider. Testing of staff's knowledge is carried out after the training.

The company obtains acknowledgement from staff that they have received the necessary training by requesting staff to sign their attendance at training sessions. Overall monitoring of attendance and testing results are recorded manually and stored in an electronic form.

SECTION 18. RISK SCORING

18.1. The Company's assessment of customer risk marks each customer account as falling within a low, medium, high-risk, or very high-risk category.

As part of our risk assessment policy, we classify potential threats based on various characteristics and operational contexts.

Very High Risk is associated with activities involving unregulated virtual currency exchanges and corporate structures using bearer shares that ensure client anonymity. These risks are exacerbated when services are provided non-face-to-face through intermediaries.

High Risk is characteristic of non-profit organizations sending funds to high-risk jurisdictions, correspondent banks, and fiduciary arrangements. Risks increase with the use of internet-based products or services susceptible to high money laundering and terrorist financing risks, especially when transactions are conducted non-face-to-face with insufficient technological safeguards.

Medium Risk applies to highly paid employees, public figures, and the general public using retail products. This risk may be moderate, particularly when using technological systems with embedded safeguards in non-face-to-face transactions.

Low Risk is observed for pensioners and average-salaried employees using products with limited transaction or deposit thresholds, especially when transactions are conducted face-to-face.

Each risk category is also influenced by the country's rating, which considers the broader geopolitical and regulatory environment.

	A	B	C	D	E	F
1	Criteria	TYPE OF CUSTOMER	PRODUCT/SERVICE	IDENTIFICATION	COUNTRY RATING	
2	Choose one	Pensioners, Average-salaried employees	internet based products, Services or products identified as po	Face to face	Germany	Assigned Risk Rating
3	Rating	1	3	1	1	High
4						
5						
6						
7						
8						
9						
10						
11						

	A	B	C	D	E	F
	Criteria	TYPE OF CUSTOMER	PRODUCT/SERVICE	IDENTIFICATION	COUNTRY RATING	
	Choose one	Highly paid employees, Public figures, General public	Retail products	Face to face	Cyprus	Assigned Risk Rating
	Rating	2	2	1	1	Medium

SECTION 19. TRANSACTIONS AND ONGOING MONITORING

19.1. Below are the most common money laundering-related red flags the Company should watch out for:

- Unusual betting patterns with players placing large bets on low-risk games or frequently changing betting patterns.
- Frequent large transactions.
- Rapid deposit and withdrawal cycles with criminals depositing large sums to their accounts and withdrawing them quickly.
- Multiple accounts and IP addresses for conducting transactions

19.2. The Company is committed to implementing thorough Customer Due Diligence (CDD) processes for all transactions. This includes a comprehensive customer verification at the time of account creation, with the collection and validation of necessary identification documents. Transparent transaction records are maintained for each customer, detailing deposits, withdrawals, and gaming activities.

19.3. The Company applies enhanced customer due diligence measures and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks arising in the following cases:

- in any business relationship with a customer situated in a high-risk third country or in relation to any transaction in relation to which the operator is required to apply CDD measures, where either of the parties to the transaction is resident in a high-risk third country
- if the operator 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 operator discovers that a customer has provided false or stolen identification documentation or information and the operator 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
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.

19.4. In the case of business relationships with customers situated in high-risk third countries or transactions where either of the parties to the transaction are resident in a high-risk third country, the enhanced measures undertaken must include:

- obtaining additional information on the customer
- obtaining information on the source of funds and source of wealth of the customer
- obtaining information on the reasons for the transactions

- conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

19.5. In the case of transactions that are complex or unusually large, or where there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose, the enhanced measures undertaken must include:

- as far as reasonably possible, examining the background and purpose of the transaction
- increasing the degree and nature of monitoring of the business relationship in which the transaction is made, to determine whether the transaction or relationship appear to be suspicious.

19.6. Depending on the requirements of the case, the enhanced measures undertaken in any case may also include, among other things:

- seeking additional independent, reliable sources to verify information provided or made available to the casino operator
- taking additional measures to understand better the background, ownership and financial situation of the customer
- taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship

19.7. When assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, and the extent of the measures which should be taken to manage and mitigate the risk, the Company takes account of the following risk factors, among other things, whether:

- the business relationship is conducted in unusual circumstances
- the customer is resident in a geographical area of high risk
- payments will be received from unknown or unassociated third parties of the customer

19.8. In addition whether the business relationship or transaction involves countries:

- identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing
- identified by credible sources as having significant levels of corruption or other criminal activity, such as money laundering, terrorism, and the production and supply of illicit drugs
- subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations
- providing funding or support for terrorism

19.9. Understanding player behavior is integral to effective ongoing monitoring. The Company utilizes behavioral analytics to establish baseline patterns for individual players and detect deviations that may indicate suspicious activities. By considering factors such as playing habits, deposit and

withdrawal frequency, and gaming preferences, unusual trends can be identified and trigger investigations where necessary. Behavioral analytics serve as a method in staying ahead of potential risks associated with money laundering or other illicit activities.

19.10. To further enhance ongoing monitoring, the Company has established predefined thresholds for various transactional parameters. Any transactions or account activities surpassing these thresholds trigger immediate alerts for review. This proactive approach allows to focus attention on high-risk activities promptly, mitigating the potential for financial crimes. Regular reviews of these thresholds are conducted to adapt to changes in the gaming landscape and to ensure that our monitoring efforts remain effective.

19.11. The Company proceeds with the ODD of clients on the following basis:

- Once per month for a High-Risk client and a Very High-Risk client.
- Once per 6 months for a Medium-risk client.
- Once per year for a Low-risk client



Established and signed on the 05 of September 2024

TETIANA BOIKO,
Executive Director of CUPWIN B.V.

List of countries No.1 (countries against which the United Nations, the United States, the UK or the European Union have imposed financial or civil restrictions) for the geographic risk assessment of the Client, the Client's UBO and the Client's partners

No.	Country code	Country
1	AF	Afghanistan
2	BA	Bosnia and Herzegovina
3	BI	Burundi
4	BY	Belarus
5	CD	Democratic Republic of Congo
6	CF	Central African Republic (CAR)
7	CU	Cuba
8	TN	Tunisia
9	NI	Nicaragua
10	GN	Republic of Guinea
11	GW	Guinea-Bissau Republic
12	IQ	Iraq
13	IR	Iran
14	KP	Democratic People's Republic of Korea (North Korea)
15	LB	Lebanon
16	LR	Liberia
17	LY	Libya
18	ML	Mali
19	RU	The Russian Federation

20	SD	Sudan
21	SO	Somalia
22	SS	South Sudan
23	SY	Syria
24	VE	Republic of Venezuela
25	YE	Yemen
26	ZW	Zimbabwe
27	MM	Myanmar (Burma)
28	TR	Turkey
29	CN	China