Cesario N.V.

Heelsumstraat 51, E-Commerce Park

Willemstad, Curaçao

AML/CFT MANUAL

October 2021

Table of Contents

Definitions and Abbreviations

Account Holder:

An individual who applied and was granted an account held at the internet gateway operated by the Company for the use of the provided Services.

AML:

Anti Money Laundering. All efforts focused on the prevention of transforming proceeds obtained from criminal activities into funds which appear to be obtained from legal activities.

CFT:

Combating the Finance of Terrorism. All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.
The Company Cesario N.V., a limited liability company under the laws of Curaçao, registered with the Chamber of Commerce of Curaçao under number 157212.

FATF:
Financial Action Task Force (www.fatf-gafi.org)

FIU:
Financial Intelligence Unit.

KYC:
Know Your Client

MLRO:
Money Laundering Reporting Officer

Non-reputable Jurisdiction:
Country mentioned on the list of the FATF as jurisdictions for which a call of action has been issued or are mentioned on the list of monitored jurisdictions.

High-Risk Jurisdiction:
Country identified as high-risk country by national or International authorities, such as the European Union and the FATF for having detrimental rules and practices in place

Which constitute weaknesses and impede international cooperation in the fight against money laundering a terrorism financing.

Player:
Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which an account has been opened providing him/her with a unique code.

Player Account:
An account granted to an individual after registration. The account is created and issued by the Company and is required for wagering with real money. Only one Player Account is permitted per person, per family and per Shared Environment.

Shared Environment:
An environment that has a common internet connection which includes but is not limited to airplanes, households, universities, libraries, cyber cafes, coffee shops and work forces.

Service:
The gaming and betting offers provided by the internet gateway operated by the Company to the Account Holder, through the Website.

Website:
the website is www.slotome.com
which are operated by the Company.

1. AML/CFT Policy

1.1 Policy

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.
The Company is committed to have procedures in place for the prevention of the misuse of its Services provided to Account Holders for money laundering, terrorism financing or other Criminal purposes such as fraud.

1.2 Objective

The Company is a limited liability company, duly incorporated and registered in accordance With the laws of Curacao. This policy is written based on the national legislation on AML, CFT and the penalization of predicate crimes of Curaçao and applicable international standards set by the FATF. Combined these regulations provide a solid, internationally accepted standard for the procedures maintained for the prevention of the misuse of the Services provided by the Company.
Proper Identification of Account Holders, verification of the identity, monitoring of Player activities and reporting of unusual activities are part of the measures the Company has in place in an effort to prevent, deter or mitigate industry related risks.

1.3 Scope

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. Regulatory Framework

2.1 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.

2.2 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.

Although Curaçao is not a EU member, the Company, in addition to the FATF rules, where applicable, adheres to AML rules issued in directives by the European Union. Subsequently the present policy is a combination of the FATF, EU 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.

3. Procedures

In an effort to be compliant with the applicable rules, regulations and international standards, the Company has procedures in place to which it attains itself to when providing Services to

Account Holders. These procedures cover the following standards:

Customer Due Diligence

- Know Your Client

- Due Diligence

- The Money Laundering Reporting officer

Risk Management

- Risk Classification

- Monitoring of Account Holder activities

Reporting of unusual transactions

Recordkeeping

3.1 Risk Management

Risk Classification
The Company maintains a risk-based approach in relation to its clients in order to effectively detect and deter any risks it may be exposed to such as money laundering, the financing of terrorism or any prohibited transaction such as fraud.

The Company maintains the following risk classification:

- Low risk

- High risk

Low risk

All Players are classified as Low risk and are subjected to Standard Due Diligence procedures related to the request for KYC documentation as per the process described above and constant monitoring of activities on the account.

High Risk

The Player activity is the determining factor for the classification of a Player as High Risk. Any Player of which an automated alert has been generated or an inappropriate activity has been detected will be categorized as High Risk, for which an Enhanced Due diligence procedure is applied. The instances in which a High risk classification is assigned includes but are not limited to those Customer Due Diligence

3.2 Know Your Customer (KYC)

3.2.1 Identification & verification

Following international standards and local applicable legislation, it is imperative for a company to know its clients. A sound KYC policy and procedure are critical in protecting the safety and soundness of a company and the financial system. In line herewith the Company has the following procedures in place.

KYC information request

An individual cannot participate in a game for money unless that individual has registered and has been provided with a Player Account. Only one Player Account is permitted per person, per family and per Shared Environment.
To be registered as a Player, an individual must register personally and submit the following

KYC information:

a. date of birth together with valid identification showing that he/ she is over eighteen (18) years of age or the applicable legal age of majority as stipulated in the jurisdiction of your residence. Identification documents which must be submitted include copy of a valid Passport, copy of other identification paper and a proof of address;

b. Player's first and last name;
c. Player's full residential address;
d. Player's valid email address;
e. payment details; and
f. a username and a password

On registration, a geographical location check is carried out on the applicant's computer IP to ensure that person is in a permitted jurisdiction. If the applicant is not in a permitted jurisdiction, he/she will not be allowed to continue the registration process. The Company proceeds to review the information provided and may request additional documentation in order to verify the provided information. The Player Account may be put on hold until satisfactory information has been received or terminated if the Company finds the information contained in the Player Account to be false or misleading.
The Company reserves the right to refuse to open or close a Player Account at its own discretion following review of the provided KYC information.

Log in details

It is not permitted for a Player to share the login details to access the system with a 3rd party. The Company reserves the right to cancel, without refund, a Player Account if the login details were disclosed to a 3rd party.

3.2.2 Due Diligence

Standard Due Diligence

The Company requests the following information to verify the identity of the Player:
1. A driver's license or valid passport;
2. A recently issued copy of a utility bill or bank statement

Standard Due Diligence is conducted in the following cases:

- Anytime during the Player onboarding;
- upon a request for withdrawal;
- when a threshold of a cumulative withdrawal of 2,000 €/ $ or equivalent is reached;
- anytime at the discretion of the Company.

The Company further reserves the right to conduct a phone verification of the Player Account to verify details provided by the Player at the time of registration or at any other time requested by the Company. The details include but are not limited to name, home address, email of the registered Player Account holder, phone number, photo ID, payment methods, bet types, amounts and event details. Failure to satisfactorily complete this verification due to the previously provided details being fake, false, incorrect, misleading, non-existing, not belonging to the Player or unable to be verified, may result in the Company closing the Player Account and the confiscation of any winnings.

Enhanced Due Diligence

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

1. A driver's license or valid passport;
2. A selfie of the Player holding the identification document;
3. A recently issued utility bill or bank statement
4. A bank statement showing the initial deposit;
5. A bank statement no older than 3 months from the bank to which a withdrawn amount should be deposited;
6. Information regarding the source of wealth.

Enhanced Due Diligence is applied as soon as a Player is classified as a High risk including but not limited to the following situations and as further discussed in the section 'Monitoring of Account Holder activities:

a) if the Player is a national of a High-Risk Country, or the geographical location check at onboarding shows that the Player is residing in a Non-reputable or High-Risk Jurisdiction;
b) upon suspicion of a Player attempting to or having created multiple Player Accounts in multiple different names;
c) upon suspicion of Player(s) being part of a syndicate of Players colluding to gain an advantage over the Company;

d) Upon suspicion of the Player being a politically exposed person (PEP);
e) at the detection of any irregular, suspicious, inappropriate or fraudulent activity;
f) anytime, at the discretion of the Company.

If the Company is not able to verify the identity of the Player based on the provided documentation and further efforts, the Company reserves the right to put the Player Account on hold pending the provision of verification information, or to terminate the account if it finds the information contained in the Player Account to be false or misleading.

3.2.3 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 Account Holders;
- 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;
- 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.
Instances as mentioned in the section Monitoring of Account Holder activities below.

3.2.4 The Monitoring of Account Holder activities

Designated personnel will conduct the reviews and the monitoring of the Player Accounts and will further conduct investigations in case any irregular activities are detected.
Security technology are in place generating automated alerts which are thereafter thoroughly investigated by the department.
The presence of any irregular, suspicious, inappropriate or fraudulent activity or any attempt thereto, will cause the pertaining Player to be classified as High risk for which EDD procedures are implemented.

Player accounts are reviewed and monitored for the presence of any of the following situations:
- the provision of fake, false, incorrect, misleading, non-existing, KYC information which do not belong to the Player or are unable to be verified;
- provision of fictitious names such that the true beneficial owner is not known;
- the detection of inappropriate play and/ or fraudulent activity;
- the detection of irregular Player activity including but not limited to the placing of zerorisk or even bets;

- complex or large transactions or groups of transactions which are likely, by their nature to be related to money laundering or the funding of terrorism
- upon suspicion of a Player attempting to or having created multiple Player 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;
- at the detection of any irregular, suspicious, inappropriate or fraudulent activity;
- anytime, at the discretion of the Company
- fraudulent or unlawful use of the system by Players, in an attempt to break into or otherwise circumvent the security measures set up by the system;
- The use of any software program endowed with Artificial Intelligence;
- attempt to log in from a Non-reputable Jurisdiction or a High Risk Jurisdiction.

Specific attention is paid to the following instances:

Multiple accounts

Only one Player Account is permitted per person, per family and per Shared Environment. If more than one Player Account is created per person, house, building, mailing address, phone number, IP address, family, Device or Shared Environment then all related Player Accounts will be closed. No winnings, refund nor deposits, will be paid out.
Family includes, but is not limited
to, parents, partners, spouse, children, siblings and close relatives.

If the suspicion arises that multiple Player Accounts have been created in multiple different names or that a Player Account is a part of a syndicate of Players colluding to gain an advantage over the Company, the Company will proceed to suspend all suspicious Player

Accounts pending an investigation. The investigation will consist of the review of playing history, IP location histories including VPN and proxy databases and action to delay ratios commonly displayed with computer sharing technology. If the Company concludes from the investigation that an Account Holder or a group of Account Holders have created multiple accounts and are playing as part of a syndicate of Players, the Company will proceed to withhold any cash or bonus winnings and reserves the right to withhold deposited funds.

Whenever an Account Holder requests for a withdrawal of funds from his/ her account, the system will check the presence of multiple accounts and further checks whether the Account Holder has used a false proxy. At the presence of multiple accounts, all the accounts will be closed, and the Account Holder will be denied the opening of a new account.

Unusual activities

If an Account Holder has unusual deposits and gets flagged by the system, the Company will perform an investigation in which the Account Holder may be requested to provide further information. The Company will suspend the account until further documentation is in place. If the Account Holder has not provided satisfying information within 30 days, the account will be terminated. The MLRO will proceed with the reporting of the unusual transaction to the relevant authority.

Withdrawal or Pay out of funds

The Company has established the following procedures with regards to the withdrawal or pay out of funds.

Request for withdrawal

Withdrawal requests must be made from a Player Account. Withdrawal requests sent by any other means of communication will not be processed. Upon receipt of a request for withdrawal, the Company will request KYC documentation verifying the identity of the Player.

The Company will not deposit withdrawn funds to another source from which it was originated. If for any reason this is no longer possible, the Company will request additional verification documentation evidencing the details and ownership of the new withdrawal method.
Transfers or pay outs will only be made to the Player. Transfers to third parties are not permitted.

Prior review of account activity

Before processing any withdrawals, the Company will conduct additional review of the Player Account for any irregular activity such as money laundering or suspicious play such as:

- The placement of a deposit without having placed any bets, or only to receive free spins. A Player must have always placed at least his deposit amount in bets before proceeding to withdraw the funds;
- the possible creation of multiple Player Accounts in multiple different names;
- possible collusion between Players.

Upon the occurrence of any of the instances mentioned above, the Company may decide to withhold funds and proceed to further request EDD documentation or conduct further investigation and resolve to:
- suspend the Player Account until receipt of sufficient verification information, where still applicable;
- immediately block the access of a Player to the system or to his/ her account and seize all funds held in the account;
- close or terminate a Player Account and seize all funds held in such account,

Followed by the report of the activity to the relevant authority as further described below.

1. Transactions using Cryptocurrency

Cryptocurrency transactions are only possible if the initial deposit was made with a crypto currency. Following this transaction all transactions (deposits, wagers and payout) with the Player must be conducted using the same crypto currency as with the first deposit.
The Company will at no time sell/buy/exchange crypto currency with and/or to FIAT currency.
The Company is bound by the following requirements as set by the Master License Holder:
- Collect and verify proof of identity and proof of address as described above in the 'Client Due Diligence' paragraph and to make sure that a Player is over 18 years of age;

- Collection and storage of hardware KYC in all pathways from signup, login, deposits and withdrawals, including but not limited to IP address, mac address and browser information to ensure that all wagering, deposits and withdrawals are to/from the same

Player (IP and computer);
- The Company will make available to the Master License holder on demand and provide proof of balance as acceptable by the Master License Holder, to ensure Player's funds have been deposited;
- Provide proof of Solvency to the Master License Holder on a periodic basis (weekly, monthly) to ensure that operator has all funds to cover all bets and jackpots and that the crypto currency is kept in a separate account.
- The Company will display the rate of exchange from crypto currencies to FIAT currency on the home page of the Website. In no way shall the Company make exchanges between any crypto currency and any FIAT currency.
- The Company must include in their Terms and Conditions and highlights that crypto currency values can change dramatically depending on the market value.
It is important to note that due to the current anti-money-laundering regulations, the Player may deposit money into the Player Account only in order to play and to use the Services. Likewise, the Player may only withdraw winnings and not the funds deposited into the Player Account. Players who deposit and withdraw without gaming activities will have their funds blocked until further notice. The Company is not a financial institution and does not grant interest on deposits. In any case, the Company reserves the unlimited right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

Notification of new payment methods will be made on the homepage of the Website and sent by e-mail to the Account Holders as they are added. For each new depositing method, this Manual and the Terms and Conditions on the Website will be updated accordingly.

3.2.5 Security review

The Company reserves the right to conduct a review at any time to validate the identity, age and/or registration data provided by the Account Holder in order to verify the use by the Customer of the provided services for any breach of the Terms and Conditions and any applicable laws. At the moment of registration the applicant provides the Company with authorization to make any relevant inquiries pertaining to his person and to use and disclose information to any third party considered necessary in order to conduct its verification checks. Third party agencies may be engaged in an effort to confirm the provided age, identity, address and payment details, the ordering of a credit report and/ or the verification of the provided information by checking it against certain public or private databases. All applicant/ Account holders are made aware that by accepting the Terms and Conditions of the Company, they agree that the provided information may be used, recorded and disclosed and that the data may be recorded by the Company or third party engaged.
The review may be performed from time to time at the discretion of the Company and/or due to regulatory, security or other business reasons,

During the review the Customer may be restricted from withdrawing funds from the account and/ or prevented from accessing certain Services offered on the website.

3.3 Reporting of unusual transactions

Any transactions or circumstances for which the Company has not received sufficient verifying information for and/or of which the Company knows, suspects or has reason to suspect that any of the transaction(s), among other actions, (i) involve funds derived from illegal activities, (ii)are intended to conceal funds from illegal activities, or (iii) involve the use of the Company system to facilitate criminal activity, may give rise to its report to the FIU in Curaçao. The Money Laundering Reporting Officer (MLRO) is in charge of the reporting with the relevant authority and will hold a list of all instances in which it did not consider it necessary to report. The decision not to report will be sufficiently supported.

3.4 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.

3.5 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.