Anti Money Laundering Policy

Anti-Money Laundering (AML) Program and Compliance Procedures

1. Company Policy

1.1 Money laundering and the financing of terrorism are some of the ever-growing threats for national and international economies throughout the world, forcing all vulnerable sectors to have measures in place for the prevention of their misuse for these purposes. It is the policy of Triumphbet Company N.V. (the "**Company**") 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.

1.2 The Company is licensed and regulated by Antillephone N.V. to offer remote games over the internet, under the National Decree August 18, 1998 No. 14. Under the license conditions issued by Curaçao, 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.

1.3 The Company is committed to the highest national and international AML and CFT standards when providing its Services and requires management and employees to follow these standards.

2. Legal framework

National regulations

Pursuant to the National Ordinance of Money Laundering (1993), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others:

a) The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT) together will all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
c) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
d) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
e) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);
f) National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

International regulations

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting International standards by regularly implementing these standards in its national legislation.

On international level, the FATF plays a very important role in the combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction.
The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

2. Objective of the Policy

2.1 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.

2.2 The Company will endeavor 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.

2.3 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.

2.4 The Company is committed to the highest national and international AML and CFT standards when providing its Services and requires management and employees to follow these standards.

3. Player Identification Program

3.1 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.

3.2 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.

3.3 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 or verified phone number; and
- Player’s username and a password.

3.4 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 3,000 per occasion or when payments to the account are made in excess of EUR 3,000. These documents shall include, to the extent permitted under the relevant data protection regulations:

- A copy of a valid identity card or passport;
- Photo of Player holding a plain white piece of paper with domain name written on it or a identity card/passport.

3.5 In certain specific instances the Company will conduct Enhanced Due Diligence by requesting the following KYC information:

- A recently issued utility bill or bank statement
- A bank statement showing the initial deposit;
- A bank statement no older than 3 months from the bank to which a withdrawn amount should be deposited;
- Information regarding the source of wealth.

In addition, the Company may perform the following Enhanced Due Diligence checks:

- 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.

Enhanced Due Diligence is applied as soon as a Player is classified as a High risk including but not limited to the following situations:

- upon suspicion of a Player attempting to or having created multiple accounts in multiple different names;
- upon suspicion of Player(s) being part of a syndicate of Players colluding to gain an advantage over the Company;
- upon suspicion of the Player being a politically exposed person (PEP) or family or close associate thereof;
- at the detection of any irregular, suspicious, inappropriate or fraudulent activity;
- anytime, at the discretion of the Company.

3.7 The Company will inform relevant Players that the Company may seek identification information to verify their identity.

3.8 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 MLRO, 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.

3.10 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 MLRO will be notified so that it may be determined whether a report is to be sent to the relevant authorities.

3.11 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.

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

4. Continuous transaction due diligence

4.1 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.

4.2 Monitoring will be conducted through the following methods: Transactions will be automatically monitored and reviewed daily for all transactions above 1000 EURO along with all the details of the users making those transactions. Documents may be required at the determination of the MLRO.

4.3 The MLRO 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.

4.4 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.

4.5 When an employee of the Company detects any activity that may be suspicious, he or she will notify the MLRO. MLRO 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.

4.6 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.

4.7 The Company will only transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.

4.8 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 MLRO shall be responsible to review the relevant service agreement with the service provider to ensure the adequacy of the agreement.

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

5. The Money Laundering Reporting Officer (MLRO)

The Company has designated an MLRO who is in charge of the review of KYC information and the monitoring of Player account activities. Specifically, the MLRO is in charge of the following:

- Ensure a proper review of the Player accounts by the personnel in relation to identification and verification of an Account Owner,
- Keep a list of registered Players;
- Monitor the reviews and investigations conducted by the designated personnel performed on the Player Account activities;
- Provide initial and ongoing training to all relevant staff ensuring awareness of their personal responsibilities and the procedures in respect of identifying Players, monitoring Player activity, record-keeping and reporting any unusual/suspicious transactions as well as other relevant policies and procedures;
- Cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity;
- Ensure that this policy is adhered to, reviewed and maintained regularly.

6. Suspicious Transactions and Reporting

The MLRO 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 MLRO 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 has no ordinary lawful purpose or is not the sort in which the Player would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
- The transaction involves the use of the Company to facilitate criminal activity.

In such cases, the MLRO will report the transaction to the Curaçao FIU. The decision not to report will be sufficiently supported. In case the report is filed with the FIU or any internal investigation is taking place, the Player shall not receive any of this information.

7. Training Programs

6.1 The Company will develop ongoing employee training under the leadership of the MLRO and senior management. The training will occur on at least an annual basis. It will be based on the Company's size, its Player base, and its resources and be updated as necessary to reflect any new developments in the law.

6.2 The training will include, at a minimum:

- how to identify red flags and signs of money laundering that arise during the course of the employees' duties;

- what to do once the risk is identified (including how, when and to whom to escalate unusual Player activity or other red flags for analysis;
- what employees' roles are in the Company's compliance efforts and how to perform them;
- the Company's record retention policy;
- the disciplinary consequences for non-compliance with legislation.

8. Recordkeeping

The Company maintains a record of all relevant documentation on a separate database for at least five years after ending a business relationship. The Company is obliged to retain files in a way that enables investigating authorities to identify a satisfactory audit trail for individual transactions including the amounts, currencies and type of transactions.

In specific circumstances, if ordered by rule of law and permitted by national law and the relevant authorities, the Company may provide copies of the records maintained.

9. Staff Due Diligence

It is imperative that the Company's employees are of undisputed integrity. To ensure this objective, the Company follows a procedure whereby all applicants must produce a curriculum vitae, at least two references and relevant educational qualification certificates, and/or professional certificates, which are checked and verified by the Company's Human Resources Department.

10. Independent testing of procedures

The Company has systems in place in order to have independent testing and evaluation of the overall adequacy of the Company's AML procedures. This evaluation helps inform management of weakness, or areas in need of enhancements or stronger controls.

Signature: 

Signed by: Cindy Drommond o.b.o. EMS Management Services N.V. as Proxy Holder

Date of Signature: July 19, 2021

Approved by: EMS Management Services Compliance Department
Date of Approval: July 9, 2021