

AML/CFT Policy

NewGenx N.V.

Table of Contents

INTRODUCTION	3
WHAT IS MONEY LAUNDERING?	3
APPLICABILITY TO NEWGENX AND ITS STAFF	4
1. POLICY STATEMENT	4
2. PURPOSE	4
3. AUDIENCE	5
4. DEFINITIONS.....	5
5. POLICY IMPLEMENTATION	6
5.1 BUSINESS RISK ASSESSMENT	7
5.2 CUSTOMER RISK ASSESSMENT	8
5.3 CUSTOMER ACCEPTANCE POLICY	8
5.4 CUSTOMER DUE DILIGENCE.....	10
RETENTION OF CDD DOCUMENTATION	11
5.3.1 IDENTIFICATION AND VERIFICATION OF THE PLAYER.....	11
POLITICALLY EXPOSED PERSONS	12
5.4 ONGOING MONITORING	12
5.6 RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE.	13
5.8 ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	14
6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	16

AML Policy

Revision	Date	Responsible Person	Security
v 1.0	15.08.2017	MRLO	Confidential
v 2.0	01.01.2021	MRLO	Confidential
V 3.0	16.05.2025	MRLO	Confidential

Introduction

This policy outlines the anti-money laundering (AML) and counter-terrorist financing (CTF) framework for all entities within the NEWGENX Group, including all subsidiary companies. It is based on the European Union's Sixth Anti-Money Laundering Directive (6AMLD) and, where applicable, references UK regulations for guidance. In the event of any conflict between national laws and regulations, NEWGENX will adhere to the most stringent applicable regulatory standard to ensure maximum compliance.

WHAT IS MONEY LAUNDERING?

Money laundering is the process of concealing the illicit origin of funds generated through criminal activities by integrating them into the legitimate financial system. This typically involves three key stages:

- **Placement:** introducing illegal funds into the financial system;
- **Layering:** conducting complex transactions to obscure the origin of the money;
- **Integration:** reintroducing the laundered money into the economy as apparently legitimate assets.

According to the **Sixth Anti-Money Laundering Directive (6AMLD)** of the European Union, money laundering offences include:

- **Concealing or disguising** the origin, nature, location, disposition, movement, or ownership of criminal property;
- **Converting or transferring** criminal property, with the aim of concealing its illicit origin or assisting any person involved in the offence to evade legal consequences;
- **Acquiring, possessing, or using** property, knowing that it is derived from criminal activity;
- **Aiding and abetting, inciting, or attempting** to commit any of the above acts.

6AMLD also introduces tougher penalties and expands criminal liability to include **legal persons** (e.g., companies), not just individuals.

Furthermore, **failure to report suspicions** of money laundering and **"tipping off"**—informing individuals involved in suspicious activity in a way that could compromise an investigation—are also considered offences under many AML frameworks.

These regulations aim to harmonize the definition of money laundering across EU member states and strengthen the overall framework for combating financial crime.

APPLICABILITY TO NEWGENX AND ITS STAFF

This policy is applicable to all NEWGENX entities, including all subsidiary companies.

This Policy sets out, among other things, the systems and processes put in place by NEWGENX to manage and effectively mitigate the risks of money laundering and terrorist financing, and how NEWGENX staff should formally raise concerns—in writing to the Managing Director and Head of Compliance—if they suspect money laundering or inadvertently become involved in it in the course of their NEWGENX activities. Staff have a positive obligation to act should they suspect or become involved in money laundering; doing nothing is not an option and may result in personal criminal liability if they fail to report money laundering when they suspect, or have reasonable grounds to suspect, that it is taking place.

In cases where national regulations may conflict or vary, NEWGENX will always adhere to the **most stringent applicable regulatory standard**, in line with international best practices, to ensure the highest level of compliance and risk mitigation.

1. Policy Statement

NEWGENX is fully committed to implementing and maintaining robust policies, controls, and procedures designed to identify, assess, manage, and effectively mitigate the risks of money laundering and terrorist financing. These measures are subject to regular review and continuous improvement to ensure they remain appropriate, effective, and aligned with applicable legal and regulatory standards.

Key components of NEWGENX's framework include:

- **Risk Management Practices:** Comprehensive methodologies to prevent the misuse of NEWGENX's services for money laundering or terrorist financing purposes.
- **Customer Due Diligence (CDD):** Standard and enhanced due diligence procedures, particularly for high-risk customers such as Politically Exposed Persons (PEPs).
- **Internal Controls:** Governance measures applicable to senior management and staff to ensure accountability and regulatory compliance.
- **Independent Audit Function:** Periodic, objective evaluations of the effectiveness of the company's AML/CTF policies, controls, and procedures.
- **Record-Keeping:** Maintenance of accurate and complete records in accordance with legal and regulatory requirements.
- **Ongoing Monitoring and Training:** Continuous monitoring of compliance with internal policies and procedures, and ensuring these are clearly communicated to all relevant personnel.

2. Purpose

The purpose of this Policy is to provide guidance on the company's approach to combating AML/CTF, in order to ensure full compliance with the relevant legislation.

This policy is based on the following legal provisions:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

3. Audience

This policy applies to all activities, services, products, and Employees of the Company, including the Company's officers, directors, full-time Employees, part-time Employees, temporary Employees, or contractors employed by the Company or affiliates of the Company, as well as the Company's third-party service providers as relevant. Such individuals will be provided with regular training to ensure awareness of this policy and their obligations under it, at least on an annual basis or more frequently as required. All employees are also expected to familiarize themselves with the third-party vendors engaged by the Company to assist in AML activities related -shore games of chance and wagering, through the internet in compliance with the regulations of the Government of Curaçao.

4. Definitions

- Money Laundering: All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering. Money laundering may generally occur in three phases.
 - Placement; The physical disposal of cash or other assets derived from criminal activity. During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos, and other legitimate businesses, both domestic and international. Examples of placement transactions include the following: Blending of

funds, purchasing significant stored value cards with currency , Foreign exchange , Breaking up amounts.

- Layering: The funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.
 - Integration; The funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses
-
- Compliance Officer A officer independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.
 - MLRO: A term used in various international rules to refer to the person responsible for overseeing a firm's anti-money laundering activities and program and for filing reports of suspicious transactions with the national FIU. The MLRO is the key person in the implementation of anti- money laundering strategies and policies. The Company has appointed a Money Laundering Reporting Officer (MLRO) to serve as the designated recipient of internal disclosures related to suspected money laundering activities and to oversee the Group's anti-money laundering (AML) framework. The MLRO, who also serves as the Group Head of Compliance, is **Xecutive Corporate Management**, which also acts in the capacity of directors of the Company.
 - The MLRO is responsible for:
 - Ensuring the implementation and ongoing enhancement of effective AML systems and processes across all NEWGENX entities;
 - Providing appropriate AML training and awareness to both new and existing employees, with regular reviews and updates to reflect evolving risks and regulatory requirements;
 - Promoting a culture of compliance and ensuring that all staff understand their obligations in preventing the misuse of the business for money laundering or terrorist financing purposes.
-
- Financing of Terrorism: Is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.
 - Unusual Transactions: These are transactions whose amount, characteristics, or frequency do not match the customer's profile.

5. Policy Implementation

The Company is committed to full compliance with all applicable laws, regulations, and directives aimed at preventing money laundering (ML), terrorist financing (TF), financing of

proliferation (FP), sanctions violations, and related criminal activity. The Company will not knowingly engage in, facilitate, or support any transactions or business relationships that:

- Involve individuals, entities, or jurisdictions listed under sanctions regimes issued by the United States (US), United Nations (UN), or European Union (EU);
- Are associated with countries or regions subject to comprehensive US sanctions;
- Involve counterparties or jurisdictions flagged in partner-imposed prohibited country lists or internal watchlists

To effectively manage and mitigate ML/TF/FP and related risks, the Company employs a four-stage, risk-based approach:

A. Identification:

- Evaluate and assess the Company's products, services, customer segments, delivery channels, and geographies to determine potential exposure to ML/TF/FP risks.

B. Documentation:

- Maintain comprehensive and accessible documentation of internal policies and procedures.
- Ensure staff are trained to recognize risk indicators and know the proper escalation and reporting protocols for suspicious or unusual activities.

C. Mitigation

- Design and implement robust internal controls and preventive measures, including due diligence, transaction screening, and customer risk assessments.
- Deploy detection mechanisms to flag potential instances of criminal conduct and ensure timely reporting to the relevant authorities.

D. Monitoring

- Conduct continuous monitoring of identified risks and mitigation measures.
- Regularly review and update controls in response to emerging threats, regulatory changes, and business developments

5.1 Business Risk Assessment

The Company conducts a comprehensive Business Risk Assessment (BRA) to identify and evaluate its exposure to ML, TF, FP and sanctions risks. The assessment ensures that AML/CFT controls are commensurate with the risks associated with the Company's operations, products, services, customer base, and geographical footprint.

The BRA is reviewed annually and upon any material change to business operations or regulatory obligations. The BRA includes the following key areas:

Product and Service Risk: Evaluation of the ML/TF risks inherent in the Company's gaming offerings (e.g., online poker, sports betting, and virtual currency). Particular focus is placed on features allowing for rapid fund movement or cashout without proportional gameplay.

Customer Risk: Classification of customers by risk levels based on geographic origin, payment behavior, funding methods, and whether they are high-net-worth individuals, Politically Exposed Persons (PEPs), or associated with high-risk industries.

Geographic Risk: Analysis of exposure to countries listed by FATF, OFAC, or other relevant authorities as non-cooperative or high-risk, as well as jurisdictions with weak AML/CFT systems or under international sanctions.

Transactional Behavior Risk: Detection of patterns such as minimal gaming activity before large withdrawals, unusual use of bonuses, or frequent account top-ups followed by inactivity. Findings from the BRA are documented and used to inform risk-based procedures and customer due diligence protocols. The effectiveness of controls derived from this assessment is validated through internal audits, transaction monitoring results, and independent testing.

5.2 Customer Risk Assessment

The Customer Risk Assessment (CRA) is an essential element of the Company's risk-based approach, aimed at evaluating the ML/TF risk posed by individual customers. It informs the level of due diligence, ongoing monitoring, and other controls applied to each customer. Each customer is assigned a risk rating (Low, Medium, High, or Very High) based on a set of risk indicators:

Identification and Verification Data: Including full name, address, date of birth, and documentary or non-documentary verification.

Behavioral Factors: Transaction volumes, frequency of deposits and withdrawals, and patterns of gameplay versus monetary activity.

Geographic Indicators: Whether the customer is based in or connected to high-risk or sanctioned jurisdictions.

Payment and Funding Sources: Use of crypto-assets, pre-paid cards, or anonymous funding methods increase risk; documented employment income or regulated bank transfers lower risk.

Third-party Data: Alerts or insights from vendors (sanctions and PEP screening, blockchain transaction tracing).

CRA is initiated at account creation and continuously updated based on the customer's activity and external inputs. Triggers for re-evaluation include:

- Cumulative deposits exceeding defined thresholds (e.g., \$2,000 or Cg. 4,000, whichever is less).
- Document KYC Verification.
- Attempted withdrawals or redemptions.
- Alerts from internal or third-party systems.

High-risk customers undergo Enhanced Due Diligence (EDD), including documentation on source of wealth and intended usage of the platform.

The CRA informs decisions on whether to escalate accounts, impose restrictions, or file unusual transactions to the FIU.

5.3 Customer Acceptance Policy

The Customer Acceptance Policy (CAP) sets forth the onboarding requirements and thresholds for escalating due diligence procedures based on CRA outcomes. The Company uses a three tiered Customer Identification and Verification system:

Level 1: Account Creation Required: Email address. Purpose: Establish account credentials and provide CIP notification. Limitations: No monetary transactions permitted.

Level 2: Customer Due Diligence (CDD) Triggered by: First attempted deposit or wager. Required Information:

- First and Last Name
- Phone Number
- Full Residential Address (no P.O. Boxes; APO/FPO acceptable)
- Date of Birth
- Government-issued ID Verification (subject to specific policies and management's discretion); The user-provided information must be verifiable by third-party vendors (including Sardine A.I. and Chainalysis) prior to transacting above the prescribed limits and can be provided in two ways: either as photos of government issues, unexpired IDs/selfie uploads (documentary), or as text inputs (non-documentary) when made available.

Level 3: Enhanced Due Diligence (EDD) Triggered by:

- Withdrawal attempts or redemptions
 - Cumulative deposits exceeding \$2,000 or (Cg. 4,000, whichever is less)
 - Behavioral red flags or vendor alerts
- Additional Requirements:
- Documentary proof of address (e.g., utility bill or bank statement)
 - Source of wealth/income documentation for high-risk accounts, if applicable
 - Explanation of transactional behavior or relationships, if applicable
- All KYC information must be verifiable via approved third-party providers before the customer is allowed to transact beyond set limits

Restricted Jurisdictions

The Company prohibits customers from countries under comprehensive sanctions and on the FATF's High-Risk Jurisdictions subject to a Call for Action list (e.g., Iran, North Korea, Syria, Myanmar) and maintains:

- A Non-Supported Countries List
- A Prohibited Jurisdictions List for monitoring and reference

Account Escalation and Review

High-risk accounts are subject to Compliance approval.

Customers that are classified as PEP are per default considered high risk customers. PEPs are subject to management approval.

The term "Politically Exposed Persons" is broad and generally includes all persons who fulfill a prominent public function. This includes:

- i. Heads of State, Heads of Government, Ministers, Deputy and Assistant Ministers, and Parliamentary Secretaries;
- ii. Members of Parliament;
- iii. Members of the Courts of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- iv. Members of courts of auditors, Audit Committees or of the boards of central banks;
- v. Ambassadors, charge d'affaires and other high-ranking officers in the armed forces; and

vi. Members of the administration, management or boards of State-owned corporations.

The term “immediate family members” of PEPs includes:

- i. The spouse, or any partner recognized by national law as equivalent to the spouse;
- ii. The children and their spouses or partners; and
- iii. The parents.

5.4 Customer Due Diligence

The Company is prohibited from keeping anonymous accounts or accounts in obviously fictitious names. It must identify the player and ask for the player’s name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge, the Company may not establish or maintain a business relationship or carry out occasional transactions. A sound CDD program is the best way to prevent AML, TF & FP.

The customer’s risk profile is essential to apply a certain level of CDD commensurate to the identified ML/TF risk. The purpose of collecting information is 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. Such an assessment is necessary in order to detect deviations from the expected behavior, which are reported to the FIU.

The obligation to undertake CDD measures when:

- 1. players engage in financial transactions equal to or above Naf. 4,000;
- 2. carrying out occasional transactions² above the monetary equivalent of NAf. 4,000³;
- 3. there is a suspicion of money laundering or terrorist financing; or
- 4. they have doubts about the veracity or adequacy of previously obtained customer identification data.

Note: a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of EUR 2,000.

For transaction above the monetary equivalent of EUR 2,000, CDD measures are applied immediately. Whether the transaction is carried out in a single operation or in several operations which appear to be linked. Transactions are considered as linked if they are carried out by the same customer through the same game or in one gaming session. A transaction consists of the wagering of a stake or the collection of winnings.

The CDD measures to be taken are as follows:

- a. Identifying the player documents, data or information;
- b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

d. 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 casino's knowledge of the player, its business and risk profile, including, where necessary, its source of funds.

RETENTION OF CDD DOCUMENTATION

In accordance with **Regulation 40 of the 2017 Money Laundering Regulations**, NEWGENX will retain copies of all customer due diligence documentation collected at the time of onboarding. These records—including identification documents, proof of address, and any supporting compliance materials—will be retained for a minimum period of **five (5) years** following the **date of the customer's last transaction** with NEWGENX.

All documentation and personal data collected will be processed and stored solely for **internal compliance purposes**, including the prevention of money laundering and terrorist financing, and will be handled in accordance with applicable data protection laws and retention policies.

5.3.1 Identification and Verification of the Player

Identification refers to the collection of personal details of the player to establish the identity of the player. Verification, on the other hand, consists of confirming the personal details collected for identification purposes using reliable, independent source documents, data or information. The personal information required and extent of verification to be carried out, will vary depending on risk.

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; and
- vi. identity number.

However, in low risk scenarios licensees may limit identification to the three personal details set out in (i) to (iii) above. On the other hand, in high risk situations, it is possible that a licensee considers the collection of additional personal details as necessary to mitigate the higher risk of ML/FT.

In addition, **proof of residential address** is required. Acceptable documents (dated within the last 3 months) include:

- Utility bill (excluding mobile phone bills)
- Full driving licence (if not already used as ID)
- Council tax bill
- Television licence
- Insurance policy (home or motor)

Where such a document does not allow verification of the player's residential address, NewGenX can obtain other documents like a bank statement, utility bill⁵, letter from a public authority or rental agreement, which should not be more than six months old, to verify the residential address. The casino can also contact the player by letter, e-mail or telephone to verify the information supplied.

POLITICALLY EXPOSED PERSONS

Politically Exposed Persons (PEPs) are defined under **Regulation 35 of the 2017 Money Laundering Regulations** as individuals who are, or have been, entrusted with prominent public functions. This includes:

- Heads of state or government;
- Senior politicians (e.g., members of parliament);
- Senior officials in government, judiciary, or military;
- Ambassadors and high-ranking diplomatic personnel;
- Senior executives of state-owned enterprises;
- Immediate family members and close associates of the above individuals.

Due to their position and potential access to public funds or influence, PEPs are considered to present a **higher risk** of involvement in money laundering or corruption. Therefore, **enhanced due diligence (EDD)** is required at both the onboarding stage and throughout the duration of the business relationship.

If a **PEP status** is identified through screening (e.g., via Onfido), the following steps must be taken:

- The individual **may not be onboarded** without **prior written approval** from both the Managing Director and the Head of Compliance;
- The prospective customer must provide detailed and verifiable information regarding their **source of wealth**, including:
 - Their current salary and other sources of income;
 - Their liquid assets, such as cash holdings and investment portfolios.

This information is necessary to establish the **legitimacy of the customer's financial resources** and to provide adequate context for any future transactions conducted through NEWGENX.

5.4 Ongoing Monitoring

In accordance with **Regulation 27(8) of the 2017 Money Laundering Regulations**, NEWGENX must apply ongoing customer due diligence (CDD) to existing clients at appropriate intervals, using a **risk-based approach**.

This review may be **triggered either periodically** or by specific risk indicators and involves a qualitative and/or quantitative reassessment of the customer's activity and profile.

Ongoing CDD is required in any of the following circumstances:

- A staff member becomes aware of **changes in a customer's circumstances** that could alter the initial assessment of money laundering or terrorist financing risk;
- There is reason to believe that the **identity of the customer** or a **beneficial owner** has changed;
- The customer engages in **transaction patterns inconsistent** with previous business behaviour or expected activity;
- There is a **change in the purpose or intended nature** of the relationship between NEWGENX and the customer;

- Other **events or observations** emerge that may influence NEWGENX's risk assessment of that client.
- **Red Flags Requiring Immediate Escalation**

The following are examples (non-exhaustive) of red flags that require attention and possible escalation:

- **Mismatch between account holder and sender:** If funds are received from a bank account not registered in the name of the client, trading must be halted. The client should be contacted for clarification. In joint account scenarios, full KYC must be conducted on all account holders. No refunds should be processed without approval from the Head of Compliance, in order to avoid a potential **tipping-off** offence;
- **Requests to trade using cash:** NEWGENX enforces a **strict no-cash policy** under all circumstances;
- **Third-party wallets:** If cryptocurrency is sent from or requested to be sent to a wallet not belonging to the client, this must be escalated for further investigation;
- **Unusual trading patterns:** One-off or sudden large trades, or a rapid sequence of high-value transactions inconsistent with historical activity, should trigger enhanced scrutiny;
- **Any suspicious behaviour:** Any activity or circumstance that raises concern should be immediately reported to the **Managing Director** or **Head of Compliance**.

These measures are essential for maintaining an effective AML/CTF compliance programme and for preventing inadvertent facilitation of illicit activity.

5.6 Reliance on third parties to perform customer due diligence.

Describe if the operator relies on third parties for CDD and how that is arranged.

5.7 Reporting of unusual transactions.

The Company will report any unusual transactions to the Curacao FIU if they're believed to be involved in potential money laundering. To protect the Compliance department, the AML Compliance Person ensures The Company personnel can report violations of the Program anonymously. Employees engaging with customers or accessing customer information will receive anti-money laundering (AML) training to recognize unusual or potentially suspicious behaviors. If employees suspect involvement with proceeds of crime, they must submit an Internal Unusual Activity Report (IUAR) to the AML Compliance Person within 24 hours. The AML Compliance Person will investigate and determine if a report to the Financial Intelligence Unit (FIU) of Curaçao is warranted within 48 hours.

The Company staff will be trained to identify unusual transactions based on customer profiles and specific indicators. All unusual transactions must be reported to the CO in an approved format, accompanied by supporting documentation.

Unusual transactions include:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);

- c. A transaction amounting to Cg. 5,000.00 or more (equivalent EUR 2,450), regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 - 1. A cashless transaction in the amount of Cg. 5,000.00 or more.
 - 2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 - 3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 - 4. A cash out in the amount of Cg. 5,000.00 or more;
 - 5. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as “objective indicators”, while (d) is referred to as “subjective indicator”. While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

The AML Compliance Person further ensures that this mechanism is well publicized to all personnel and will take necessary steps to ensure reports of potential violations remain anonymous and confidential. Regardless of whether a report is made anonymously, The Company has zero tolerance for retaliation against an employee for reporting a potential violation up to and including termination. All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

Further, the Company will retain copies of all actions, decisions, and processes outlined in this document for a minimum of seven years. The records will be electronically stored, to be printed as a hard copy when necessary. The records will also be organized in a manner that facilitates easy retrieval to enable reporting to the Curacao FIU without undue delay.

5.8 Anti-Money Laundering Compliance Program

The Company maintains proper internal controls to mitigate risks targeted by the Program with focus on customer identification and transaction monitoring. The Company has implemented the following internal controls to mitigate risks targeted by the Program: (i) KYC Program; (ii) Transaction Monitoring; (iii) Sanctions and Prohibited Jurisdictions; (iv) Fraud Prevention; (v) Employee training; (vi) Independent Testing.

- **Know Your Customer Program** – The Company has established, documented, and maintains a KYC Program. The Company will: (1) collect certain identification information from each customer; (2) utilize risk-based measures to verify the identity of each customer; (3) record

customer identification information and the verification methods and results.

Each customer of the Company will be initially screened at onboarding and periodically thereafter for as long as they remain a customer.

- **Transaction Monitoring** – is executed to prevent involvement of the Company with ML/TF and to safeguard the reputation of the Company. While in conducting ongoing scrutiny of transactions there are transactions that are not consistent with what it is expected from the customer, the Company establishes the source of the funds used for that transaction. The Company must obtain sufficient information and documentation with regard to the transaction to determine the reason for this deviation. If needed, the risk profile of the customer may have to be revised. After receiving this information, the Company decides whether the transaction is an unusual and needs to be reported to the FIU.

The level of on-going monitoring depends on the risk profile of the customer, but even in low-risk situations there is a degree of oversight to ensure that the business relationship is still considered as a low risk one.

The Company conducts ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the Company's knowledge of the customer, the customer's business and risk profile.

-Sanctions and Prohibited Jurisdictions - The Company is committed to complying with all applicable sanctions, including U.S. UN, and EU sanctions, by taking the following measures:

- a. prohibition of individuals or entities listed on applicable assets freeze lists, such as the US list of specially designated nationals and block persons, the EU consolidated list of financial sanctions targets, or any list maintained by any relevant authority;
- b. prohibition of entities owned or controlled by entities on the lists referred above;
- c. we prohibit and restrict Users in certain countries or territories. For example, US Persons are generally prohibited from dealing with Cuba, Iran, Syria, North Korea, and Crimea ("**Restricted Territories**")

The Company will have in place a process to freeze and block accounts of all customers that are a confirmed sanctions match, and will escalate those customers to business partners requiring such escalations within 24 hours.

- **Fraud Prevention** – the compliance program is focused to systemically detect, deter, and mitigate fraudulent activities. Involving a combination of policies, procedures, technology, and education to protect against fraud and related crimes.
- **Employee Training and Reporting Guide**

It is required that all new employees subject to this policy, receive AML/OFAC training at least annually, New Employees are assigned to the training as a part of the onboarding process. Employees that are delinquent may be subject to disciplinary actions. Relevant employees include those responsible for the following:

- i. customer onboarding and due diligence (including high-risk customer monitoring;

- ii. monitoring customer transactions and electronic fund transfers;
- iii. addressing customer queries or concerns (customer service teams); and
- iv. technology functions related to AML activities.

The AML Compliance Person is responsible for developing a risk-based training program and ensuring that staff members requiring advanced training due to their job description and/or responsibilities within the Company receive such training. A training log will be maintained.

vi. Independent Testing

The Company will conduct independent testing on the Company's AML program on a periodic basis, and no less than twice annually. When conducted, the review will assess the implementation and effectiveness of the Company's AML/OFAC program and the adequacy of controls over any related risks. The Compliance Officer is responsible for updating the Company's risk assessment in regards to any issues raised during the independent testing and taking necessary corrective actions and remediate findings. Independent testing has not yet been conducted on the program but the decision to test will be determined at a later date.

v. Employee Training and Reporting Guide

It is required that all new employees subject to this policy, receive AML/OFAC training at least annually, New Employees are assigned to the training as a part of the onboarding process. Employees that are delinquent may be subject to disciplinary actions. Relevant employees include those responsible for the following:

- i. customer onboarding and due diligence (including high-risk customer monitoring;
- ii. monitoring customer transactions and electronic fund transfers;
- iii. addressing customer queries or concerns (customer service teams); and
- iv. technology functions related to AML activities.

The AML Compliance Person is responsible for developing a risk-based training program and ensuring that staff members requiring advanced training due to their job description and/or responsibilities within the Company receive such training. A training log will be maintained.

vi. Independent Testing

The Company will conduct independent testing on the Company's AML program on a periodic basis, and no less than twice annually. When conducted, the review will assess the implementation and effectiveness of the Company's AML/OFAC program and the adequacy of controls over any related risks. The Compliance Officer is responsible for updating the Company's risk assessment in regards to any issues raised during the independent testing and taking necessary corrective actions and remediate findings. Independent testing has not yet been conducted on the program but the decision to test will be determined at a later date

6. Compliance and Consequences of Non-Compliance

Failure to comply with AML legislation may result in sanctions being brought against employees such as fines and imprisonment or the Company including criminal prosecutor, and/or fines. These could affect the Company's ability to operate as well as seriously damage the Company's reputation.

Separate and in addition to the foregoing, an employee may also be liable for failure to meet record keeping and client identification responsibilities and requirements, failure to provide assistance or provide information during a compliance examination, or disclosing the fact that a unusual transaction report was made, or disclosing the contents of such a report with the intent to prejudice a criminal investigation.

“Tip Off” shall be defined as revealing to a third party that an internal or FinCEN report has been filed. Similarly, “prejudicing an investigation” involves disclosing to a third party that law enforcement is either investigating or preparing to investigate an individual. Disclosing to a suspected money launderer that a disclosure has been made will almost certainly undermine any subsequent investigation,

“Assist”

An employee commits an offense if he or she: (i) enters an arrangement which he or she knows, or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person; (ii) acquires, uses or has possession of criminal property; and (iii) conceals, disguises, converts, transfers or removes criminal property.