AML Policy

Company Policy

It is the AML policy to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company strives to comply with all applicable requirements under the legislations in force in the jurisdictions in which the Company operates, to prevent of the use of the financial system for the purpose of money laundering and terrorist financing.

The Service is owned by UniqueGame N. V., a company registered in Curaçao with registration number 144499 and address: Dr. H. Fergusonweg 1, Curaçao and its partners: TechFin Dev Ltd with registration number 1962590 and address: Craigmuir Chambers, 18 Russell Hill, Road Town Tortola, British Virgin Islands and Mileniumpro Services Limited with registration number HE430118 and address: Avlonos, 1, Maria House, 1075, Nicosia, Cyprus. The Company is required to have in place adequate measures to prevent its systems from being used for the purposes of money laundering, terrorist financing or any other criminal activity.

Objective of the Policy

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. It is also committed to its social duty to prevent serious crime and not to allow its systems to be abused in furtherance of these crimes.
The Company will endeavour to keep itself updated with developments both at national and international level on any

initiatives to prevent money laundering and the financing of terrorism. It commits itself to protect, at all times, the organization and its operations and safeguards its reputation and all from the threat of money laundering, the funding of terrorist and other criminal activities.

The Company's policies, procedures and internal controls are designed to ensure compliance with all applicable laws, rules, directives and regulations relevant to the Company's operations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place.

Player Identification Program

The Company will take reasonable steps to establish the identity of any person for whom it is proposed to provide its service (hereinafter "Players"). For this purpose, the process for the registration of Players provided for under the General Terms and Conditions of the Company provides for the due diligence process that must be carried out before the opening of a user account.
The Company will keep at all times a secure online list of all registered Players and information and documents will be retained in accordance with the applicable data protection obligations.
The Company will collect certain minimum Player identification information from each Player who opens an account. The Company will not accept to open anonymous accounts or accounts in fictitious names such that the true beneficial owner is not known.
The information required will include at least:

- Player's date of birth (showing that the player is over eighteen (18) years of age);
- Player's first and last name;
- Player's place of residence;
- Player's valid email address; and

- Player’s username and a password.

Documents to verify the identity information received will be requested from the Player if and when there is considered to be risk or uncertainty about the information provided and prior to any payment in excess of EUR 2 000 per occasion or when payments to the account are made in excess of EUR 2 000. These documents shall include, to the extent permitted under the relevant data protection regulations:

- A copy of a valid identity card or passport;
- Proof of address.

The Company may supplement the use of documentary evidence by using other means, which may include:

- independently verifying the Player’s identity through the comparison of information provided by the Player with information obtained from a reporting agency, public database or other source;
- Checking references with financial institutions; or
- Obtaining a financial statement.

The Company will inform relevant Players that the Company may seek identification information to verify their identity.
Any employee of the Company who becomes aware of an uncertainty in relation to the accuracy and truthfulness of the Player information provided shall immediately notify the AML Compliance Person, who will review the materials and determine whether further identification is required and or so that it may be determined whether a report is to be sent to the relevant authorities.
If a potential or existing Player either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not

open a new account and, after considering the risks involved, consider closing any existing account. In either case, the AML Compliance Person will be notified so that it may be determined whether a report is to be sent to the relevant authorities.
If a Player has been identified as attempting or participating in any criminal or unlawful activity, the Company will take the appropriate steps to immediately freeze the account of the Player.

If any material personal information of a Player changes, verification documents will be requested.

Continuous transaction due diligence

The Company will monitor account activity with special attention, and to the extent possible, the background and purpose of any more complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.
Monitoring will be conducted through the following methods:
Transactions will be automatically monitored and reviewed daily for all transactions above 1 000 EURO along with all the details of the users making those transactions. Documents may be required at the determination of the AML Compliance Person.
The AML Compliance Person will be responsible for this monitoring, will review any activity that the monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the relevant authorities.
Parameters that signal possible money laundering or terrorist financing include, but are not limited to:

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent reason.

- Many small, incoming wire transfers or deposits made using checks and money orders.
- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent specific purpose.

When an employee of the Company detects any activity that may be suspicious, he or she will notify the AML Compliance Person. AML Compliance Person will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a report.
The Company will not accept cash or non-electronic payments from Players. Funds may be received from Players only by any of the following methods: credit cards, debit cards, electronic transfer, wire transfer cheques and any other method approved by the Company or respective regulators.
The Company will only transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.
To the extent the Company utilizes a third party to process and record payments to and from Player and accounts, the Company will use best efforts to ensure the services provider has transaction monitoring systems in place which will allow for screening of the transactions pursuant to these provisions and in accordance with the applicable legislation. The AML Compliance Person shall be responsible to review the relevant service agreement with the service provider to ensure the adequacy of the agreement.

Records relating to the financial transactions shall be maintained in accordance with the data protection and retention requirements in the applicable jurisdiction of Curaçao.

Suspicious Transactions and Reporting

The AML Compliance Person will report any suspicious transactions (including deposits and transfers) conducted or attempted by, at or through a Player account involving EUR 1,000 or more of funds (either individually or in the aggregate) where the AML Compliance Person knows, suspects or has reason to suspect:

- the Player is included on any list of individuals assumed associated with terrorism or on a sanctions list;
- the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade laws or regulations or to avoid any transaction reporting requirement under law or regulation;
- the transaction involves the use of the Company to facilitate criminal activity.