

BetMaximus

ANTI MONEY LAUNDERING POLICY - AML

JANUARY 2024

Gladiator Holding N.V.

Company Number: 161721

Registered Address: Zukikertuintjeweg Z/N

Zuikertuin Tower,

Willemstad, Curaçao



Preface:

The provided terms used in this Policy shall have the same definition provided in the latest Terms and Conditions of BetMaximus.

Where the context so requires, the use of the masculine gender shall include the feminine and the singular shall include the plural and vice versa.

BetMaximus recognizes its obligations with respect to the anti-money laundering and countering the funding of terrorism (**"AML/CFT"**) commitments arising from the Prevention of Money Laundering and Funding of Terrorism Regulations (**"PMLFTR"**) and other relevant laws.

The guidelines issued by BetMaximus consider the recommendations made by the Financial Intelligence Analysis Unit with the Malta Gaming Authority, in terms of the provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations and in accordance with FIU (Financial Intelligence Unit).

This Policy is applicable to the activities of the BetMaximus including its director and employees. The Policy sets up procedures in order to meet obligations arising from the PMLFTR.

BetMaximus acknowledges the fact that the AML/CFT regulatory framework is applicable to it as a subject person thus adopting a risk-based approach.

The Player/s wishing to use the services of BetMaximus agree to abide by all the rules and regulations relating to AML/CFT.

BetMaximus reserves the right to suspend the Players Account should the Player not abide by the provisions of this Policy.

Contents:

Preface	2
1. Registration of Players.....	4
2. Anonymous Accounts	4
3. Examination of transactions	4
4. Payments of winnings	4
5. Acceptance of wager	5
6. Maximum limit of payment out of Player's account	5
7. Source of Wealth and Funds	5
8. On-Going Monitoring	6
9. Politically-Exposed Persons.....	6
10. Risk Assessment	7
11. Money Laundering Reporting Officer	8
12. Compliance Officer	9
12. Reporting Suspicious Activity and Transactions	9
13. Record keeping	11
14. Training	11
Annex I CDD – Customer Due Diligence	12
Annex II EDD- Enhanced Due Diligence	17
Annex III PEP - Politically Exposed Persons	18

1. Registration of Players

The process for the registration of the Players is provided for under the **Terms & Conditions**. This provides for the due diligence process that must be carried out before the opening of Accounts. The due diligence procedure is carried out for the purposes of the prevention of money laundering and financing of terrorism ("ML/FT").

Before any opening of an Account there must be registration by the Players which involves the provision of accurate details and documentation to BetMaximus. It is the Player's responsibility to immediately provide BetMaximus with updated information to any information/documentation provided at the initial Account opening stage. BetMaximus has the discretion to verify reliability of a Player with third parties who previously provided any information on the Player.

Under the registration, the Player has to fill in all the information requested, and it is Player's responsibility to ensure that the information provided is complete, valid and accurate. BetMaximus reserves the right to conduct identification and verification procedures. In a situation when a BetMaximus suspects that a Player provided unreal/inaccurate information, the Player's Account might be closed and blocked by BetMaximus pending investigation. It shall be the Player's responsibility to notify BetMaximus of any updates or changes of his personal data.

If BetMaximus becomes conscious that a potential Player has provided false information, BetMaximus will immediately cancel that person's registration as a Player and close his Account. No person under eighteen.

(18) years of age may be registered as a Player and any funds deposited or any money won by such person shall be forfeited. Where a minor, manages to make use of the gaming service, BetMaximus shall take all necessary steps to prevent such minor from making further use of its gaming service and to return the minor to the state in which the minor was prior to playing, returning any monies wagered and confiscating all winnings, if any. BetMaximus shall, at all times, keep a secure online list of all registered Players. Any one individual can only register a single Account with BetMaximus and multi-account practices are strictly prohibited.

2. Anonymous Accounts

BetMaximus shall not open anonymous Accounts or Accounts in fictitious names such that the true beneficial owner is not known.

3. Examination of transactions

BetMaximus reserves the right to monitor all the transactions with a view to prevent ML/FT. Furthermore, BetMaximus reserves the right to examine with special attention, and to the extent possible, the background and purpose of any complex or large transactions and any transactions which are particularly likely, by their nature, to be related to MT/FT.

4. Payments of winnings

A Player requesting the first withdrawal following registration shall be required to verify his identity through the submission of a copy of an identification document. The withdrawal request shall not be acceded to by BetMaximus prior to receipt of a copy of this document from the Player. In all cases, BetMaximus reserves the right to suspend a cash-out request pending verification of the Player's identity, age, and location. Payments of winnings or refunds shall be transferred back through the same channel from which

Player had made the original transfer in the first place. Where this is not possible, the Player shall be requested to provide an alternative channel together with sufficient proof that such channel relates back to the Player. It shall be within BetMaximus's sole discretion to determine whether proof provided by the Player is sufficient or not.

5. Acceptance of wager

BetMaximus shall not accept a wager from a Player unless:

- an Account has been established in the name of the Player and there are adequate funds in the Account to cover the amount of the wager; and
- the funds necessary to cover the amount of the wager are provided in an approved way.

6. Maximum limit of payment out of Player's account

BetMaximus shall carry out **Customer Due Diligence ("CDD")** through the verification of the Player's identity, age and residence upon the value of a transaction executed by the Player reaches or exceeds two thousand Euro (€2,000). The details of the CDD can be found in Annex I of the Policy. CDD process will likewise be undertaken if the Player executes a series of linked transaction which, though individually below the €2,000 threshold, when taken cumulatively meet or exceed this threshold. If the transaction or series of transactions are considered to be high risk, BetMaximus shall carry out **Enhanced Due Diligence ("EDD")**. The details of the EDD can be found outlined in Annex II of this Policy.

CDD is intended to allow BetMaximus to know who its customer is and to build a customer profile on the basis of which BetMaximus would be able to assess the customer's activity to identify any unusual behaviour.

BetMaximus shall conduct on-going monitoring of the Players' transactions to determine the moment in time when the €2,000 is reached and ensure that such obligations to collect CDD are not avoided by the Player.

The CDD application when reaching €2,000 threshold it's applied in regards to players which are making the deposits through Credit Card/Sofort.

BetMaximus cannot accept cash from Players and funds may be received from the Players only by any of the following methods:

- credit cards;
- debit cards;
- bank transfer;
- e-wallets.

7. Source of Wealth and Funds

BetMaximus shall collect sufficient information from the Players, and where necessary documentation, to establish the Player's source of wealth as well as his expected level of activity. A declaration from the Player including some details relative to the nature of his employment/business, usual annual salary, pay slips will be sufficient. The assessment of the risk posed by a natural person is generally based on the player's economic activity and/or source of wealth. A player having a single source of regular income

will pose a lesser risk of ML/FT than a customer who has multiple sources of income or irregular income streams.

In this situation, BetMaximus shall collect sufficient information and, where it is necessary, documentation to establish a customer's source of wealth as well as the expected level of activity. Source of wealth consists in determining the activities which generate the customer's net worth and whether this justifies the projected and actual level of account activity. BetMaximus shall also make research on the social media platform/internet, also the income proof for the last six months is required from the customer.

8. On-Going Monitoring

BetMaximus shall ensure that all Players' documents, data or information held is up-to-date which means that BetMaximus shall obtain from the Players fresh identification documents when these expire and shall carry out on-going monitoring and verification of the consistency of data provided. Additionally, as part of the on-going monitoring obligations of BetMaximus, Players transactions shall be scrutinised and BetMaximus shall ensure that such transactions are consistent with Players regular transactions and business and risk profile.

Regarding the carrying out on-going monitoring of the business relationship, BetMaximus shall: ensure that the documents, data or information held are kept up-to-date, i.e.: obtaining fresh identification documents when the expiry date of identification documents held on file is reached; inconsistencies regarding the data already registered.

9. Politically-Exposed Persons

BetMaximus shall require Players to identify and confirm whether they are considered to be Politically Exposed Persons ("PEP") in terms of the rules and regulations relating to AML and CFT through an EDD. The definition of the PEP is detailed in the attached Annex III.

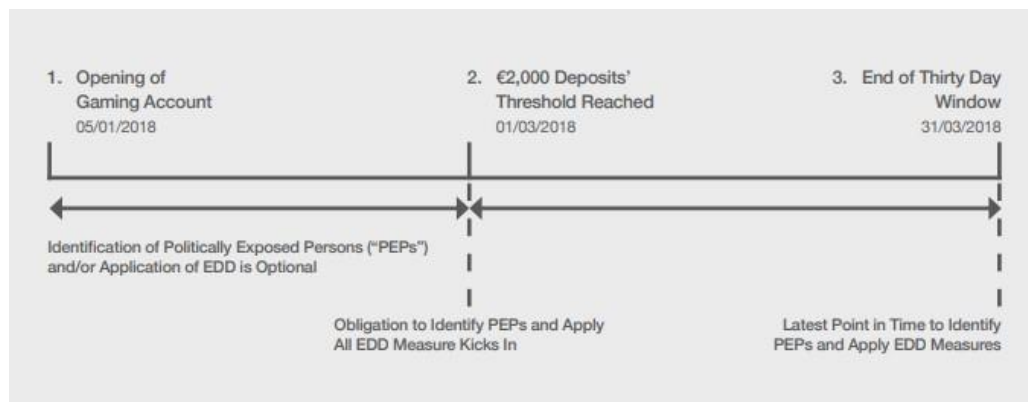
If a Player identifies himself as a PEP, prior to accepting any deposits from such persons BetMaximus shall seek to obtain senior management approval to accept the PEP to become a Player. Moreover, BetMaximus shall also establish what their source of wealth, and where applicable source of funds originates from.

In situations where PEPs involved, it's required the application of pre-established EDD measures:

- a) Obtain senior management approval to service the PEP.
- b) Establish their source of wealth and, where applicable, their source of funds; and
- c) Conduct enhanced on-going monitoring of the customer's activity

In establishing the source of wealth and source of funds of a PEP, BetMaximus are to determine the extent of the information and/or documentation requested on the basis of the risk posed by the customer. Whilst it is true that all PEPs are to be considered as high risk, the degree of this risk will still vary from one PEP to another.

Politically Exposed Persons – Record



10. Risk Assessment

BetMaximus's risk management system is designed to identify the risks it faces and has measures in place to keep those risks to an acceptable minimum. The existence of risk presents both threats and opportunities to BetMaximus.

BetMaximus admit the fact that the AML/CFT regulatory framework that is applicable to it as a subject person adopting a risk-based approach. BetMaximus therefore will take necessary measures proportionate to the ML/FT risks to which it is exposed in order to prevent and mitigate the said risks from materializing themselves, in accordance with Financial Investigation Unit of Curaçao and the Regulatory Authority. Each Player who participates in BetMaximus's activities expose BetMaximus to different risks. A player risk assessment will therefore be carried out so that BetMaximus will be able to identify potential risks upon entering a business relationship with, or carrying out an occasional transaction for, a Player, as applicable. This risk assessment enables BetMaximus to develop a risk profile for the Player and to categorise the ML/FT risk posed by such Player as low, medium or high.

The **Business Risk Assessment** comprises of four steps:

- **Customer risk:** The risk of ML/FT may vary in accordance with the customer income; BetMaximus shall monitor all sources of income, as a customer having a single source of regular income can pose a lesser risk of ML/FT than a customer who has multiple sources of income or irregular income flow.
- **Product, Service, and Transaction risk:** When identifying the risk associated with the transactions, BetMaximus consider and measures the risk of the level of transparency, or transaction affords, the value of the transaction, the customer of accounts held or cards issued.
- **Interface risk/ Delivery Channel:** The policies, procedures, systems and controls that BetMaximus holds are including: to prevent the misuse of technological developments in money laundering and terrorism financing schemes; and to manage any specific risks associated with non-face-to-face business relationships or transactions.

• **Geographical risk:** BetMaximus measures the indicators related to nationality, residence and place of birth of a customer, such variables has to be analysed as these might be indicative of a increased geographical risk

When carrying out their business and Player risk assessments, BetMaximus will consider the following list of ML/FT risk indicators, including:

- insufficient, incomplete or suspicious information or information that cannot be verified provided by the Player;
- use of proxies, unverifiable IP address or geographical location, disposable email address or mobile number, ever changing devices used to conduct transactions;
- unusual patterns of transaction activity (e.g. volumes, velocity, structuring to avoid detection/reporting obligations, source, destination);
- the potential for cybercriminals to launch ransom-ware attacks.
- official economic indicators such as average national income, average disposable income etc. issued by national public bodies or reputable financial institutions

As potential mitigating measures against these elevated threats, BetMaximus shall carry out robust CDD procedures (and collect IP addresses and other device identifiers when appropriate) as well as continue applying the ongoing monitoring. BetMaximus will ensure that the documents, data or information are kept up-to-date.

Risk probability is the chance of an identified ML/TF risk materialising as part of everyday operations across the industry. This can also be interpreted as the vulnerability of each area identified and how likely the area is to be exploited by criminals. Some risks are therefore more likely to occur than others.

Risk impact describes the expected damage to the operator and industry should the identified ML/TF materialise without any specific control measures in place. The potential impact is not the same for all identified risks as some may have a greater impact than others. When determining the impact of an identified risk, consideration has been given to factors such as:

- Facilitation of criminal conduct
- Risk of regulatory fines and legal prosecution
- Reputational damage to operators and/or the industry overall
- Loss of business as a result of customer rejection

The ongoing monitoring of a business relationship usually includes: the transactions undertaken throughout the course of the relationship in order to ensure that the transactions undertaken are in

accordance with BetMaximus's knowledge of the customer and of the business, risk profile, where necessary, the source of funds, also ensuring that the documents, data or information held by BetMaximus are kept up to date.

When carrying out the customer risk assessment, BetMaximus will have a methodology which relies on different pillars, as described below:

<u>First risk categorisation</u>
--

<i>*upon registration without KYC documentation or any other information and/or investigation about the customer</i>
HIGH RISK
1) Country: FATF lists, EU list identifying high risk 3rd countries with strategic deficiencies, and/or the jurisdictions featuring in the top 20 countries of the Basel Index"
2) Affiliate source : Regardless If the source is organic or 3rd party source
3) Email domain: IF the user is using a disposable email address, is another indicator that it might berelated to Fraud since such addresses do not require authentication
MEDIUM RISK
1)Country: not included in FATF lists, EU list identifying high risk 3rd countries with strategic deficiencies, and/or the jurisdictions featuring in the top 20 countries of the Basel Index"
2) Affiliate source :If the source is organic and NOT 3rd party source
3) Email domain: IF the user is using a disposable email address, is another indicator that it might berelated to Fraud since such addresses do not require authentication
LOW RISK
1)Country: not included in FATF lists, EU list identifying high risk 3rd countries with strategicdeficiencies, and/or the jurisdictions featuring in the top 20 countries of the Basel Index"
2) Affiliate source :If the source 3rd party
3) Email domain: IF the user is NOT using a disposable email address, is another indicator that it mightbe related to Fraud since such addresses do not require authentication

<u>Latest risk categorisation</u>
(after account is checked/KYC requested and account investigation is begun)
HIGH RISK
1) CASE 1:
A) Country: FATF lists, EU list identifying high risk 3rd countries with strategic deficiencies, and/or the jurisdictions featuring in the top 20 countries of the Basel Index"
B) No KYC documentation received
C) Affiliate source : Regardless If the source is organic or 3rd party source
2) CASE 2:
A) Country: regardless of jurisdiction
B) NO SOURCE OF FUNDS & SOURCE OF WEALTH received from depositors which passed the10.000EUR threshold
<i>*After PEP screening, if passed will be included in MEDIUM RISK CATEGORY</i>
<i>**After PEP Screening, if passed user and also user provides KYC documentation + Source of Funds + Wealth will be included in LOW RISK CATEGORY</i>
MEDIUM RISK
1) CASE 1:
A) Country: FATF lists, EU list identifying high risk 3rd countries with strategic deficiencies, and/or the jurisdictions featuring in the top 20 countries of the Basel Index"
B) KYC Documentation received

C) <u>Affiliate source : Regardless If the source is organic or 3rd party source</u>
<u>2) CASE 2:</u>
<u>1)Country: not included in FATF lists, EU list identifying high risk 3rd countries with strategic deficiencies, and/or the jurisdictions featuring in the top 20 countries of the Basel Index"</u>
B) <u>KYC Documentation not received</u>
C) <u>Affiliate source: Regardless If the source is organic or 3rd party source</u>
<u>LOW RISK</u>
<u>A)Country: not included in FATF lists, EU list identifying high risk 3rd countries with strategic deficiencies, and/or the jurisdictions featuring in the top 20 countries of the Basel Index"</u>
B) <u>KYC Documentation received</u>
C) <u>Affiliate source: Regardless If the source is organic or 3rd party source</u>
<u>Flagged Disposable Emails Domains</u>
<u>bvhhs.com</u>
<u>sartess.com</u>
<u>yopmail.com</u>
<u>mailnator.com</u>
<u>GetNada</u>
<u>MailCatch</u>
<u>MailDrop</u>
<u>MohMal</u>
<u>MyTemp</u>
<u>OwlyMail</u>
<u>ThrowAwayMail.com</u>
<u>TrashMail</u>
<u>10minutemail.com</u>
<u>E4ward</u>
<u>GuerrillaMail.</u>
<u>EmailOnDeck</u>
<u>Dispostable</u>
<u>Sharklasers</u>
<u>Mailinator</u>
<u>Airmail</u>
<u>Spambox</u>
<u>Guerillamail</u>
<u>Mailsac</u>
<u>Blur</u>
<u>Bloody Vikings</u>
<u>E4ward.com</u>
<u>Spamgourmet</u>
<u>GishPuppy</u>
<u>Spamex</u>
<u>Jetable.org</u>

<u>Spamfree24</u>
<u>Choicemail1.com</u>
<u>Deadspam.com</u>
<u>Dcemail.com</u>
<u>E-mail.com</u>
<u>Emailgo.de</u>
<u>Getonemail.com</u>
<u>Gishpuppy.com</u>
<u>Goemailgo.com</u>
<u>Gotmail</u>
<u>Guerillamail</u>
<u>Hatespam.org</u>
<u>Inboxalias.com</u>
<u>Kasmail.com</u>
<u>Killmail.com</u>

<u>Mail-filter.com</u>
<u>Mailbidon.com</u>
<u>Mailcatch.com</u>
<u>Mailms.com</u>
<u>Mailnull.com</u>
<u>Mailtv</u>
<u>Manybrain.com</u>
<u>Monumentmail.com</u>
<u>Mytempemail</u>
<u>Quickinbox.com</u>
<u>Rtrtr.com</u>
<u>Shiftmail.com</u>
<u>Nomail</u>
<u>Owlpic.com</u>
<u>Pookmail.com</u>

The customer risk assessment has been implemented in Everymartix system, showing the exact methodology regarding the **First Risk Categorization** and **Latest Risk Categorization**.

The automated task has been implemented in connection with the **Customer Risk Assessment**, when the first verification is made, meaning the First Risk Assessment which is made upon onboarding stage, in the context sequentially to registration process.

The First Risk Categorization represents the basic verification that will be made directly upon registration, looking at several indicators that will allow us to assess the exposure/risk, as follows:

- Country
- Registration source (affiliate source)
- Email domain

BetMaximus have divided the customers into the following three risk categories:

1. LOW-RISK PLAYER

2. MEDIUM-RISK PLAYER

3. HIGH-RISK PLAYER

Basically, BetMaximus have implemented three roles in GPlat named as the above-mentioned categories that they will be assigned to all existing accounts and further on to every new account that will sign-up based on the mentioned criteria from below:

HIGH-RISK PLAYER:

Country: included in the high-risk country list

Affiliate source: Regardless of If the source is organic or 3rd party source

Email domain: Regardless of the user using a disposable email address

MEDIUM RISK PLAYER:

Country: not included in the risky country list

Affiliate source: Regardless of if the source is organic or 3rd party source

Email domain: If the customer is using a disposable email address

LOW RISK PLAYER:

Country: not included in the risky country list

Affiliate source: Regardless of if the source is organic or 3rd party source

Email domain: If the customer is not using a disposable email address

HIGH-RISK/RESTRICTED COUNTRIES:

Albania; Afghanistan; Bahamas; Barbados; Burkina Faso; Cambodia; Cape Verde; Cayman Islands; China; Democratic People's Republic of Korea (DPRK); Ethiopia; Haiti; Iran; Jamaica; Jordan; Madagascar; Mali; Mauritania; Morocco; Mozambique; Myanmar; Nicaragua; Pakistan; Panama; The Philippines; Senegal; Solomon Islands; South Sudan; Sri Lanka, Turkey, United Arab Emirates, Gibraltar, Syria, Yemen and Uganda.

France, French Territories, Curacao, The Netherlands, Spain, Italy, Portugal, Belgium, Dutch West Indies, UK, Poland, Romania, Greece, Lithuania, Aruba, Bonaire, Saba, Sint Eustatius, St. Maarten, Singapore and US.

The second step regarding the Latest Risk Categorization is made for customers that reached a total amount of deposits of 2.000 EUR or more or if they have an active pending withdrawal (or requested the first withdrawal), and the verification of the criteria is performed in real time, then the Risk Category is updated based on the Roles (Criteria) the customer has registered on the account. (And the roles from the latest risk categorization are being updated in real time based on the changes/amendments that occurred during the course of the business day such as documents/SOF/SOW getting verified, PEP screening & sanctions completed, etc.

Regarding the 2.000-euro threshold or in case of a withdrawal request, a KYC Form is automatically sent and the tag "Waiting for KYC documents" is being assigned on the accounts. Opposed to Waiting for KYC documents, the tag "Verified Identity" will be assigned as soon as the customers KYC Documentation gets validated.

In essence, the Latest Risk Categorization tags will be triggered by certain roles that are present on the account and can be related the customer getting verified in the meantime or have his SOF/SOW checked/verified or get the score screening regarding PEP verification. Periodically we are conducting a manual assessment on the accounts in cause to be re-checked in order to ensure that the Latest Risk categorization is in line with the automatically assigned GPlat roles based on the criteria.

As soon as the Latest Risk Assessment is performed dynamically, for customers who reached the 2.000-euro threshold or more; or 1st withdrawal/pending withdrawal, the initial First Categorization Risk role will be removed and will be replaced with new one (from Latest Risk Categorization).

Triggers – ROLES (GPlat Backoffice account tags related to Customer Due Diligence Process)

Related to KYC:

- Not verified (or not provided yet)

- o Waiting for KYC documents

- o no KYC related role

- Verified (provided docs):

- o Verified Identity

Related to SOF/SOW Verification:

- Not verified (or not provided yet)

- o Source of Wealth Review / Source of Funds Review

- Verified role:

- o Source of Funds Verified / Source of Wealth Verified

Related to PEP Screening

- Not verified (or not checked yet)

- o No role about pep on account

o PEP under review

· Verified has role:

o Non-PEP

o PEP

COUNTRY: HIGH RISK COUNTRY

HIGH-RISK PLAYER:

KYC STATUS: not verified or verified

SOF/SOW STATUS: Not verified

PEP STATUS: Not verified

MEDIUM RISK PLAYER:

KYC STATUS: Verified

SOF/SOW STATUS: Verified

PEP STATUS: Not verified

LOW RISK PLAYER:

KYC STATUS: verified

SOF/SOW STATUS: Verified

PEP STATUS: verified

COUNTRY: NOT HIGH-RISK COUNTRY

HIGH-RISK PLAYER:

KYC STATUS: not verified

SOF/SOW STATUS: Not verified

PEP STATUS: Not verified

MEDIUM RISK PLAYER:

KYC STATUS: Verified

SOF/SOW STATUS: Not verified

PEP STATUS: Not verified

LOW RISK PLAYER

KYC STATUS: verified

SOF/SOW STATUS: Verified

PEP STATUS: verified or unverified

Additionally, BetMaximus will identify and assess other relevant verifications in due course, based on Customer Risk Factors; Product/Service, Transactional Risk Factors; Geographical Risk Factors; Delivery Channel Risk Factors in which the analysis can be established in scenarios like: Customer KYC request, Validation and Verification; Customer source of wealth/source of funds request, Validation and Verification and the Latest PEP & Sanctions Screening.

BetMaximus must establish, record, maintain and operate appropriate procedures and controls which require verification of the identity of the customer using reliable, independent source documents, data or information, and where there is no cooperation from the customer:

- 1) The ongoing customer relationship or transaction will proceed no further;
- 2) The business relationship should be terminated and
- 3) A disclosure to be made to relevant authorities if applicable

Identification and Verification of the Customer is usually made on the course of the onboarding stage. Identification consists in the collection of a series of personal details on the customer. Verification on the other note consists in confirming the personal details collected for identification purposes through the use of documentation, information. KYC process is applicable regarding the first withdrawal, and it depends also on the customer profile and the velocity thresholds.

The standard identification procedure consists in meeting the personal details:

- (a) name and surname;
- (b) residential address;
- (c) date of birth;
- (d) place of birth;
- (e) nationality; and
- (f) identity reference number where applicable

In low-risk situations BetMaximus's taking in consideration the identification to the three personal details (name and surname, permanent residential address) and regarding the high-risk situations BetMaximus may collect additional personal details.

WHEN KYC & CDD is made - Threshold deposit Limit Reached (2,000-euro total deposit-calculated in real time since the establishment regarding the business relationship; or on a daily basis taking into account all deposits effected by a customer since the establishment of the business relationship / First Withdrawal / High Risk player (PEP/Deposit pattern/ geo location / funding method). Lifetime deposits are taken into consideration and all deposits made by a customer since the establishment of the business relationship are calculated daily and are automatically send via email to Payments Team/Finance with all registered accounts which reached or passed the 2.000-euro threshold and havenot yet been validated or verified.

Regarding the Customer Risk Assessment, this will be carried out in the case of the business relationship not later than thirty (30) days from when the pre-established threshold (2.000 euro) is met.

Moreover, in case where the imposed timeframe of 30 days has elapsed since the threshold of two thousand (EUR 2,000) and the customer did not provide the requested information and documentation, BetMaximus's is to consider restricting the account until compliance with BetMaximus request. In case information and documents are not provided after restricting the account, BetMaximus may consider termination of the business relationship with the customer.

The CDD documentation is obtained within the 30 days from when the 2.000-euro threshold was reached given the First Risk Categorization and Latest Risk Categorization Rules, also based on the alert generated by PIQ. BetMaximus is able to check the date of 2.000 EURO threshold. Moreover, BetMaximus is using the option to block the deposit method ("withdraw only" setting). HOW & WHAT - Requesting KYC documents and Carrying out electronic checks:

A) Identity Card – Valid Government Issued ID Verification Document (driver's license, passport, national ID and in some instances birth certificate),

B) Proof of address – Issued within the last 3 months (utility bill such as electricity or water bill, or a bank statement in your name, showing the address registered on his casino account), must contain customer's full name, address and date of issue,

C) Funding Method – Bank cards (such as front and back copies of the debit/credit card, with the middle digits and security CVV code covered) / Official bank statements or Screenshots in the case of e-wallets (must contain customer's personal data & transaction(s) made into his casino account).

D) Source of Wealth/Source of Funds – Must contain reliable data from which customer's income is earned as supporting evidence; and/or financial documents which are attesting the source of wealth or source of funds (such as bank statements, monthly pay-slips, Employment Detail Summary).

E) Verification call – Needed when additional check is required in addition to KYC documentation

Additional KYC may be required if:

- the documentary evidence supplied is doubted by the risk officer e.g. detail mismatch on Identity card and proof of address and user cannot explain discrepancy.
- transaction is suspicious or raises red flags. for example, the source of funds for a transaction
- the transaction includes a PEP
- where the customer is established in a high-risk jurisdiction

ACTION STEPS:

a) Threshold reached: high risk + Level of restriction to be applied when request is sent for KYC documentation and CDD applied.

b) Obtaining the necessary information and documentation from the customer to meet the CDD obligations, moreover the customer is not to be allowed to effect any withdrawals

from the account independently of the amount involved.

*Apply respective due diligence roles when full KYC is in place i.e. Verified Identity/ Source of Wealth Verified & remove risk roles.

FAILURE TO COMPLETE CUSTOMER DUE DILIGENCE:

- For (a) above: Restriction stays in place – Available Funds Blocked & STR filed within 24 hours.
- For (b) above: Low risk – funds returned to user's gaming account after 48 hours

High risk – Restriction in place + funds returned to gaming account after 48 hours + STR filed within 24 hours; Restriction in place + STR filed

Reporting a STR has to take place when BetMaximus's having reasonable grounds to suspect that ML/ FT may be taking place, taking in considerations all the red flags indicated by Financial Investigation Unit of Curaçao

- Customer does not cooperate in the carrying out of CDD.
- Customer attempts to register more than one account with BetMaximus.
- Customer deposits considerable amounts during a single session by means of multiple pre-paid cards.
- Customer deposit 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 he normally carries out.
- Customer enquires about the possibility of moving funds between accounts belonging to the same gaming group. (regarding the duplicate accounts)
- 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 displays suspicious behaviour in playing games that are considered as high risk.

11. Money Laundering Reporting Officer

There shall be appointed a Money Laundering Reporting Officer ("MLRO") whose main responsibility will be to consider any internal reports of unusual or suspicious transactions and, where necessary, follow up the same by filing a Suspicious Transaction Report ("STR") with the Regulatory Authority. The location of the MLRO is to be present where BetMaximus is actually conducting its activities from.

Other responsibilities of the MLRO include the following:

- Monitoring compliance with this policy
- Reporting to the relevant board or authorities on compliance with this policy
- Coordination and monitoring of BetMaximus's day-to-day compliance with applicable laws and the Policy;
- Conducting employee training programs relative to the AML/CTF for employees and maintaining records evidencing such training;
- Receiving and reviewing any reports of suspicious activity from employees and/or officers of BetMaximus.
- Issuing the proper assessment for internal reports, the submission of STRs to the FIU, as well as responding to any requests for information received from the FIU
- Developing, implementing and monitoring systems, management of policies and procedures relevant to the business
- Ensuring there are mechanisms to facilitate the reporting of any suspicions that money laundering may be taking place, receiving and investigating any such reports and in turn making reports to the FIU
- Identify training needs and organize relevant training sessions, with regular refresher sessions

The MLRO must be able to dedicate proportionate time to the tasks associated with this position as well as have the required resources to carry out the same. This would include:

(a) connection to any and all information that may be considered necessary by the MLRO for the proper evaluation of internal reports, the submission of STRs to the FIU, as well as responding to any requests for information received from the FIU; and

(b) ample resources and time to review internal reporting procedures, assess internal reports in an efficient manner, and acknowledge by the set timeframes when it comes to responding to requests for information by the FIU or submitting STRs.

12. Compliance Officer

The compliance officer ensures that BetMaximus complies with its outside regulatory and legal requirements, as well as internal policies and bylaws, also oversees the daily implementation of its AML/CFT measures, policies, controls and procedures.

BetMaximus ensures that: the FIU is provided with access to any data, information or documentation it may request in the carrying out of its functions; the MLRO and also the Compliance Officer makes himself accessible to the FIU, including for any meetings and/or interviews that the FIU may want to carry out.

13. Reporting Suspicious Activity and Transactions

BetMaximus shall conduct in place internal and external procedures providing for the reporting of suspected or known instances of ML/FT or of proceeds of crime as well as instances where there are reasonable grounds to suspect as much as provided for in Regulation 17 of the PMLFTR. The internal reporting

procedures will allow BetMaximus's employees and/or officers to even report the suspected activity of ML/FT to the MLRO. It will be then up to the MLRO to determine if the information available can be considered as sufficient for the filing of the STR to the Regulatory Authority.

When the ML/FT suspicion is linked to a transaction still to be processed, BetMaximus shall refrain from carrying out the same, BetMaximus shall file the STR and delay the execution of the transaction for one (1) working day following the day on which it files the STR. During this time the Regulatory Authority has to determine and communicate to BetMaximus whether it objects to the execution of the said transaction.

Where refraining from carrying out the transaction is not possible or doing so would prejudice an analysis or investigation of the suspected instance of ML/FT, BetMaximus may decide to proceed with the transaction's execution. The impossibility to refrain from processing a transaction must arise from the nature of the transaction itself and then BetMaximus must then submit a STR to the FIU immediately afterwards.

BetMaximus's reporting obligations arise in the following circumstances including:

- suspicion that transactions are linked to ML/FT;
- When in the course of its business activities, a Player is linked to ML/FT or that ML/FT is being committed or may be committed independently of whether any transactions have taken place or otherwise; and
- When there are reasonable grounds to suspect that ML/FT may be taking place, this being a more objective ground for reporting; this implies that a further obligation to report arises where, on the basis of objective facts, BetMaximus ought to have suspected that ML/FT existed.
- STR Filling, in case where there is a suspicion of FT or that funds are the proceeds of criminal activity. BetMaximus shall look out for the following red flags that give rise to reporting obligations include:
 - When the Player provides false identification information or does not cooperate in the carrying of CDD;
 - When BetMaximus notices the Player undertakes unusual rapid movement of assets and/or funds;
 - Player attempts to register more than one account with BetMaximus;
 - Player deposits considerable amounts during a single session by means of multiple prepaid cards;
 - Player deposit funds well in excess of what is required to sustain his usual betting patterns;
 - Player makes small wagers even though he has significant amounts deposited, followed by a request to withdraw well in excess of any winnings;
 - Player makes frequent deposits and withdrawal requests without any reasonable explanation;
 - Noticeable changes in the gaming patterns of a Player, such as when the Player carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
 - Customer enquires about the possibility of moving funds between accounts belonging to the same gaming group.
 - 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 displays suspicious behaviour in playing games that are considered as high risk.

14. Record-keeping

BetMaximus shall retain, amongst others, records of CDD, ongoing monitoring, internal and external reports, and such other records as are sufficient to permit the reconstruction of individual transactions and prove compliance with the PMLFTR, and any applicable procedures issued by the Regulatory Authority in terms of Regulation 17 of the PMLFTR.

15 Training

BetMaximus shall provide AML/CFT training to all employees and/or officers of BetMaximus as part of its obligations of Regulation 5(5) of the PMLFTR, also is providing employees from time to time with training in the recognition and handling of operations and transactions which may be related to proceeds of criminal activity, money laundering or the funding of terrorism.

CDD (Customer Due Diligence)

The resolution of the Player's risk profile is essential to allow BetMaximus to apply necessary CDD level, to enable BetMaximus to get to know the Player and to build the Player's profile.

IDENTIFICATION

BetMaximus first and foremost shall establish the identity, jurisdiction, and purpose of each Player, and the nature of transaction (business relationship or occasional). BetMaximus will obtain from the Player his full name, place and date of birth, permanent residential address, identity/passport number, nationality.

The standard identification procedure consists in the gathering of the following personal details:

- (a) name and surname;
- (b) permanent residential address;
- (c) date of birth;
- (d) place of birth;
- (e) nationality; and
- (f) identity reference number where applicable.

VERIFICATION

To verify the identity of the Player, BetMaximus shall obtain the copy of the following documents:

- an unexpired national or government-based passport, identity card or driving license

Where any such documents does not allow verification of Player's residential address, BetMaximus shall verify the residential address, by obtaining one of the following documents which should not be more than six (6) months old:

- a recent statement or reference letter issued by a recognized credit institution; or
- a recent utility bill issued in relation to services linked to that residential property; or
- correspondence from a central or local government authority, department or agency; or
- a lease agreement;
- an official conduct certificate;
- any other government-issued document not mentioned above; or

- the mailing of correspondence via registered mail or by means of a courier which allows the subject person to obtain documentary evidence that the correspondence was effectively delivered at the residential address provided by the customer and signed for by the same.

- Electronic Sources – These include sources like E-ID (or Bank-ID) and electronic commercial databases. In this context, BetMaximus have to consider the question of reliability. Sources which are considered as equivalent to official government documents are to be considered as bearing the same level of reliability.

Documents used for verification purposes need not be obtained as hard-copies, it shall be possible for the Player to send to BetMaximus the same electronically through electronic mail or other audio-visual means. BetMaximus shall ensure that documents obtained are clear, legible and of good quality.

BetMaximus may also vary the extent of verification depending on the risk posed by the particular business relationship. This can be measured by:

- Varying the nature of the documentation obtained - In low risk situations for example it is possible for BetMaximus to verify a customer's identity on the basis of government issued documents or alternative, but reputable information sources, even where these do not contain photographic evidence of one's identity (e.g.: birth certificates, licences issued by government or public authorities, bank statements etc.). This also in view of the additional details that BetMaximus can hold on a customer (e.g. IP address, device geolocation etc.).

- Varying the extent of the personal details verified – Verification is intended to ensure that BetMaximus knows who it is dealing with and therefore the personal details collected for identification purposes need always be verified in their consistency. While the verification of the basic identification details that may be collected in low risk situations needs to be carried out in all instances, the verification of any other personal details is left to the discretion of BetMaximus as long as it has sufficient comfort that it knows who its customer is.

When using sources for verification purposes, BetMaximus ensures as much as possible that the documents obtained are authentic or reproduce authentic ones.

The CDD measure also requires the development of a customer business and risk profile, the key element being having sufficient information available so as to allow the detection of unusual activity in the course of a business relationship. BetMaximus's collecting sufficient information and, where it is necessary, documentation to establish a customer's source of wealth as well as the expected level of activity. Source of wealth consists in determining the activities which generates the customer's net worth and whether this justifies the projected and actual level of account activity.

Application, Extent and Timing of CDD Measures

CDD measures in regards with Regulation 9(1) of the PMLFTR, provides that needs to be applied when carrying out transactions amounting to Euro two thousand (€2,000) or more, whether carried out within the context of a business relationship or otherwise.

In the situation of an occasional transaction, the obligation to carry out CDD will be determined on the value of the said transaction reaching or exceeding Euro two thousand (€2000). BetMaximus shall execute a series of linked transactions which, though individually below the said threshold, would cumulatively meet

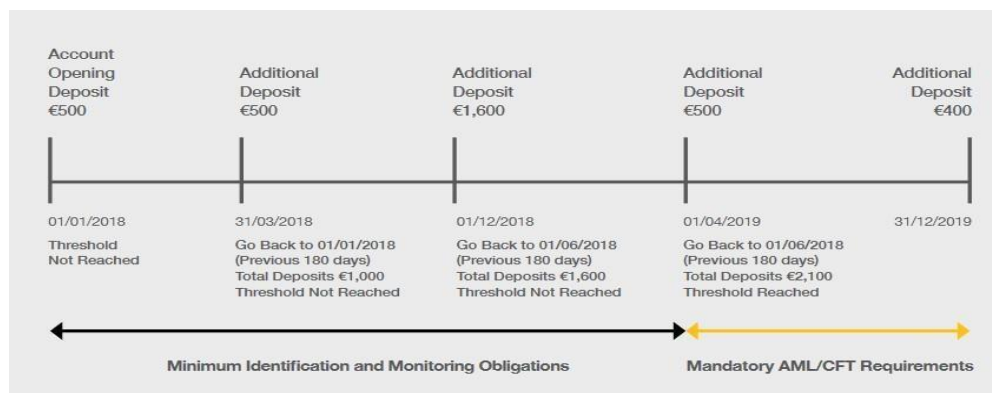
or exceed the Euro two thousand (€2000) threshold. In this case transactions are considered as linked if for example they are carried out by the same customer through the same game or in one gaming session. In this context, BetMaximus has to carry out a customer risk assessment, identify the customer and verify their identity.

The CDD application when reaching €2,000 threshold it's applied in regards to players which are making the deposits through Credit Card/Sofort.

Even before reaching the €2,000 threshold, BetMaximus has measures in place which allow it to apply a level of on-going monitoring. Regarding these systems, BetMaximus ensures that:

- We are able to determine the moment in time when the Euro two thousand (€2,000) threshold is met.
- The player does not avoid the application of CDD measures by avoiding the Euro two thousand (€2000) threshold.
- We are able to deny the application for the opening of an account by a person who has inputted manifestly false details.
- We are able to detect instances which give rise to a suspicion of ML/FT.

Application of the Rolling Period:



Customer Due Diligence Obligations:

In case where Player Deposits Fund- €2,000 Deposit Threshold is reached, BetMaximus shall determine if the Customer is a PEP, if it's not a PEP BetMaximus will carry out the Customer Risk Assessment which can be evaluated in three stages:

A. LOW :

- Verification of Personal Details

- On-Going Monitoring to detect unusual activities, to keep information and profile updated, and to ensure relationship remains Low Risk

- Report Suspected Cases of ML/FT

B. MEDIUM :

- Collect additional personal details

- Verify personal details using documents with photograph

- Collect source of wealth information if no statistical models used

- On-going monitoring to detect unusual activities, and keep information and profile updated

- Report Suspected Cases of ML/FT

C. HIGH :

- Collect additional personal details

- Verify personal details using documents with photograph

- Collect source of wealth information and documentation

- Enhance on-going monitoring to detect unusual activities, and keep information and profile updated

- Take additional measures to address any other risk identified

- Report Suspected Cases of ML/FT

Inability to Complete CDD measures:

BetMaximus shall not enter into a business relationship or undertake an occasional transaction unless it has verified the true identity of the Player.

Where it proves impossible for BetMaximus to complete CDD within the timeframe acceptable to BetMaximus, BetMaximus shall not:

- allow any activity of any kind by the Player or provide any other service to the Player and, to this end, BetMaximus may decide to either close the Player's account or profile or to keep it deactivated in its entirety; and

- determine whether it is necessary to lodge a STR with the Regulatory Authority.

Should BetMaximus be in possession of funds or assets belonging to the Player which may have been received in advance in relation to a service to be provided by BetMaximus, and there no grounds to suspect ML/FT or the transaction has not been suspended by the Regulatory Authority or by operation of the law, nor is there an attachment or freezing order, BetMaximus shall remit the funds or assets to the same source and through the same channels used to receive them, and this after having considered whether there is any

other legal impediment to their remittance. BetMaximus will indicate in any transaction script that the funds or assets are being remitted back due to the inability to complete CDD.

Application of CDD measures to existing customers:

BetMaximus is handling all pre-existing procedures which are applied in order to meet the CDD obligations as explained in this document. BetMaximus continues applying the same procedures while paying special attention to the on-going monitoring obligations.

In case when the Euro two thousand (€2000) threshold has already been met, BetMaximus applies the new revised procedures for the existing customers on a risk-sensitive basis but within a reasonable time period.

EDD (Enhanced Due Diligence)

EDD is applicable for players who pose a higher risk. EDD measures are further measures to the CDD measures, which BetMaximus shall apply in order to ensure that the increased risks presented by specific business relationships are better monitored and administered.

EDD must be applied in four (4) different scenarios:

- Non-Face-To-Face (where BetMaximus determines that additional EDD measures are required);
- PEPs;
- Suspicion or any other particular cases presenting higher risk as outlined in the Policy;
- Failure to satisfy either aspect of verification.

Therefore, in addition to the CDD measures set out hereabove, BetMaximus shall apply one or more of the

following measures:

- Verification through the use of recognized commercial electronic data providers;
- Establishing the identity of the Player by using additional documentation and information wherein the Player shall provide BetMaximus with additional documentation to confirm the personal details by means of documents listed hereabove. The documents obtained in terms of this particular EDD measure are required to be additional to the documents obtained when carrying out CDD and should have been obtained from other independent sources. The additional documents cannot be the same documents obtained for CDD purposes;
- Verify or certify the documentation supplied using supplementary measures. This measure consists in the certification of the documentation used for the purposes of the verification of identity by a warranted legal professional, certified accountancy professional, a notary, a person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction. Such certification should be evidenced by a written statement stating that:
 - the document is a true copy of the original document;
 - the document has been seen and verified by the certifier; and
 - the photo is a true likeness of the applicant for business or the beneficial owner

The certifier must sign and date the copy document (indicating his name clearly beneath the signature) and clearly indicate his profession, designation or capacity on it and provide his contact details. Where doubts have arisen about the existence of the certifier, subject persons should make independent checks to verify the existence of such certifier and document such checks.

PEP (Politically Exposed Persons)

PEP as a natural person who is or has been entrusted with prominent public functions and includes his immediate family members or persons known to be close associates of such persons but shall not include middle ranking or more junior officials. For the purposes of the Player acceptance process, BetMaximus shall apply EDD in relation to PEPs residing in another Member State of the Community or in any other jurisdiction.

The term PEP is broad and generally includes all persons who fulfil a prominent public function. In fact Regulation 11(7) of PMLFTR states that a natural person who is or has been entrusted with a prominent public function shall include:

- a) Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries;
- b) Members of Parliament or similar legislative bodies;
- c) members of the superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- d) members of courts of auditors, or of the boards of central banks;
- e) ambassadors, chargé d'affaires and other high-ranking officers in the armed forces;
- f) members of the administrative, management or supervisory boards of state-owned enterprises; and
- g) anyone exercising a function equivalent to those set out in paragraphs (a)-(f) above within an institution of the European Union or any other international body.

With respect to the term 'immediate family members' of PEPs, the PMLFTR provide that the term shall include:

- a) the spouse, or any partner recognised by national law as equivalent to the spouse;
- b) the children and their spouses or partners; and
- c) the parent.

With respect to the term 'persons known to be close associates', the PMLFTR provide that the term shall include:

- a) a natural person known to have:
 - joint beneficial ownership of a body corporate or any other form of legal form;

- or any other close business relations with that PEP.

b) a natural person who has sole beneficial ownership of a body corporate or any other form of legal form that is known to have been established for the benefit of that PEP.

The application of EDD to PEPs, their immediate family members and close associates is mandatory as long as a PEP remains entrusted with a prominent public function, as defined above, and for at least a subsequent twelve (12) month period from when he ceases to be so entrusted.

The data required to determine if a customer (or its beneficial owner) is a PEP can be obtained either from the customer (e.g. by completing a standardised self-declaration as to his/her status or, to the extent which may be applicable, that of its beneficial owners) or by using reliable electronic databases to screen their customer database. In establishing the source of wealth and source of funds of a PEP, BetMaximus is to determine the extent of the information and/or documentation requested on the basis of the risk posed by the customer.

Despite the fact that the situations involving PEPs are mandatorily subject to EDD measures, BetMaximus shall still carry out the Customer Risk Assessment.

The occasional transaction or business relationship may disclose additional factors indicative of a high risk of ML/FT which BetMaximus may have to address through measures other than those which have to be applied when dealing with PEPs.

The next variables might suggest that a business relationship or an occasional transaction involving a PEP poses a higher risk:

a) when the customer is seeking to have access to a product, service or transaction that is capable of being misused to launder the proceeds of corruption or bribery;

b) personal wealth or lifestyle is inconsistent with known legitimate sources of income or wealth;

c) credible allegations of financial misconduct; and

d) the PEP is entrusted with a prominent public function in a jurisdiction where there is a higher risk of corruption and where information available indicates that the jurisdiction shows the following characteristics (therefore, the subject person should assess the jurisdiction separately).

When undertaking additional CDD measures on PEPs, their family members or persons known as close associates, BetMaximus shall apply all the EDD measures set out in Regulation 11(5) of the PMLFTR, such as:

a) obtaining senior management approval

b) taking adequate measures to establish the source of wealth and funds involved

c) conducting enhanced ongoing monitoring

d) EDD measures for long-term insurance business.

Version Number	Version/Amendments	Approved By	Date	Signature
V1	Initial draft	Vlad Profeanu (CEO)	2024.01.10	