

Anti-Money Laundering Policy & Procedures
Lone Rock Holdings N.V.

Table of Contents

DEFINITIONS & ABBREVIATIONS	3
VERSION CONTROL	4
1. INTRODUCTION	5
2. APPLICABILITY	5
3. SCOPE & PURPOSE	7
3.1. BUSINESS RISK ASSESSMENT (MACRO)	7
3.2. CUSTOMER DUE DILIGENCE (CDD)	8
3.2.1 <i>Identification and Verification of the Customer</i>	8
3.2.2 <i>Identification and Verification of the Beneficial Owner</i>	13
3.2.3 <i>Obtaining Information on the Purpose and Intended Nature of the Business Relationship</i>	13
3.2.4 <i>On-Going Monitoring</i>	14
3.3. APPLICATION, EXTENT & TIMING OF CDD MEASURES	16
3.4. POLITICALLY EXPOSED PERSONS (PEPs) & SANCTIONS	17
3.5. APPLICATION OF CDD MEASURES TO EXISTING CUSTOMERS	19
3.6. INABILITY TO COMPLETE CDD MEASURES	20
4. THE MONEY LAUNDERING REPORTING OFFICER (MLRO)	21
5. REPORTING SUSPICIOUS ACTIVITY & TRANSACTIONS	23
5.1. DEFINITIONS	23
5.2. RED FLAGS	23
5.3. REPORTING	25
5.4. TIPPING OFF	27
6. DATA RETENTION	28
6.1 PURPOSE OF DATA RETENTION	28
6.2 RETENTION PERIOD	28
6.3 SECURE STORAGE AND DISPOSAL	28
6.4 REVIEW AND UPDATES	28
7. TRAINING & AWARENESS	29
7.1 TRAINING CONTENT	29
7.2 ROLE-BASED TRAINING	29
7.3 REGULAR TRAINING SESSIONS	29
Matters to Note:	30
FIG. 1 - CUSTOMER DUE DILIGENCE OBLIGATIONS	32
FIG 2 – RISK ASSESSMENT	33

Definitions & Abbreviations

AML: Anti-Money Laundering

AMLPP: Anti-Money Laundering Policies and Procedures

Client(s): being an individual or corporate entity applying for an account/service/product from/with BetInAsia

Company: Lone Rock Holdings N.V.

CTF: Counter Terrorist Financing

EDD: Enhanced due diligence

EEA: European Economic Area

EMI: Electronic Money Institution

EU: European Union

FATF: Financial Action Task Force

FIU: Financial Intelligence Unit - Curacao

HMT: Her Majesty Treasury Sanction List

KYC: Know Your Client

ML: Money-Laundering

MLRO: Money Laundering Reporting Officer

OFAC: Office of Foreign Assets Control

PSP: Payment Service Provider

RF: Red Flag

RO: Reporting Officer

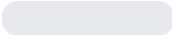
SAR: Suspicious Activity Report (Internal Document)

STR: Suspicious Transaction Report

TF: Terrorist Financing

UN: United Nations

Version Control

Date	Version	Change	Requestor	Sign Off
	v.1	N/A		Nenad S
01.05.2024	v.2	Inclusion of funding & age requirements in Section 3.2 + CDD measures for corporate entities	James PG	Nenad S
23.07.2024	v.3	Amended Section 3.2 (1) to reduce UBO threshold to 10% from 25% and to list frequency of PEP/Sanction checks on customers; also amended Section 5.2 to include money-passing on P2P products as a ML red flag;	James PG	Nenad S
02.09.2024	v.4	Inserted a new Chapter 6 (Data Retention); updated company address	James PG	Nenad S
29 Apr 2025	v.5	Adjusted for clarity and typos; Updated MLRO email and details; Clarified screening process for corporate customers; Specified types of screening checks.	Jasna S	Gino Campbell

1. INTRODUCTION

This AML/CTF Policy serves as an all-inclusive manual detailing the Company's dedication to thwarting the misuse of our services for unlawful financial endeavours, including activities like money laundering and the funding of terrorism.

As part of our unwavering commitment to ethical business practices and responsible financial operations, this AML Policy articulates the strategies, procedures, and safeguards the Company put in place to identify, mitigate and report suspicious transactions effectively. The Company is committed to high standards of anti-money laundering compliance and requires Directors, Management, Employees, Contractors and other associated third parties to adhere to these standards in preventing the use of its products and services for ML/TF purposes.

By adhering to this policy, the Company aims to safeguard its reputation, uphold its regulatory obligations and contribute to the overall integrity of the online gaming/betting sector. The Company holds online operating licences across multiple jurisdictions. To maintain these licences, we are required to have processes in place to prevent and detect money laundering and terrorist financing; and comply with local legislation in each jurisdiction.

The impact of a breach of these obligations to the Company can be very significant and can include adverse media coverage, reputational damage to the brand, financial or legislative penalties and/or suspension/revocation of our licences. Therefore, it is vital that the risks of money laundering and terrorist financing are effectively managed.

2. APPLICABILITY

This Policy is applicable to all employees, contractors, agents, clients, partners and other stakeholders directly or indirectly associated with the Company. It is incumbent upon each individual to familiarise themselves with the principles and procedures outlined within this Policy and to actively participate in its implementation.

Money Laundering is defined as:

- the conversion, exchange or transfer of property knowing or suspecting that such property is derived directly or indirectly from, or the proceeds of, criminal activity or from an act/s of participation in criminal activity, for the purpose of concealing or disguising the origin of the property or of assisting any person or persons involved or concerned in criminal activity.
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect of, in or over, or ownership of property, knowing or suspecting that such property

is derived directly or indirectly from criminal activity or from an act or acts of participation in criminal activity.

- the acquisition, possession or use of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity.
- retention without reasonable excuse of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity.
- attempting any of the matters or activities defined in the above foregoing sub-paragraphs (i), (ii), (iii) and (iv).
- acting as an accomplice in respect of any of the matters or activities defined in the above foregoing sub- paragraphs (i), (ii), (iii), (iv) and (v).

Terrorist Financing

Terrorist Financing (TF) is the process of making funds or other assets available, directly or indirectly, to terrorist groups or individual terrorists to support them in their operations. This may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organisations and traditional criminal organisations involved in money laundering operations.

Another difference is that while the money launderer moves or conceals criminal proceeds to obscure the link between the crime and the generated funds and avails himself of the profits of crime, the terrorist's ultimate aim is to obtain funds and resources to support terrorist operations.

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between the organisation or the individual terrorist and its or his/her legitimate funding sources. While ML is concerned with obscuring the source of the funds, FT is mostly concerned with obscuring the end recipient of the funds.

The risk of TF is most likely to manifest itself at withdrawal stage. However, there may be indicators that a transaction may expose the Company to funding of terrorism risks even at inception stage. Examples include situations where (a) there is negative publicity implicating the customer with terrorism or organisations linked to terrorism; or (b) the customer has links to one or more jurisdictions or areas where terrorists are active or which are known to sympathise and support terrorists and terrorist organisations. The use of anonymous means of payment to fund an account in any such situation would further accentuate the risk of FT, especially when remitting funds withdrawn by the customer.

In the above situations it becomes imperative to carry out EDD even when the customer requests to withdraw the funds. Whatever the payment method used, it has to be ascertained that the institution to which the funds are remitted is situated in a reputable jurisdiction and has equivalent AML/CFT requirements as are applicable to the Company. If the withdrawal is being made through a channel or a form that favours anonymity, the Company will - to the best extent possible - ascertain itself that it has established that the funds will eventually end up in the customer's hands.

ML/TF offences need not involve money, since the money laundering legislation covers assets of any description. In consequence, any person who commits an acquisitive crime (i.e., one that produces some benefit in the form of money or an asset of any description) is deemed to inevitably commit a money laundering offence.

3. SCOPE & PURPOSE

The primary aim of this Policy is to establish a robust framework that effectively prevents, detects, and discourages activities associated with money laundering, terrorist financing, and other financial crimes within the Company's operations.

Within this document, we elaborate on the fundamental elements of the Company's AML program, encompassing Customer Due Diligence (CDD), Know Your Customer (KYC) protocols, heightened monitoring, risk evaluation, reporting responsibilities, and continuous staff training. Through the deployment of these measures, we aspire to construct a secure and safeguarded environment for our clients, simultaneously nurturing trust and reliability within the broader financial landscape.

3.1. Business Risk Assessment (Macro)

To identify potential money laundering and terrorist financing risks we may encounter, the Company conducts a comprehensive business risk assessment on an annual basis. This assessment is crucial to establish and maintain effective measures, policies, controls and procedures aimed at preventing and mitigating these risks.

The Business Risk Assessment reviews the overall risk profile across the following risk factors:

- Customer risk;
- Product risk;

- Payment risk; and
- Location/Geographic risk.

The documented business risk assessment receives approval from the Board of Directors and - upon request – is only shared with relevant authorities, such as the Financial Intelligence Analysis Units and/or licensing Authorities.

3.2. Customer Due Diligence (CDD)

CDD consists of four measures:

- I. identifying and verifying the customer's identity on the basis of documents or information obtained from a reliable and independent source;
- II. if applicable, identifying any beneficial owner and taking reasonable measures to verify that person's identity, and to understand the ownership and control structure of the customer;
- III. assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- IV. conducting ongoing monitoring of the business relationship.

3.2.1 Identification and Verification of the Customer

In brief, customer 'identification' involves gathering a set of personal information from the customer, while 'verification' entails confirming the accuracy of the collected personal details using data, information and documents obtained from reliable and independent sources.

The specific personal information to be collected and the level of verification required should be determined based on the level of risk associated with the customer. Consequently, the Company has the flexibility to adjust identification and verification procedures based on the risk posed by each individual client.

The standard procedure for customer identification includes the collection of the following personal details during account registration:

- (a) Full name;
- (b) Permanent residential address;
- (c) Date of birth;
- (d) Place of birth;
- (e) Nationality; and

(f) Relevant identity reference number, where applicable.

In situations where the risk is deemed 'low', the Company may choose to limit identification to only the three personal details mentioned in (a) to (c) above.

During registration¹, the Company's policy is to obtain the following information:

- (a) Full Name
- (b) Permanent residential address (incl. postal code)
- (c) Date of birth
- (d) E-mail address
- (e) Phone number

Conversely, in high-risk scenarios, we may find it necessary to collect additional personal information to mitigate the increased risk of money laundering and terrorist financing.

Regardless of the approach taken, it is essential that the identification and verification procedures enable the Company to consistently confirm the customer's true identity and integrity. To achieve this, all new customers will undergo screening² prior to onboarding through a third-party system specifically designed to identify PEPs, sanctions, and adverse media.

To uphold this standard, the Company will utilize a comprehensive end-to-end compliance platform (CaaB) capable of verifying and authenticating customers worldwide. This platform will allow the Company to tailor risk appetite and configure rules to align with applicable regulatory requirements. Additionally, the platform will facilitate efficient and accurate screening of customers against global PEP, sanctions, and adverse media databases. All AML screening processes will strictly adhere to the guidelines established by the Financial Action Task Force (FATF).

Following onboarding, the Company will perform routine PEP, Adverse media and Sanction checks:

¹ The above information is collected in two stages, but prospective customers are not allowed to place any bets before the above information is collected.

² The screening will be applied, at a minimum, to individual customers, and for the corporate entity customers, to the UBOs (>10% down to a natural person) and all directors.

- semi-annually, to capture any changes in the customer's status and ensure continuous compliance;
- whenever there are significant transactions, unusual activity, or changes in account information (e.g., updating personal details, large deposits, or withdrawals; and
- in response to updates or changes in regulatory requirements or sanction lists, which may necessitate more frequent reviews.

This systematic approach ensures the Company maintains compliance with AML (Anti-Money Laundering) regulations and promptly identifies and manages any new risks.

Purple Alpha Ltd and its subsidiaries, including Lone Rock Holdings N.V., exclusively provide services to individuals who are 18 years of age or older. Any discovery of underage customers utilizing the Company's services will result in the immediate closure of their accounts as per our stringent policies and regulatory obligations. Further to this, all customer deposits must unequivocally emanate exclusively from reputable banking institutions or licensed payment providers, with transactions explicitly designated in the name of the intended recipient. The acceptance of third-party funding or cash receipts is categorically forbidden within our framework.

Following initial screening, the identities of customers conducting business with the Company must be verified in line with applicable legislation in the relevant jurisdictions. In the Company's case, this occurs when a client deposits (cumulatively) EUR (€)2,000 (or currency equivalent) or more; or before reaching the afore-mentioned thresholds if they are flagged for unusual activity. At this stage, the Company's policy is to request the following documentation:

❖ **Proof of Identity**

- Valid National Identity Document; or
- Valid Passport; or
- Valid Driving licence;

❖ **Proof of Address**

- Utility bill (Water, Gas, Electricity, Tax, Phone Bill, TV, and home internet provider); or
- Bank Statement; or
- Government issued 'Certificate of Residence'.

CDD measures are not in principle applicable until the said threshold is reached. However, on reaching the said threshold, the Company will carry out a customer risk assessment, identify the customer, verify their identity and, if deemed high risk, determine the customer's source of wealth and the source of the funds used for the said transactions. These measures are to be carried out either when the player reaches the threshold or when they collect any winnings/withdrawal stage.

Where a corporate entity wishes to open an account the following due diligence documentation is required:

- Certificate of Incorporation
- Memorandum and Articles of Association
- Register of Directors
- Passport³ and proof of address⁴ for the UBO(s) (>10% down to a natural person)
- Passport and proof of address for all the directors
- Register of Members/Shareholders

Due to the very nature of our business, the Company engages with customers solely in non-face-to-face interactions. Given these unique circumstances, when using documentary and/or electronic sources for verification, the following should be noted:

Documentary Sources – As a general rule, identity verification should be conducted by referencing an unexpired government-issued document that includes a photograph of the customer's identity (e.g., passport, identity card, residence permit, driver's licence, etc.). In cases where such a document does not confirm the customer's residential address, the Company can instead refer to and obtain any of the following documents, which should not be older than six months:

- correspondence from a central or local government authority, department or agency;
- a lease agreement;
- an official (police) conduct certificate;
- any other government-issued document not mentioned above (ex: Tax Certificate).

³ A colour copy of an in-date government issued identity document bearing the photograph of the individual e.g. Passport, drivers licence.

⁴ A copy of a proof of address document such as a utility bill or financial statement. – this document should be dated in the last 3 months and addressed to the individual's residential address.

Documents used for verification purposes need not be obtained as hard copies, but it is also possible to obtain the same electronically through electronic mail. What is important is that the documents are clear, legible and of good quality.

Also, there may be instances where the sources used for verification lack reference to the customer's residential address. In such cases, the Company can either request an additional document to verify the provided residential address or leverage existing information, such as IP addresses or device location data, which corroborates the customer's residence. The latter option can be particularly valuable when using E-ID, and requesting a documentary source for residential address verification may be challenging.

When employing documentary sources for verification purposes, the Company makes every effort to ensure the authenticity of the documents obtained or their faithful reproduction. Assessing the authenticity of certain documents may be more straightforward than others. For instance, government-issued identification documents like identity cards and passports can be cross-referenced against official templates and visually inspected for the typical security features they should contain. Conversely, documents issued by financial institutions, utility companies, and similar entities may not readily lend themselves to straightforward authenticity checks.

Verification entails not only the presentation of documents, but also the confirmation that the individual submitting the document matches the information therein. In most cases, the Company can establish this correlation based on data it possesses (e.g., geolocation information, IP address data, funding method data, etc.), which can corroborate the details presented in the customer's documents.

When the Company cannot satisfy either aspect of verification, it is expected to undertake supplementary measures to establish this connection. Therefore, apart from obtaining identification documents, the Company will assess whether additional or Enhanced Due Diligence measures are necessary. Some of these measures may include requesting additional identification documents or mandating an initial payment through an account held by the customer in a reputable jurisdiction. Different measures may be employed, as long as the operator can demonstrate that they achieve an equivalent effect.

Electronic Sources - Any sources deemed equivalent to official government documents should be considered equally reliable. These sources encompass technologies such as E-ID (or Bank-ID) and electronic commercial databases. Even within this context, the Company must scrutinise the reliability of these sources.

Furthermore, the use of electronic sources may necessitate additional measures to confirm that the individual whose identity is verified based on these sources is indeed the actual client. This is particularly relevant when using electronic commercial databases because, in

the absence of built-in automated checks, a positive result merely indicates that an individual's personal details correspond to those provided by the client, but does not guarantee that the client is that individual. Conversely, electronic sources like E-ID and Bank-ID, which require credentials unique to a specific individual, are considered to establish a strong enough link, obviating the need for additional measures.

Employees are obliged to communicate clearly with clients regarding the specific documents or information sought by the Company, minimising any ambiguity or potential for misunderstanding. Furthermore, in all situations without exception, the Company must conduct identity verification using data, documents and/or information obtained from trustworthy and independent sources.

3.2.2 Identification and Verification of the Beneficial Owner

As a general rule, the Company must ensure that customers are registering an account for their own personal use. In this regard, the Company's Terms and Conditions include specific language requiring registering players to explicitly confirm that they are registering to play on their own behalf. This said, the Company is aware that it should not solely rely on this declaration and has implemented ongoing procedures to detect any potential instances where a player may be playing on behalf of third parties. It's acknowledged that in most cases, the Company – like similar brokerages - will not encounter situations involving beneficial owners. Nevertheless, these scenarios cannot be completely ruled out.

3.2.3 Obtaining Information on the Purpose and Intended Nature of the Business Relationship

One of the Customer Due Diligence (CDD) requirements for gambling brokerages is to comprehend the reasons why a potential customer is interested in acquiring specific services or products. In the context of our business (i.e., a gambling brokerage), the purpose behind opening a gaming account is typically straightforward, and in this limited scope, additional information is not required from customers.

However, this CDD measure also encompasses the development of a customer's business and risk profile. The primary objective here is to gather sufficient information to enable the detection of any unusual activity during the course of the business relationship.

To achieve this, the Company collects adequate information and, when necessary, documentation to establish the customer's source of wealth and the expected level of activity. Source of wealth entails identifying the activities that contribute to the customer's net worth and determining whether this justifies the anticipated and actual account activity. It's important to note that this is not intended to be a detailed forensic accounting exercise.

The extent of information collection should align with the level of money laundering and terrorist financing (ML/FT) risk identified through a customer risk assessment. In cases where the risk is low, a declaration from the customer with basic details (e.g., nature of employment/business, typical annual income, etc.) may suffice. Social media can also serve as a source of information.

However, when the ML/FT risk is higher or when the Company has doubts regarding the accuracy of the information collected, it augments the information obtained with independent and reliable data and documentation.

In building a customer business and risk profile, the Company may also explore the use of statistical data to create behavioural models for assessing customer activity. If the Company opts for this approach, it can utilise data from the following sources:

- a. Official economic indicators, such as national income averages or disposable income averages, published by national public bodies or reputable financial institutions.

OR

- b. Data collected over time by the Company itself, allowing the creation of an average player profile.

3.2.4 On-Going Monitoring

Ongoing monitoring of a business relationship includes:

1. **Ensuring that documents, data or information held are kept up-to-date:** This is not intended as a requirement to repeat Customer Due Diligence (CDD) from scratch, but to ensure that the Company's understanding of the customer and the information at its disposal remains current. The Company will assess on a risk-sensitive basis whether new information requires verification or if changes are substantial enough to necessitate a fresh customer risk assessment and/or CDD process.
2. **Scrutiny of transactions to ensure they are consistent with our knowledge of the customer:** The Company conducts on-going monitoring of clients' gambling habits and behaviours to ensure that the transactions are consistent with their associated risk profile. This includes analysing clients' transactions in order to identify suspicious and/or fraudulent behaviour, and/or unusual patterns which appear to have no valid economic purpose. A full audit trail of all transactions is maintained.

If the Company observes that the account activity of a customer does not align with what is known or expected from that customer (e.g., activity not supported by the customer's source of wealth, deviating from the average profile or account activity observed to date, or failing to

match the customer's typical transaction patterns), the Company will investigate this unusual activity and, when required, determine the origin of the funds used for such activity.

Depending on the extent of the observed deviation and the explanations provided by the customer, the Company may need to reconsider its initial risk assessment and gather specific information and documentation on the customer's source of wealth, if applicable.

The level of ongoing monitoring will inevitably vary depending on the customer's risk profile. However, even in low-risk situations, there must be some degree of oversight to confirm that the business relationship still merits its low-risk classification. A change in circumstances may necessitate a re-evaluation of the risk exposure for the Company, potentially leading to an intensification of CDD measures

All Company employees must be diligent and mindful of suspicious or unusual betting activity and/or transactions during their daily tasks and must not assume it is another person's responsibility to monitor or report such activity. All employees have the ability to raise internal suspicions by emailing the MLRO directly (mlro@betinasia.com).

3. Obtaining, where necessary, Source of Funds (SOF) and Source of Wealth (SOW) information/documentation: Source of Funds refers to the activity (ex., occupation or business) generating the funds used in a particular transaction. Source of Wealth is much broader and refers to all of the economic activities which have generated the client's wealth and can include, for example, income through employment or business, inheritance, sale of property.

The extent of documentation requested will vary depending on the risk posed by the customer. In lower risk situations the Company may take less intrusive and less exhaustive steps to establish the source of funds and source of wealth of the client (such as publicly available information). In higher risk situations, the Company will not just rely on information provided by the customer, but will require documentary evidence.

The collection of Source of Wealth data from individual bettors is essential, particularly targeting those with gross settlements exceeding €30k within a year or those engaging in suspicious activities flagged by the MLRO. These criteria serve as a baseline for ongoing assessment, subject to potential adjustments in the future.

Customers presenting a high risk of ML/TF will be engaged directly to establish their source of funds and wealth. This engagement will be conducted by the appropriate Relationship / Customer Service Manager and the customer will be asked to provide sufficient information (proof of income, assets owned etc.) to give comfort that their deposits are not the proceeds of crime.

In the event that a customer fails - within the agreed timeframe - to provide adequate source of funds and wealth information/documentation, their account will be suspended and a decision to report to the relevant authorities will be considered. The decision to suspend and the decision to report are separate processes. A decision to suspend a customer will be taken by the operations department. Should an account be suspended by the said team, that customer can no longer be given access to our products/services until sufficient information is received to justify re-opening the account.

3.3. APPLICATION, EXTENT & TIMING OF CDD MEASURES

Once the EUR (€) 2,000 threshold is reached, the Company is required to conduct a customer risk assessment. These obligations encompass the completion of the CDD measures outlined in Section 3.2 above.

In cases where the Company identifies a high-risk situation, Enhanced Due Diligence (EDD) measures must be applied. This involves taking more rigorous steps in the application of CDD, which may include gathering more comprehensive information regarding the source of wealth and source of funds, as well as implementing any additional measures deemed necessary to mitigate the risks identified through the customer risk assessment. These additional measures may include steps to verify and confirm the customer's identity, as referenced in Section 3.2 (I) above.

EDD measures are also warranted in cases where there are concerns about the funding method used by a customer or when a customer employs multiple payment methods. When doubts arise regarding whether the payment method used to fund the gaming account legitimately belongs to the customer, the Company may, for instance, request clear documentation, such as an image of the card displaying the cardholder's name or, in the case of an e-wallet account, a screenshot of the account showing the name and email address of the account holder.

Risk not only influences the extent of information collected for source of wealth purposes, but may also result in a delay in the obligation to collect such information when activity levels are minimal. For example, a customer who reaches the EUR (€)2,000 threshold over the course of a year poses a lower risk than one who reaches the same threshold within a week. However, similar to any decisions made while applying the risk-based approach, it's crucial that the Company properly documents any determinations made.

During the implementation of CDD measures, customers may be permitted to continue using their gaming accounts while the Company collects any necessary information from the concerned customer. However, until the Company obtains the required information and documentation from the customer to fulfil its CDD obligations, the customer should not be

allowed to make independent withdrawals from the account, regardless of the withdrawal amount. Furthermore, if, after ninety (90) days from reaching the EUR (€)2,000 threshold, the customer has not provided the requested information and documentation, the Company is to terminate the relationship.

3.4. POLITICALLY EXPOSED PERSONS (PEPs) & SANCTIONS

Politically Exposed Persons (PEPs): PEP is defined by the Financial Action Task Force (FATF) as an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused for the purpose of committing ML offences and related predicate offences, including corruption and bribery, as well as conducting activity related to TF.

Indeed, persons who have occupied notable positions in politics or held public office could expose the Company to an increased money laundering risk owing to their potential vulnerability to corruption. In this regard, and as per Section 3.2.1 above, the Company screens all customers using a third-party system commissioned to screen for PEPs, Sanctions and any adverse media.

This heightened risk also encompasses their immediate family members and individuals recognized to have close affiliations with them. It is essential to underscore that being designated as a Politically Exposed Person (PEP) does not automatically suggest wrongdoing on the part of individuals or entities. Nonetheless, it designates the client or beneficial owner for heightened scrutiny due to the elevated risk category. Public functions exercised at levels below the national level should typically not be deemed prominent. However, when the political exposure of such positions is comparable to those at the national level, such as a high-ranking official at the state level, the Company will assess, based on a risk-based approach, whether individuals in such roles should be treated as PEPs. Prominent public functions encompass:

- Heads of State, heads of government, ministers and deputy or assistant ministers;
- Members of Parliament;
- Members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;
- Ambassadors, charges affairs and high-ranking officers in the armed forces; and

- Members of the administrative, management or supervisory boards of State-owned enterprises.

Immediate family members include:

- a spouse;
- a partner (including a person who is considered by his national law as equivalent to a spouse);
- children and their spouses or partners; and
- parents.

Persons known to be close associates include:

- any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP; and
- any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is a PEP.

To ascertain whether an individual qualifies as a known close associate of a PEP, the Company must consider any relevant information within its possession or which is publicly available. This determination does not require proactive research by staff members.

Sanctions: Sanctions are imposed by Governments and international bodies such the EU and UN, and may apply to individuals, entities and governments. In this respect, the Company utilizes a third-party AML Risk Screening tool to assist it in scrutinising our customer database.

The Company adheres to HMT , EU, UN and OFAC (USA) sanctions regimes and, as mentioned in Section 3.2.1 above, uses a third-party AML Risk Screening tool to assist it in scrutinising our customer database. To ensure the Company is compliant with such sanctions regimes all customers are screened against Sanction Lists on a regular basis.

In case a person is identified as a PEP or a close associate according to the aforementioned guidelines, staff members are mandated, considering risk factors, to:

- Obtain appropriate approval from senior management prior to initiating a business relationship with such clients. The MLRO and at least one Director of the Company are required to grant approval for opening an account as defined in this context.

- ii. Employ suitable measures to ascertain the origin of wealth and funds involved in the business relationship or occasional transaction. The Company will request individuals involved to provide comprehensive details about the source of wealth.
- iii. Continuously enhance monitoring of the business relationship, which entails active scrutiny of the account and updates of relevant documentation at intervals of no longer than 3 months.

The Company will carry out or, in the case of (iii) above, implement these measures at any point in time between the establishment of the business relationship and the point in time when the EUR (€) 2,000 threshold is met, but not later from the lapse of thirty (90) days from when the said threshold is reached.

When determining the source of wealth and source of funds for a Politically Exposed Person (PEP), the Company should tailor the extent of information and documentation requested based on the associated risk presented by the PEP. While all PEPs are inherently considered high risk, the level of risk can still vary among different PEPs. Consequently, in situations with lower perceived risk, the Company may opt for less invasive and exhaustive measures to establish the source of the PEP's funds.

During the review of client documentation, conducted as per the frequency outlined in this document, the Company will systematically screen such accounts for PEPs on each occasion.

3.5. APPLICATION OF CDD MEASURES TO EXISTING CUSTOMERS

The Company will conduct a risk re-assessment and update records in response to any modifications in the circumstances of the Client or significant alterations in the management structure of a corporate client. This review will be initiated as a response to these events.

The initial client onboarding documentation will be revised when prompted by the client, such as when there are alterations in the designated officer of a corporate client. Additionally, a mandatory update will be conducted every two years, or as required due to the expiry of documents initially collected. However, this frequency can be exceeded if the inherent regulations and policies demand more frequent reviews due to elevated client risk profiles. By adhering to this process, the Company guarantees the availability of up-to-date information for each client.

Moreover, in alignment with its operational strategy, the Company will exclusively engage with esteemed Corporate Clients who hold established familiarity with the business. These clients may be entities with whom the Company's leadership has direct interaction or those

recommended by individuals held in high regard by the Company's shareholders and/or directors. The Company will refrain from promoting its services or onboarding Clients lacking endorsements from credible, well-known, and dependable referees. It is imperative that such endorsements stem from either ongoing business relations with the Company or from individuals boasting enduring affiliations with the Company's senior management and/or shareholder. These endorsements shall be diligently documented within the pertinent Client File.

3.6. INABILITY TO COMPLETE CDD MEASURES

There may be situations where a customer is unwilling to provide the Company with the required information or documentation, even after repeated requests. In such cases, while maintaining a record of all communication attempts:

1. The Company is required to terminate its business relationship with the customer if they fail to produce the required documentation within 28 days. This entails suspending all account activity or discontinuing any other services provided to the customer. The Company may choose to either close/block the account or suspend it. If the latter option is preferred, the Company will ensure that the account has a EUR zero (€0) balance at the time of suspension, and any remaining funds in the account should be handled as outlined below.

If, subsequent to the closure/blocking or suspension of the gaming account, the customer provides the requested CDD documentation/information, the Company will assess whether the delay in receiving the requested documentation/information impacts the risk of ML/TF associated with the business relationship.

2. The Company will evaluate whether there are any reasons to suspect ML/TF. It is important to note that the customer's reluctance to provide CDD documentation should not automatically equate to a suspicion of ML/TF.

To determine if there are any grounds for suspicion, the Company will consider all available factors and information, including the payment methods used, the games played, the customer's playing behaviours, any existing customer information held by it (ex.: jurisdiction of residence) and information accessible through sources like the internet. If there are reasonable grounds to suspect ML/TF, the Company must submit a Suspicious Transaction Report (STR) to the relevant authorities, as specified in Section 5 of this document.

It's crucial to emphasise that if there are grounds to suspect ML/TF, the STR should be filed promptly, as per the requirements in the AML/CFT regulations, even if the thirty-day period allowed for collecting the necessary CDD information or

documentation has not yet elapsed or the customer has not initiated further transactions.

3. In cases where there are no grounds to suspect ML/TF and the transaction has not been suspended by the relevant authorities or by operation of the law, and there is no attachment or freezing order in place, the Company will have no legitimate AML/CFT-based reason to retain the funds. Thus, when remitting the funds, the Company will:

- a. Determine whether there are any other legal obstacles to transferring the funds,

AND

- b. Transfer the funds back to the same source through the same channels used for receiving the funds (aka. 'closed loop').

If, for any reason, the Company cannot remit the funds to the same source through the same channels, it must seek new instructions from the customer. If these instructions raise suspicions, the Company should file an STR and suspend the remittance until the relevant authorities express their stance on the transaction.

In such circumstances, when remitting funds, the Company should also, to the extent that this may be possible, include a note or instructions indicating that the funds are being remitted due to the inability to complete CDD requirements.

4. THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

Gino Steven Campbell, born on 11th of September 1968, bearing a Kingdom of Netherlands Passport numbered NP50973D5, and residing at Santa Rosa 7, Curacao, is the Company's Money Laundering Reporting Officer (MLRO). Amongst other duties, the MLRO shall be responsible to:

- Develop, implement and maintain a comprehensive AML program tailored to the Company's specific risks and operations;
- Regularly review and update the AML program to reflect changes in the regulatory landscape and evolving risks;
- Monitor customer transactions and behaviour for any suspicious activity that may indicate money laundering or terrorist financing;

- Promptly report any suspicious transactions to the appropriate authorities and maintain records of such reports;
- Establish and oversee customer due diligence (CDD) and enhanced due diligence (EDD) procedures;
- Ensure that Know Your Customer (KYC) checks are conducted for all customers during the onboarding process and periodically as required;
- Review and approve or reject high-risk customer accounts;
- Develop and deliver AML training programs to educate all employees about their AML responsibilities;
- Keep staff informed about the latest AML regulations and developments;
- Stay up-to-date with relevant AML laws/regulations, and ensure the Company's compliance;
- Maintain records and documentation to demonstrate adherence to AML regulations;
- Use risk assessments to adjust AML policies and procedures accordingly;
- Maintain accurate records of customer due diligence, transaction data, and AML investigations;
- Submit Suspicious Activity Reports (SARs) to the appropriate authorities in a timely manner when necessary;
- Establish and maintain effective communication channels with law enforcement agencies and regulatory authorities;
- Cooperate fully in any investigations related to AML matters;
- Report regularly (quarterly) to senior management and the board of directors on AML matters, highlighting risks, trends, and compliance status;
- Submit an annual AML Report covering governance and operational matters;
- Maintain independence and authority within the organisation to carry out AML duties effectively;
- Regularly assess and enhance the effectiveness of the AML program through ongoing monitoring and feedback loops;

- Collaborate with other departments to improve processes and controls related to AML.

The MLRO's role is critical to maintaining the integrity of our Company's operations and reputation. By fulfilling these responsibilities diligently and proactively, the MLRO contributes to a robust AML framework that mitigates risks and ensures compliance with applicable AML laws and regulations.

5. REPORTING SUSPICIOUS ACTIVITY & TRANSACTIONS

All staff must raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds for suspicion, that a customer is engaged in ML/TF.

5.1. Definitions

Knowledge: Having knowledge means actually knowing something to be true;

Suspicion: Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion does not need to be clear, however, it must be based on some evidence - even if that evidence is tentative. Typically, suspicion will arise when something unusual is noticed and when a subsequent investigation continues to produce unusual or contradictory facts;

Reasonable grounds for suspicion: Reasonable grounds for suspicion is an objective test of suspicion. Failure by a customer to provide the appropriate documentation and / or information for the purposes of verification of identity and/or source of wealth verification can be considered reasonable grounds for suspicion. In practice, in the regulated sector, the law interprets 'reasonable grounds for knowing or suspecting' as whether a person 'should have reasonably known or suspected' based on the information available. This stricter interpretation comes from the fact that directors and employees of regulated entities such as the Company receive specific anti-money laundering training. All directors and employees are consciously aware of the Company's AMLPP and shall integrate that consciousness into everyday business activities.

5.2. Red Flags

The following is a list of possible red flags which employees should be aware of:

- Customer does not cooperate in the carrying out of CDD.
- Customer attempts to register more than one account.

- Customer deposits considerable amounts during a single session by means of multiple prepaid cards.
- Customer deposits funds well in excess of what is required to sustain usual betting patterns.
- Customer makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions they normally carry out.
- Customer enquires about the possibility of moving funds between accounts belonging to different customers.
- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the customer's wealth, income or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- Customer seek to use a peer-to-peer betting product to transfer money from one account to another.
- Customer supplies insufficient source of wealth documentation when requested to substantiate the level of betting.
- Any information request received from a regulator or police authority that explicitly notes or implies that a customer is involved in ML/TF. Such instances must be referred to the MLRO without delay.

All reports should be sent via email to the MLRO. Staff are reminded to report a suspected instance of ML/FT to the MLRO even when their immediate superior is in disagreement with them. It will then be up to the MLRO to determine if the information available can be considered as sufficient for a STR to be filed with the relevant Financial Intelligence Unit (FIU).

When the ML/FT suspicion is linked to a transaction still to be processed, it is important that the Company refrains from carrying out the same, files a STR and delays the execution of the transaction for one (1) working day following the day on which the MLRO files the STR.

However, if refraining from processing the transaction is not feasible or doing so could harm an ongoing analysis or investigation into the suspected ML/TF activity, the Company may opt to proceed with the execution of the transaction. In such cases, the decision to proceed must be justified by the transaction's unique nature and circumstances. Following the transaction's execution, the Company brokerage is obliged to submit an STR to the FIU without delay.

On receipt of an Internal Suspicious Activity Report (SAR), the MLRO will investigate the suspicion and will decide whether to submit a Suspicious Transaction Report (STR) to the appropriate FIU. The decision to submit a Suspicious Transaction Report (STR) to the appropriate Financial Intelligence Unit is the sole responsibility of the MLRO. All decisions will be made independently of operational processes. Where a decision is made to submit a SAR to the FIU, the MLRO must do so as soon as is practicable after completing their investigation.

Generally, the MLRO will make this determination independently without involving staff members or the Board of Directors. However, the MLRO may choose to seek advice from external legal experts. Similarly, the MLRO will not disclose the specific actions taken to the individual within the Company responsible for the client relationship.

As part of standard procedure, the Board of Directors will be notified if there is a potential STR event that has been brought to the attention of the MLRO, along with the course of action decided by the MLRO.

5.3. Reporting

One of the Company's primary responsibilities is the timely submission of Suspicious Transaction Reports (STRs) to the Financial Intelligence Unit (FIAU). This obligation comes into play when the MLRO determines the presence of knowledge or suspicion regarding funds being associated with criminal proceeds, terrorism financing, or individuals involved in money laundering or terrorism funding.

STRs serve as a crucial information source for the FIU, supporting its analytical functions. Therefore, the quality of the information provided is of paramount importance. Additionally, given the speed at which funds and assets can be transferred, it is imperative that this information reaches the FIU promptly. To meet these goals, the Company will do its utmost to provide the following information in any STRs the MLRO files:

Status of account – The MLRO will shed light on whether the account is active, suspended or closed/blocked) including the balance held in the gaming account as at date of submission of the STR. Where no specific field is available on the STR Form to provide this information, the MLRO will include it in the general field ‘Additional Comments’.

Suspicious Transaction/Activity – Where available, the MLRO shall also provide the following information:

- Value and volume of withdrawals and deposits effected on a yearly basis over at least the five (5) years immediately preceding the submission of the STR.
- Unusual and/or significant increases in the value and/or frequency of deposits during a particular time-frame.
- Gaming activity which is not commensurate with the volume and/or value of deposits.
- Whether the customer effected an unusually large number of deposits using prepaid cards in a relatively short period of time.
- Cases in which an unusual time lag had passed between gaming activity and the preceding deposit/s.
- Payment methods used to effect withdrawals and deposits.
- Details relating to credit card numbers and/or any other bank account details used, such as the IBAN used for withdrawals and deposits. In the case of a payment service provider (PSP) the account identifier with the PSP should also be provided.
- An excel sheet showing all the deposit/withdrawal transactions(including date, time, amount, deposit and withdrawal method). Any attempted/unsuccessful deposits should, where possible, also be included.
- The IP addresses used to log on to the gaming account.
- The email address and phone number used to register for the gaming account and/or used for communication purposes.
- The statement and attitude of the player following for example the suspension of a gaming account.
- Copy of due diligence documents (including identification document and proof of address when available).

- Information on whether checks were carried out using third party intelligence databases, social media and/or open sources. Any information obtained through such searches will also be provided to the FIU.
- Any details as to the sources through which adverse information was obtained, including, where available, the URL to any adverse information found online and/or other information on the subject such as the involvement in companies.
- Information on whether any linked accounts were detected.
- A brief explanation on the gameplay, type of wagering and type of games.
- Contact details of the MLRO.

5.4. TIPPING OFF

Having made a report, an employee should not indicate their suspicions to the customer or reveal that a report has been made; as such actions could constitute the criminal offence of “tipping off”. The Company shall not provide customers with detailed explanations as to why an application to enter a business relationship or to process any transactions has been declined. The standard response is that the client would not match the Company’s criteria or risk appetite as laid out in its internal policies and procedures. The Company shall treat suspicious approaches to do business in the same way as a suspicious transaction as described hereunder, even if no transaction takes place.

In alignment with established AML principles, upon receipt of a Suspicious Transaction Report (STR), the Financial Intelligence Unit (FIU) may issue directives or instructions for the Company to implement measures concerning the client’s account or assets. These measures are intended to facilitate the FIU’s ongoing investigations or inquiries, or to enforce executive orders. For instance, this may involve the temporary suspension of a client’s account and/or balance within the Company.

Throughout this period, it is a priority for the Company to limit communication with the client. Should the client reach out, the Company’s response should be confined to notifying them that their account is currently undergoing a ‘routine random business review.’ Any further communication with the client must adhere to this stance, refraining from additional comments.

In line with courteous practices, the Company is encouraged to reach out to the client to inform them once the ‘routine random business review’ has been finalised, and their account has been reinstated. This communication should maintain consistency with prior interactions

and refrain from disclosing the specific reasons for the temporary suspension or blocking of the account.

All employees, including the Board of Directors shall be aware that if they disclose to the Client/person concerned or to a third party the fact that information has been demanded by the regulator or any relevant authority on any matter relating to Money Laundering or that information has been or may be transmitted to the regulator or relevant authorities, or that an analysis or an investigation has been/is being/may be carried out, will be guilty of an offence.

No employee or member of the Company's Board of Directors should be fearful of reporting a suspicion or genuine cause of concern to the MLRO.

6. Data Retention

6.1 Purpose of Data Retention

In accordance with regulatory requirements and our commitment to maintaining robust Anti-Money Laundering (AML) controls, the Company retains relevant data and records to ensure the integrity of our AML compliance program. This data retention is necessary for the detection, investigation, and prevention of money laundering, terrorist financing, and other related financial crimes.

6.2 Retention Period

To meet our legal obligations and support the effectiveness of our AML policies, the Company will retain all relevant AML-related records, including but not limited to, customer identification information, transaction records, and any related communications or reports, for a period of six (6) years from the date of the transaction or the conclusion of the business relationship, whichever is later.

6.3 Secure Storage and Disposal

All retained data will be stored securely and will be accessible only to authorised personnel. At the end of the six-year retention period, records will be securely disposed of in accordance with the Company's data destruction policies, unless otherwise required by law or ongoing legal obligations.

6.4 Review and Updates

The retention period and the necessity of retaining specific types of data will be reviewed periodically to ensure continued compliance with applicable laws and regulations. Any updates or changes to this policy will be communicated promptly to all relevant personnel.

7. TRAINING & AWARENESS

The Company is dedicated to maintaining a robust AML/CTF awareness program to ensure that all employees understand and effectively manage AML risks and meet their identification and documentation obligations as required by applicable laws and regulations. The primary objective of this program is to instill a culture of vigilance and compliance, thus minimising the risk of ML/TF and enhancing our overall AML/CTF capabilities.

7.1 Training Content

The Company's AML/CTF awareness program provides comprehensive training materials that cover:

- The fundamentals of AML/CTF laws and regulations applicable to our industry.
- Specific AML risks associated with our industry and services.
- Procedures for customer identification, due diligence, and record-keeping.
- Reporting obligations for suspicious activities and transactions.

7.2 Role-Based Training

The Company customises training content to different roles within the agency structure, ensuring that each employee and stakeholder understands their unique AML responsibilities. This includes but is not limited to:

- Agents involved in customer onboarding and transactions.
- Management personnel overseeing AML compliance.
- Contractors and third-party service providers associated with our agency.

7.3 Regular Training Sessions

To maintain a high level of AML awareness, we conduct regular training sessions for all employees. These sessions are scheduled and documented to ensure that everyone remains informed about the latest AML developments and best practices.

Furthermore, as part of our onboarding process, all new employees/contractors receive AML/CTF training to equip them with the knowledge necessary to meet AML obligations from the start of their engagement.

7.4 Continuous Improvement

The Company commits to regularly review and enhance its AML awareness program to address evolving risks and industry best practices. We adjust training content, controls, and procedures as necessary to ensure the program remains effective.

Date: 29 Apr 2025

Matters to Note:

- a. This document is to be read in conjunction with the National Ordinance Reporting Unusual Transactions (NORUT) and the National Ordinance Identification when Rendering Services or NOIS applicable in the territory of Curaçao.
- b. This document shall be reviewed at least annually by the Board of Directors of the company.
- c. Testing the effectiveness of the company's Anti-Money Laundering Policies and Procedures (AMLPP) will be done as part of an external audit and will be subject to a separate report produced by such external auditor on that yearly occasion.
- d. Reference to employees and/or officers of the company refers to professional employees engaged in the company's business, their support staff and the Board of Directors. It does not refer to ancillary staff who are not engaged in the day-to-day core activities of the company's business.
- e. The registered office of the Company is at ZUIKERTUINTJEWEG Z/N, (ZUIKERTUIN TOWER) CURACAO

Fig. 1 - Customer Due Diligence Obligations

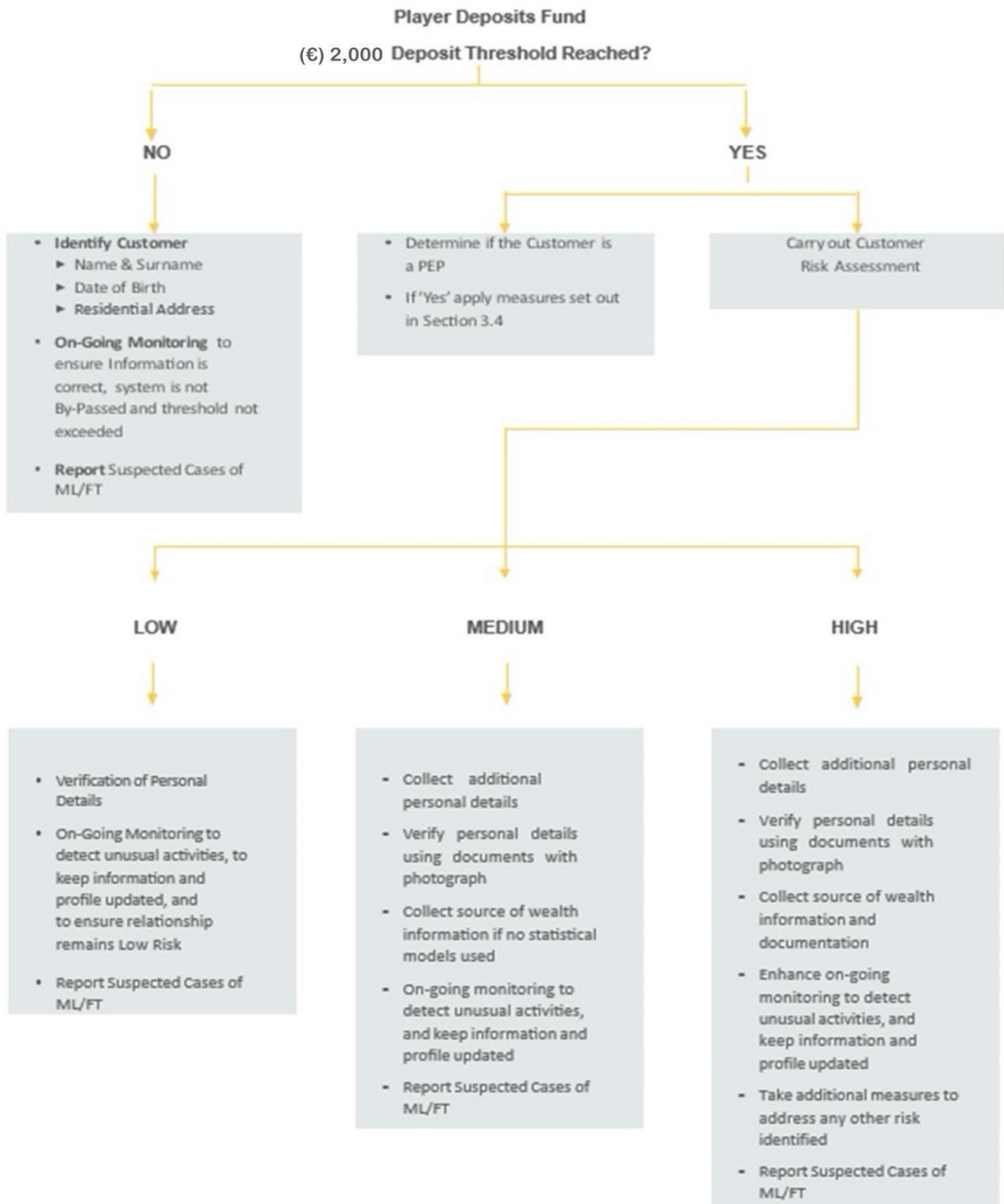


Fig 2 – Risk Assessment

FUNDING METHODS

	Low	Low-Medium	Medium	Medium-High	High
Bank transfers (EEA or equivalent safeguards)	X				
Debit/credit cards issued by banks (EEA or equivalent safeguards)	X				
Debit/credit cards issued by other licensed financial institutions		X			
EEA-licensed payment service providers			X		
Non-EEA licensed PSP				X	
EEA-licensed PSP that can be funded with cash or quasi-cash				X	
Prepaid cards/vouchers					X
Cryptocurrencies					X
Peer to Peer transfers					X
Cash					X

GAME TYPES

	Low	Low-Medium	Medium	Medium-High	High
--	-----	------------	--------	-------------	------

Fixed odds games without hedging (ex: slots, lotteries, bingo)	X				
Fixed odds games where hedging is possible (ex: blackjack, baccarat, roulette)			X		
Sportsbetting			X		
P2P games (ex: poker, betting exchange)				X	

CHANNEL

	Low	Low-Medium	Medium	Medium-High	High
Remote & automated registration on an electronic platform without 3rd party intervention	X				
Facilitation of registration by a land-based intermediary				X	
Use of master account set-up					X