INTERNAL AML POLICY OF ONLINE BETTING COMPANY/ONLINE CASINO

of POINDER B.V. - revision #3 dated 09.09.2024

SECTION 1. INTRODUCTION

1.1. POINDER B.V. registration number 166111, a company organized and existing under the laws of Curacao, whose registered office is at Abraham Mendez Chumaceiro Boulevard 03, 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 (I) 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