

AML/KYC Policy

1. Introduction

Anti-Money Laundering and Know Your Customer Policy (hereinafter - the “AML/KYC Policy”) is designated to prevent and mitigate all possible risks of Unlimited Solutions B.V. (hereinafter – the Company/Betunlim) being involved in any kind of illegal activity.

Money laundering is the process by which criminals attempt to conceal the illegal origin of the proceeds of their criminal activity (drugdealing, weapons dealing, human trafficking, kidnapping, etc.) allowing them to maintain control over the proceeds and ultimately, providing a legitimate cover for their sources of income.

The Company is fully committed to be constantly vigilant to prevent money laundering and combat the financing of terrorism in order to minimize and manage risks such as the risks to its reputational risk, legal risk and regulatory risk.

To protect the funds of our Customers and ensure compliance with international trade standards, the Company operates exclusively in accordance with the laws on combating money laundering and countering the financing of terrorism and criminal activities. This Policy aims to comply with the rules and guidance contained in the following laws, namely:

- the National Ordinance Penalization of Money Laundering (NOPML),
- the National Ordinance on the Reporting of Unusual Transactions (NORUT),
- the National Ordinance on Identification of clients when Rendering Services (NOIS),
- Directive (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018,
- NATIONAL ORDINANCE of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance)
- FATF recommendations,
- CFAFT documents.

2. Risk based approach

As per the applicable laws, the Company adopts a risk based approach. It hence identifies and analyses its risks and subsequently makes use of measures, policies, controls and procedures to curb any undesired risks, amongst which those related to the money laundering and funding of terrorism risks from materializing. The approach, allows for flexibility and significant discretion to be exercised by the Company. This in itself entails significant responsibility.

Risk Assessment

Risk assessment entails:

- i) recognition of existence of risk
- ii) undertaking of a risk assessment, and
- iii) implementing systems and strategies to manage and control the identified risks.

There is no doubt that the business of remote gaming is deemed risky. The risk assessment will however identify the key risks the company faces as well as the level of these risks, so

that, consequently, the necessary measures are adopted to manage and control the identified risks. This procedure will specify the controls and processes that are to be followed so as to ensure that the risks which the Company has identified and which it will face as part of its operations will not materialize. The Company's organizational risk assessment which is to be approved by the Board of Directors takes the following factors into consideration:

- i) recognition of existence of risk
- ii) undertaking of a risk assessment, and
- iii) implementing systems and strategies to manage and control the identified risks.

The risk assessment will identify the key risks the company faces as well as the level of these risks, so that, consequently, the necessary measures are adopted to manage and control the identified risks. This procedure will specify the controls and processes that are to be followed so as to ensure that the risks which the Company has identified and which it will face as part of its operations will not materialize. The following factors are taken into consideration:

i. Product/Service Risk

Some gaming products/services/transactions are more vulnerable to criminal exploitation than others. These include, for instance, gaming products or services that allow the customer to influence the outcome of a game, be it one player alone or in collusion with others.

The Company minimizes the risk by offering only games certified by international laboratories. The Company does not offer new games from the providers, which have no history on the market. This minimizes the risks and product risk is regarded as considerably low.

ii. Geographical Risk

This is the risk posed to the Company by the geographical location of the customers, however also the geographical locations of its suppliers and service providers. The element to be considered in respect of this fraud management procedure is primarily that attributable to the customers and the source of funds of the said customers. The nationality, residence and place of birth of a customer should be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak anti-money laundering and counterfeit terrorism system, countries known to suffer from a significant level of corruption, and countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction will be considered as high risk. The opposite is also true and hence may be considered as presenting a medium or low risk.

The Company does not accept players from the countries from "Call for action" list of FATF as far as the risks are considered too high.

The Company accepts clients from countries which are on so called grey list of FATF, but these clients are regarded as high-risk clients.

The company also takes into consideration the following list of countries:

- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);

- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

The countries, from which the clients are considered high risk clients:

Bulgaria
Burkina Faso
Cameroon
Croatia
Democratic republic of Congo
Haiti
Kenya
Mali
Monaco
Mozambique
Namibia
Nigeria
Philippines
Senegal
South Africa
South Sudan
Syria
Tanzania
Venezuela
Vietnam
Yemen

The countries, from which the clients are considered medium risk clients:

Russia
Afghanistan
Cuba
Byrma
Ethiopia
Iraq
Libia
Lebanon
Liberia
Somali
Sudan

The clients from other countries can be considered low risk in case there are no other grounds to consider them high risk clients.

The Company does not accept residents from these countries:

Aruba
Curacao
France
The Netherlands

Sint Maarten
Spain
Ukraine
Great Britain
USA

iii. Customer Risk

This relates to the type of customer being provided with the service.

The Company has 2 types of non-welcome clients:

1) PEPs (politically exposed persons)

The company generally does not accept PEPs, but a person which ceases to be a PEP might be accepted as a client.

The individual will be screened so as to determine whether he is a PEP, or in any way associated to a PEP.

A person who considers himself/herself a PEP or has doubts about his/her PEP status, must inform our team via e-mail support@betunlim8.com.

2) Sanctioned persons

The company observe US and EU sanction lists and does not accept natural persons from these lists as clients.

Checks would also be carried out to ensure that the individual is not subject to any sanctions or other statutory measures.

The Company considers the following natural persons as high risk clients:

- 1) High spenders (more than 2 700 USD/month or equivalent)
- 2) making one or series of deposits/withdrawals within short period of time (usually 24 hours) which amounts to 2 700 USD or more.
- 3) Customers which make irregular deposits with no obvious reason.

3. Customer due diligence

The Company does not accept legal entities as clients and does not plan to do it.

The Company has no anonymous accounts and opens only one account for one person.

The Customer due diligence (CDD) measures to be taken are as follows:

- a. Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- b. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the player, its business and risk profile, including, where necessary, the source of funds.

Criteria for applying EDD or Simplified Due Diligence (SDD)

SDD is applied to low-risk players, EDD is applied to high-risk players.

Enhanced due diligence measures include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

SDD is applied to low-risk clients if the Company hasn't taken other decision.

In case when SDD applied, it is allowed not to collect source of wealth documents.

4. Identification of the players

1. *When identifying the player*, at a minimum the following information must be collected:

- i. full name;
- ii. permanent residential address;
- iii. date of birth;
- iv. place of birth;
- v. nationality;
- vi. and identity number.

The Company has a list of documents which must be provided by the Customer for the purpose of identity verification, namely: a color copy of the passport (the first two pages with pictures and details, as well as the page with the residential address stamp, if there is one) or a color copy of the national ID card. Upon the request of the Company additional documents must be provided: a copy of the Customer's driver's license, utility bills (as proof of address). The verification process also involves mandatory confirmation of the Customer's phone number.

The Company reserves the right to request additional documentation if it deems necessary upon times in order to complete their AML checks and compliance standards. MLRO and CO are entitled to demand photo/video of the Customer with the passport at any time they consider appropriate.

Withdrawals from the Customer's account is allowed only after the Customer's identity has been verified on the basis of the documentation provided and a completed questionnaire. Withdrawals can be made only to the account belonging to a person identified as a Customer of the Company (personal account holder on the Website). Withdrawal of funds to third parties are prohibited. Internal transfers between Customers are also forbidden.

Carry out a Customer Risk Assessment

This is done to have sufficient information available to detect unusual activity in the course of the business relationship. At this stage, a provisional risk rating will be assigned based on the initially collected information. This is revised once questions are answered or additional information received.

3. *Verification of an identity* refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources. Where such a document does not allow verification of the player's residential address, the Company can obtain other documents like a bank statement, utility bill, letter from a public authority or rental agreement, which should not be more than six months old to verify the residential address. The Company can also contact the player by letter, e-mail or telephone to verify the information supplied. It can also send a verification code to the e-mail address to verify that the address is current and genuine. Verification can also be done by technical methods – for instance, using Sumsb bases. Where the Company does not have sufficient comfort that it knows its player, it is expected that it will take additional measures to do so. Some of these measures include requesting additional identification documents, asking the player to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

4. *Sanctions screening and PEP status screening*. All players are screened against sanctions lists of the UN and EU.

5. Ongoing monitoring

Ongoing monitoring of identity

Ongoing monitoring of identity aims at keeping the records up to date. In case the document has expired the Company contacts the player and demands to update the information.

In case the person's IP which does not correspond to the place of residence the Company may contact the player for explanations.

Ongoing transaction monitoring

AML-Compliance ensures that an "ongoing transaction monitoring" is conducted to detect transactions which are unusual or suspicious compared to the customer profile.

This transaction monitoring is conducted on three levels:

1) The first Line of Control:

The company works solely with trusted Payment Service Providers whom all have effective AML policies in place as to prevent the large majority of suspicious deposits from taking place without proper execution of KYC procedures onto the potential customer.

2) The second Line of Control:

The Company makes its network aware so that any contact with the customer must give rise to the exercise of due diligence on transactions on the account concerned. In particular, these include:

- Requests for the execution of financial transactions on the account;
- Requests in relation to means of payment or services on the account;

Also, all transactions must be overseen by employees overwatched by the AML compliance officer who is overwatched by the general management. The specific transactions submitted to the customer support manager, possibly through Compliance Officer must also be subject to due diligence. Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to the knowledge of the customer (KYC), their financial behavior, and the transaction counterparty. These checks will be done by an automated System, while an Employee crosschecks them for additional security. The transactions observed on customer accounts for which it is difficult to gain a proper understanding of the lawful activities and origin of funds must therefore rapidly be considered atypical (as they are not directly

justifiable). Any staff member must inform the AML division of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known of the customer.

3) The third Line of Control:

As a last line of defense against AML Compliance Officer will do manual checks on all suspicious and higher-risk users in order to fully prevent money laundering.

Money Laundering Reporting officer and Compliance Officer

To monitor in accordance with the legal requirements, the Company appoints Money Laundering Reporting officer (MLRO) and Compliance Officer (CO) that develops Anti-money laundering measures and Know Your Customer procedures (AML/KYC), which are obligatory for all employees of the Company.

The Compliance Officer is responsible for the effective enforcement of the AML/KYC Policy. Compliance Officer duties are the following:

- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the Company's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the Company's efforts against money laundering and financing of terrorism and financing of proliferation.

MLRO's duties are as following:

- To design and implement the AML program;
 - To make necessary changes to the AML program;
- AML program is approved by Management board of the Company.

One person can occupy both positions.

The MLRO and CO are entrusted to ensure that all the operations of the Company are consistent with the international standards for combating money laundering and terrorist financing and that all the documents provided by the Customer are up to date and fully comply with the relevant legal requirements. As a result, by opening an account on the Website the Customer unconditionally accepts the AML policy, agrees with the following rules and undertakes to observe them.

6. Reporting of suspicious transactions

Recognition of unusual transactions

An unusual transaction is a transaction inconsistent with the player's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the player. The purpose of collecting information is to provide the Company with documentation to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship. Based on the NORUT legislation, objective and subjective indicators have been established by means of which the Company assesses whether a customer's transaction qualifies as an unusual

transaction. Management must provide its staff with specific guidance and training in recognizing and adequately documenting unusual transactions. All these unusual transactions must be reported to CO.

CO must keep an adequate filing system of these records.

If internally reported transactions are not reported to the FIU by the Company, the reason shall be adequately documented and signed off by the CO and/or management.

The following transactions or intended transactions are deemed unusual:

- a. Transactions by or on behalf of a natural person, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- b. Transactions in the amount of 2700 USD or more (number of transaction within 24 hours on the amount of 2700 USD or more).

Reporting of unusual transactions:

By virtue of article 11 of the NORUT, the Company reports unusual transaction or any intended unusual transaction to the FIU without delay.

All unusual individual transactions or series of transactions must be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting. The documentation of unusual transactions has to register with the FIU and to get access to the goAML reporting portal after validation by the FIU.

The compliance officer prepares a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The Company reports to the FIU the details of the transactions by means of the goAML reporting portal.

The reports and the submission of the thereto related information (all supporting documents) should be done in English.

Record keeping

The records of all players transactions and players related documents (ex: passports, identity cards and etc.) are kept in electronic format during 5 years.

7. Staff training

MLRO and CO should take external training on regular basis – every year.

Staff training can be organized on place. CO drafts the staff training program, which should be approved by management.

Every member of the team related to KYC and AML procedures should receive initial training from CO when start performing his/her duties.

The Initial training includes the detailed study of:

Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction (the recent version),

NATIONAL ORDINANCE of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance).

The conditions on which the license is granted.

As a result of training the new team member is offered tests so the MLRO can be sure the new member is ready to perform its duties.

8. An independent audit function to test the AML program

The AML compliance program must be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party.

The audit must be external. The audit organization must have previous experience in auditing AML program. The company to perform an audit must not be registered in “Grey list” FATF countries.

These tests must include at least:

- An evaluation of the institution’s anti- money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer’s file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system’s ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management.