

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY

Version:	2.0.
Date of version:	25.03.2025
Created by:	Yevhenii Pyroh
Approved by:	Andrii Zabiaka
Confidentiality level	Confidential

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

Table of Contents

Introduction	3
1. Risk-Based Approach (RBA)	4
1.1. Business Risk Assessment (BRA)	4
1.2. Customer Risk Assessment (CRA)	4
1.3. Policies, Procedures, and Controls	7
2. Customer Due Diligence (CDD)	9
2.1. Identification and Verification of Identity	10
2.2. Basic CDD Measures	11
2.2.1. Understanding the Business Relationship	11
2.2.2. Thresholds and Triggers for CDD	11
2.2.3. Ongoing Monitoring	12
2.3. Specific CDD Measures for Different Risk Levels	12
2.3.1. Simplified Due Diligence (SDD) for Low-Risk Customers	12
2.3.2. Standard Due Diligence (CDD) for Medium-Risk Customers	13
2.3.3. Enhanced Due Diligence (EDD) for High-Risk Customers	13
3. Record Keeping and Documentation	15
4. Inability to Complete CDD	16
5. Ongoing Monitoring and Review	17
6. Reporting of Unusual Transactions	18
7. PEP and Sanctions Screening	20
7.1. PEP Management	20
7.2. Screening Process	21
7.3. Ongoing Sanctions Screening	21
8. Record-Keeping	23
9. Compliance Officer	24
10. Employee Training and Awareness	25
11. Contact Information	26

HIGHBET B. V.

Abraham Mendez, Chumacciro Blvd. 03, Willemstad, Curacao

Introduction

This Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) policy is designed to ensure that Highbet B.V. (hereinafter referred to as "the Company") complies with all legal obligations under the AML/CTF regulations in Curacao. The policy outlines the strategies, measures, and procedures implemented by the Company to detect, prevent, and report any activities related to money laundering, terrorist financing, and other financial crimes on baocasino.com ('the Website'). The policy is reviewed annually and whenever significant changes in the business or regulatory environment occur.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

1. Risk-Based Approach (RBA)

The Company adopts a comprehensive Risk-Based Approach (RBA) to identify, assess, and mitigate risks associated with money laundering (ML) and terrorist financing (TF). This approach is integral to ensuring that resources are allocated efficiently, focusing on areas where risks are higher.

In order to work risk-based, the Company continuously follows the latest developments regarding money laundering and terrorist financing.

The RBA includes the following components:

1.1. Business Risk Assessment (BRA)

The Business Risk Assessment (BRA) is conducted to evaluate the overall risk exposure of the Company's operations. The Company revises its business risk assessment whenever there are changes to the environment within which the Company is operating and within its business activities, such as introduction of new payment methods, new markets, new games or regulatory changes. In the absence of changes, the Company assesses its business risk at least once a year, to evaluate whether any changes thereto are necessary.

This risk assessment has to be documented and approved by the Board of directors of the Company. It should also be made available to the GCB upon request.

This assessment considers, including but not limited to, such factors as:

- customer demographics, including their financial history, source of wealth, and geographic location;
- the nature and complexity of the Company's products and services, including online gaming and transaction processing;
- the channels through which the Company engages with customers, particularly non-face-to-face transactions that might increase the risk of ML/TF;
- the regulatory environment in which the Company operates, including local and international AML/CTF requirements.

The BRA is reviewed annually or whenever there are significant changes in the business environment, such as the introduction of new products, expansion into new markets, or changes in regulatory requirements.

This risk assessment has to be documented and approved by the Board of directors of the casino. All aspects of the Business Risk Assessment should be covered, including:

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

1.2. Customer Risk Assessment (CRA)

The Customer Risk Assessment (CRA) process is designed to evaluate the risk profile of each customer. This assessment is conducted either prior to carrying out an occasional transaction or during the customer

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

onboarding process (establishing business relationships) and is regularly updated throughout the business relationship. Customers are assessed based on various risk factors, including but not limited to:

- **Geographic Location:** The geographical risk is the risk posed to the Company by the geographical location of the player and the source of wealth of the business relationship. The nationality, residence and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered as high risk. Customers from high-risk jurisdictions, as identified by FATF or other regulatory bodies, are subject to enhanced scrutiny. The company also takes into account a variety of sources of information produced by the FATF and non-governmental well-known bodies, including but not limited to:
 - countries on the FATF list of High-Risk Jurisdictions subject to a Call for Action;
 - countries on the FATF list of Jurisdictions under Increased Monitoring;
 - countries on the CFATF Public Statement;
 - countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
 - countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
 - countries sanctioned by the OFAC;
 - countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
 - countries on the Corruption Perception Index compiled by Transparency International.
- **Customer Profile:** Consider factors such as the nature of the customer's business, occupation, source of wealth, and source of funds. Categories of customers whose activities may indicate a higher risk include:
 - customers who have multiple sources of income;
 - customers with irregular income streams;
 - PEPs;
 - high spenders (money can be derived from illegal activities);
 - disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
 - casual customers like locals/tourists, especially when spending pattern changes;
 - improper use of third parties, criminals use third parties to gamble and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
 - customers using multiple casino player rating accounts to hinder a casino to track their gambling activities;
 - unknown customers (redeeming large amounts of chips);

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

- junkets (junket operators monitor player activity and issues and collect credit).
- **Product, service and transaction risk:** Unusually large or complex transactions, patterns that deviate from the norm, or transactions with no apparent economic or lawful purpose. A higher risk of ML/FT presents the use by customer of the following payment methods (including but not limited to):
 - proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
 - cash. Land-based casinos (or physical establishments of online casinos) are used to exchange large amounts of illicit proceeds in small denominations for larger ones;
 - anonymous payment methods such as pre-paid cards and virtual assets;
 - use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
 - types of specific games (e.g. roulette, craps -> even bets);
 - peer to peer gaming;
 - the use by customer of accounts held or cards issued in the name of third parties;
 - the transfer of funds from one gaming account to another;
 - types of financial services (credit/marker, currency exchange, check cashing);
 - multiple casino accounts or wallets (internet operator may own and control multiple web sites);
 - changes to financial institution accounts to fund casino account;
 - identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
 - using cash to fund a pre-paid card poses similar risks as cash;
 - games involving multiple operators (Poker on platforms shared by multiple operators);
 - electronic wallets (e-wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling.
- **Relationship with Politically Exposed Persons (PEPs):** Customers who are PEPs or have close associations with PEPs are automatically considered higher risk.
- **Distribution channels risk.** The channels through which a casino establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction:
 - channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

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

Based on the risk factors, customers are categorized into the following risk levels:

- **Low Risk:** Customers with minimal risk of money laundering or terrorist financing. These customers may include individuals with a transparent and verified source of income from low-risk countries.
- **Medium Risk:** Customers with moderate risk, typically those with complex financial activities or connections to jurisdictions with some AML/CFT deficiencies.
- **High Risk:** Customers who pose a significant risk, such as those involved in high-risk industries, with opaque ownership structures, or from high-risk jurisdictions. High-risk customers also include those with large, complex transactions or relationships with PEPs.

Criteria of defining a higher risk are described above.

The company should maintain appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. It should identify and assess the money laundering or terrorist financing risks that may arise whenever:

- a new product is developed;
- a new business practice emerges;
- a new delivery mechanism becomes available;
- a new or developing technology is used for both new and pre-existing products.

In such cases, a risk assessment should take place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. Such risk assessments must be documented. Where risks are identified, measures must be taken to mitigate these risks.

1.3. Policies, Procedures, and Controls

The Company established and maintains policies, procedures and controls to mitigate and manage effectively the risks identified in the operator's risk assessment of money laundering, terrorist financing and proliferation of weapons. The measures, policies, controls and procedures to mitigate ML/FT/FP risk include:

- Customer Due Diligence (CDD);
- Record keeping procedures;
- Reporting procedures;

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

- Risk management measures including Customer Acceptance Policies (CAP), Customer Risk Assessment (CRA) procedures, internal control, compliance management and communications of such policies, procedures and controls, employee training and employee screening policies and procedures.

These measures are clearly documented and approved by the Board of directors. The Company monitors the implementation of these controls and enhances them if necessary. The Company takes enhanced measures to manage and mitigate the risks where higher risks are identified.

The Company clearly expresses the Company's senior management's commitment to combat the abuse of its facilities, products and services for the purpose of money laundering, terrorist financing and the proliferation of weapons of mass destruction purposes. The Company strongly intends to comply with current anti-money laundering, combating the financing of terrorism and financing of proliferation legislation as well as regulations, in particular the laws and regulations regarding customer due diligence, the reporting of unusual transactions and keeping adequate records of clients and transactions (NOIS, NORUT, Sanctions National Ordinance, Kingdom Sanction Act).

The anti-money laundering policies and procedures have been made in writing and have been approved by the Company's senior management. The Company's policies and procedures have been duly communicated to its employees.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

2. Customer Due Diligence (CDD)

Customer Due Diligence (CDD) is a critical component of the Company's AML/CTF framework, ensuring that the identity of each customer is verified and that their activities are consistent with their risk profile.

CDD measures are applied in the following scenarios:

- when players engage in financial transactions of 4,000 Naf (or equivalent in EUR, USD, or other currencies, available on the web-site) or more, either as a single transaction or as a series of related transactions;
- when there is suspicion of money laundering (ML) or terrorist financing (TF);
- when there are doubts about the accuracy or adequacy of previously obtained customer identification data;
- when establishing a new business relationship or opening an account for a customer.

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, its source of funds.

Basic CDD measures involve the collection and verification of the following customer information:

- full legal name, permanent residential address, date of birth, and nationality;
- verification of identity through government-issued documents such as a passport, national ID, or driver's license;
- verification of the customer's residential address using utility bills, bank statements, or other official documents not older than six months;
- confirmation of the customer's source of funds and source of wealth, particularly in cases where large or frequent transactions are involved;
- screening against global sanctions lists and Politically Exposed Persons (PEP) databases before establishing a business relationship.

The CDD process involves several key steps to ensure that the company accurately identifies and understands its customers. These measures vary depending on the risk classification of the customer. At that, the Company is prohibited to disclose the fact that an unusual transactions report is being reported to the FIU. If the Company has a suspicion that transactions relate to money laundering or terrorism funding,

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

it should take into account the risk of tipping-off when performing the CDD process. If the Company reasonably believes that performing the CDD process will tip-off the player, it may choose not to pursue that process, and should file an unusual transaction report to the FIU.

2.1. Identification and Verification of Identity

The first step in the CDD process is the identification and verification of the customer's identity. This includes collecting personal details and verifying them using reliable, independent sources.

Required Information:

- full name;
- date of birth;
- place of birth;
- nationality;
- permanent residential address;
- government-issued identification number (e.g., passport, ID card, driver's license).

Verification Methods:

- unexpired government-issued documents with photographic evidence (e.g., passport, national ID card);
- verification of residential address using documents not older than 6 months (e.g., utility bill, bank statement, letter from a public authority or rental agreement);
- use of technological measures such as geo-location data, IP address information, and biometric checks to verify the identity of online customers.

The Company can also contact the player by letter, e-mail or telephone to verify the information supplied. It can also send a verification code to the e-mail address to verify that the address is current and genuine. Verification can also be done by checking social media, telephone directories, companies registries or media and news sources. Biometric checks can also be used to confirm that the individual providing the document is the one described therein. In some circumstances the Company is able to cross reference the information in its possession with geo-location information, IP address data, funding method data etc.

All players should be screened against sanctions lists of the OFAC, UN and EU. If Curaçao publishes a local list with designated persons and organizations, the casino should also take that local list into account.

The casino must ensure it does not do business with customers that are subject to international sanctions. Before doing business or performing an occasional transaction for the first time with a player, the casino should check published lists of known or suspected terrorists or other sanctioned persons or companies.

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

When the Company does not have sufficient comfort that it knows its player, the Company takes additional measures to do so, such as requesting additional identification documents, asking the player to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction,

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

In case of business participants the Company must obtain satisfactory evidence to identify these business participants. It has to take reasonable steps to verify the identity of the beneficial owner, using information or data that was obtained from a reliable source. At the minimum identification information, verification and evidence must be gathered for all persons holding 25% or more of the shares or voting rights or a person who otherwise exercises ultimate effective control of the customer. Where no natural person is identified as mentioned above, the natural person who holds the position of senior managing official should be identified.

2.2. Basic CDD Measures

2.2.1. Understanding the Business Relationship

The company must obtain sufficient information to understand the nature and purpose of the business relationship. This includes gathering information on the customer's source of wealth, source of funds, and the intended use of the company's services.

For low-risk customers, an ID and proof of residential address will suffice, in some cases source of funds might be requested.

For medium- and high-risk customers, additional documentation may be required to verify the source of wealth and the purpose of transactions. This may include income statements, business documents, or publicly available information.

2.2.2. Thresholds and Triggers for CDD

The Company undertakes Customer Due Diligence measures when:

- players engage in financial transactions equal to or above Naf. 4,000;
- carrying out occasional transactions² above the monetary equivalent of Naf. 4,000³;
- there is a suspicion of money laundering or terrorist financing; or
- the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

In case the Company carries out an occasional transaction above the monetary equivalent of NAF. 4,000, it applies CDD measures. The Company also applies CDD measures when it executes a series of linked transactions which, though individually below the applicable threshold, would cumulatively meet or exceed the NAF. 4,000 threshold. Transactions are considered as linked if, for example, they are carried out by the same player through the same game or in one gaming session. In this context, the Company has to identify the player, carry out a customer risk assessment and verify the identity of the player.

Whenever an occasional transaction presents a high risk of ML/TF, the enhanced due diligence measures applies.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

2.2.3. Ongoing Monitoring

Ongoing monitoring is a critical component of the CDD process. The company must continuously monitor customer transactions to ensure they are consistent with the customer's profile and risk level.

Transaction Monitoring:

- the company must scrutinize transactions to identify unusual or suspicious activity, including transactions that deviate from the customer's normal behavior;
- all accounts held by the customer with the company must be linked to detect patterns such as the use of third-party identities or multiple accounts.

Updating Information:

- the company must ensure that all customer information, including identification documents and risk assessments, is kept up-to-date. This includes obtaining new documents when existing ones expire and reviewing the customer's risk profile regularly.

2.3. Specific CDD Measures for Different Risk Levels

The level of CDD applied varies depending on the customer's risk classification. The following outlines the specific measures for low, medium, and high-risk customers.

2.3.1. Simplified Due Diligence (SDD) for Low-Risk Customers

Simplified Due Diligence may be applied to customers who pose a low risk of money laundering or terrorist financing. In these cases, the extent of the CDD measures may be reduced, taking into account the lower risk involved. Simplified Due Diligence measures are:

- identification and verification of the customer's identity may occur after the establishment of the business relationship;
- the frequency of customer identification updates and ongoing monitoring may be reduced, provided there are no signs of increased risk;
- the purpose and intended nature of the business relationship may be inferred from the type of transactions or relationship established.

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.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

2.3.2. Standard Due Diligence (CDD) for Medium-Risk Customers

Standard Due Diligence is applied to customers who present a moderate risk. This involves a thorough collection and verification of customer information, as well as regular monitoring. Standard Due Diligence measures are:

- identification and verification of identity, address, and financial background through reliable sources, with a focus on consistency between the customer's profile and their activities;
- regular updates to customer information and risk assessments, with additional scrutiny if changes in behavior or risk profile are detected;
- enhanced monitoring of transactions, including real-time alerts for unusual or suspicious activities.

2.3.3. Enhanced Due Diligence (EDD) for High-Risk Customers

Enhanced Due Diligence is required for customers who pose a high risk of money laundering, terrorist financing, or other illicit activities. This includes customers including but not limited to Politically Exposed Persons (PEPs), those from high-risk jurisdictions, and customers with complex financial structures. This concerns also new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Enhanced Due Diligence measures include but 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. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- 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.

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

2.3.4. Timing of CDD Measures

As indicated in par. 2.2.2. hereof, the verification of identity has to be conducted when engaging in financial transactions equal to or in excess of Naf. 4,000. This implies that all CDD measures must have been conducted at the time the threshold is reached. However, the Company applies a minimum level of CDD measures prior to reaching the threshold. Thus, simultaneously with the opening of an account, the Company identifies the customer by collecting the minimum personal details, being: name and surname,

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

permanent residential address and date of birth (set as the minimum requirements in case of low risk business relationships) and conducts the PEP status screening and sanctions screening.

The threshold is to be calculated on a daily basis taking into account all deposits and withdrawals made by the player since the establishment of the business relationship, including any peer-to-peer transfers. Once the threshold is reached, the Company carries out a customer risk assessment and meets its remaining CDD obligations.

In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the Company obtains any necessary information from the customer concerned. However, if the Naf. 4,000 threshold is reached because of a deposit of the player, he cannot further deposit funds into the account or withdraw funds from the account. He still will be able to play, using the funds already in his account. However, if the Naf. 4,000 threshold is reached because the customer wants to withdraw his money, a complete freezing of the account occurs. In this case it will not be possible for the customer to continue playing.

Besides that, if the requested information and documentation is not received within 30 days from the moment the Naf. 4,000 threshold was reached, the Company terminates the relationship with the player and reports the transaction to the FIU if a presumption of money laundering or terrorist financing exists. If no presumption of money laundering exists, the funds should be transferred to the same bank account or wallet it was deposited from. If presumption of money laundering or terrorist financing exists, internal procedures should indicate whether the funds are blocked or not. Consideration should be given to the fact that by blocking the account, the customer may be tipped off.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

3. CDD-Related Record Keeping and Documentation

All records related to the CDD process, including identification documents, risk assessments, transaction records, and reports, must be maintained for at least five years after the business relationship ends. These records must be stored securely and be easily accessible for inspection by regulatory authorities.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

4. Inability to Complete CDD

If the company is unable to complete the CDD process due to the customer's failure to provide the necessary information, the company must take the following actions:

- the business relationship should not be established or, if already established, must be terminated;
- any ongoing transactions should be halted, and funds should not be accepted or withdrawn;
- if there is a suspicion of money laundering or terrorist financing, the transaction must be reported to the Financial Intelligence Unit (FIU) as an unusual transaction.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

5. Ongoing Monitoring and Review

The Company conducts ongoing monitoring of customer transactions and activities to detect any inconsistencies with the customer's risk profile or potential indicators of ML/TF. This includes:

- real-time transaction monitoring systems that flag unusual or suspicious activities for further investigation. Regular updates to customer information, particularly when there are changes in the customer's circumstances, such as a new address or change in employment;
- periodic reviews of customer accounts based on their risk level, ensuring that the level of scrutiny matches the current risk assessment;
- immediate action, including the potential freezing of accounts, if suspicious activities are detected. All such actions are documented and reported in accordance with the Company's reporting procedures.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

6. Reporting of Unusual Transactions

The following transactions or intended transactions are deemed unusual:

- transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance of Curacao;
- transactions in the amount of NAf. 5,000 (or equivalent in EUR, USD, or other currencies, available on the web-site) or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means. This includes but is not limited to:
 - ✓ a cashless transaction in the amount of NAf. 5,000 (or equivalent in EUR, USD, or other currencies, available on the web-site) or more. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client;
 - ✓ accepting or releasing a deposit in the amount of NAf. 5,000 (or equivalent in EUR, USD, or other currencies, available on the web-site) or more at the request of the client;
 - ✓ sale to a customer of chips in the amount of NAf. 5,000 (or equivalent in EUR, USD, or other currencies, available on the web-site) or more. "Chips" include but is not limited to tokens and credits;
 - ✓ a cash out in the amount of NAf. 5,000 (or equivalent in EUR, USD, or other currencies, available on the web-site) or more;
 - ✓ presumed money laundering transactions or terrorist financing.

It shall be noted that a transaction may be a single transaction, but may also be a series, combination or patterns of transactions involving a total amount of the monetary equivalent of NAf. 5,000 (or equivalent in EUR, USD, or other currencies, available on the web-site) or more and is considered per gaming day.

The Company has established a robust reporting mechanism for unusual transactions, ensuring that all suspicious activities are promptly reported to the Financial Intelligence Unit (FIU) of Curacao. The reporting process includes:

- a clear internal reporting structure where employees escalate suspicious activities to the Compliance Officer without delay;
- the use of the goAML portal for external reporting to the FIU, including detailed reports of the transaction, customer information, and supporting documentation;
- a strict non-disclosure policy that prohibits informing customers or third parties about the filing of a report or the investigation of their activities;
- a compliance audit trail that ensures all reports are documented, and any decisions not to report a transaction are justified and recorded by senior management.

Reporting on player transactions shall include at least the total amount, the nature of credits and debits to each gaming account, as well as, where applicable, the nature of the payment instrument used thereby,

HIGHBET B. V.

Abraham Mendez, Chumacciro Blvd. 03, Willemstad, Curacao

and, where applicable, a unique indication, not directly traceable to the identity of the player, of the debited and credited payment account per registered domain name or software applications.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

7. PEP and Sanctions Screening

The Company conducts rigorous sanctions screening of all customers and transactions against relevant global sanctions lists, including those issued by the OFAC, United Nations, European Union, and the local Curacao authorities. Sanctions screening is performed:

- during the onboarding process, before any transactions are processed;
- on an ongoing basis, particularly when updates to sanctions lists are released;
- automatically through integrated systems that alert the Compliance Officer if a customer or transaction matches a sanctioned entity.

The Company takes immediate action to freeze assets and block transactions involving sanctioned individuals or entities, in compliance with the applicable laws.

7.1. PEP Management

PEPs (Politically Exposed Persons) pose heightened risks due to their potential access to public funds or involvement in corruption. The following steps are applied to PEPs:

- **Identification:** PEPs are identified via specialized screening tools at onboarding. Ongoing monitoring is applied throughout the relationship.
- **Escalation:** Any PEP is escalated to senior management for review. Approval from senior management is required before a relationship is established.
- **Ongoing Monitoring:** PEP accounts are subject to continuous monitoring, with annual reviews to assess ongoing risks.

In relation to foreign politically exposed persons (PEPs) in addition to performing normal customer due diligence measures, the Company:

- has appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- obtains senior management approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship for existing customers or for conducting the occasional transaction). The approval can also be from the manager of the Compliance department;
- takes reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the player's spending pattern matches his legal source of funds. The Company requests a statement from the player about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources. When public sources cannot, or can insufficiently verify the received information, the casino can request the customer to provide documents; and
- conducts enhanced ongoing monitoring of the business relationship.

The Company takes reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

Although stricter customer due diligence is required for each PEP, this customer due diligence does not have to be the same for every PEP. The measures are tailored to the risk of the PEP, where the following is 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.

This means that the measures taken can be tailored by the Company to the risks in a specific case.

The requirements for all types of PEP should also be applied by the Company to family members or close associates of such PEPs.

Screening for PEP status has to be carried out before establishing the business relationship or conducting the occasional transaction. In addition, the Company must regularly screen for PEP status during the business relationship. Should a player who had not been identified as a PEP at on-boarding stage result to have become one, the Company is required to implement the measures described above within the 30 (thirty) day window of observing that the person is a PEP. Failing with these, shall result in termination of business relationship with this customer.

7.2. Screening Process

As part of our commitment to maintaining the highest standards of compliance with international laws and regulations, all customers, including individuals, entities, and associated third parties, shall be subjected to screening before doing business or performing occasional transaction and periodically throughout the business relationship.

Customers will be screened against multiple sanctions lists, including but not limited to:

- the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury;
- the United Nations (UN) Consolidated Sanctions List;
- the European Union (EU) Sanctions List;
- national sanctions lists, issued by the relevant regulatory authorities in the countries of the customer's residence or operation;
- Interpol databases;
- Europol watchlists;
- National Security Councils' lists of various countries, to identify whether the customer poses potential risks to national security of such countries.

7.3. Ongoing Sanctions Screening

Sanctions lists are updated frequently, and the company ensures that all customers are regularly rescreened against these updated lists. Automated monitoring tools shall be employed by the Company to flag any new sanctions or security alerts that may impact existing customers, prompting immediate review and investigation by the compliance team.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

In case of a match or "red flag" during screening or ongoing monitoring, the case will be escalated to the Compliance Department for further investigation. No business activity shall proceed until the issue has been thoroughly reviewed and cleared by the relevant internal teams.

If the customer's screening result mistakenly identifies them as a match to a sanctions list or security database (a "false positive"), the Compliance Officer will personally review the case to verify whether the match is incorrect.

Confirmed sanctions matches lead to immediate account suspension and notification to authorities.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

8. Record-Keeping

The Company adheres to strict record-keeping requirements as mandated by AML/CTF regulations. The following records are maintained for a minimum of five years after the termination of the business relationship or the date of the transaction:

- customer identification documents, including copies of passports, ID cards, and utility bills;
- detailed records of transactions, including the amounts, dates, and parties involved, ensuring that individual transactions can be reconstructed if required by authorities;
- internal and external reports of unusual transactions, including the rationale for reporting or not reporting a transaction;
- documentation of all risk assessments, due diligence measures, and ongoing monitoring activities.

These records are stored securely and are accessible only to authorized personnel. The Company ensures that records are available to competent authorities upon request.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

9. Compliance Officer

The Company has appointed a Compliance Officer who is responsible for overseeing the implementation of the AML/CTF policy and ensuring compliance with all regulatory requirements. The Compliance Officer's responsibilities include:

- 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 design an internal procedure about when reporting of unusual transactions will lead to blocking/freezing of user accounts, taking into account the risk of tipping off the player;
- 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.

HIGHBET B. V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

10. Employee Training and Awareness

The Company recognizes that the effectiveness of its AML/CTF measures depends on the awareness and vigilance of its employees. As such, the Company has implemented a comprehensive training program that includes:

- initial training for all new employees on the Company's AML/CTF policies, including their role in preventing and detecting ML/TF activities;
- ongoing training to ensure that employees are kept up to date with changes in AML/CTF regulations, emerging risks, and best practices;
- specialized training for employees in high-risk roles, such as those responsible for customer onboarding, transaction monitoring, and reporting;
- testing and certification to ensure that employees have a thorough understanding of the Company's AML/CTF procedures and their responsibilities.

The Company also promotes a culture of compliance by encouraging employees to report any concerns or suspicions related to ML/TF, without fear of retaliation.

To demonstrate compliance with aforementioned staff training guidelines, the Company maintains records that include:

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

HIGHBET B.V.

Abraham Mendez, Chumaceiro Blvd. 03, Willemstad, Curacao

11. Contact Information

If you have any questions or need further information regarding this Policy, please do not hesitate to contact us. We are committed to ensuring clarity and transparency in all our dealings and are here to assist you with any concerns.

Contact Information:

To: Compliance Team

Email: compliance@highbet.tech

For prompt assistance, please include your name, contact details, and a brief description of your inquiry. Our compliance team will respond to your query as soon as possible.

Director



Andrii Zablaka

