(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 09 of September 2024

Agnesa Kleine,
Executive Director of POINDER B.V.

Annex No.1

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