

AML-CFT POLICIES & PROCEDURES

Policy Owner:	Aspera Operations B.V.
Approved by:	Roland Eduard Gertruda de Mei Managing director Capital Trust Corporation N.V.
Signature	
Reviewed By:	Akhil Konjan Veedu Ravi
Title:	Compliance Officer
Signature	
Version:	v.5
Approval date:	25/11/2025

DOCUMENT REVISION HISTORY

Version	Date Updated	Date Approved	Drafted By	Approved By	Description of Changes
v.1	25.04.2025	25.01.2024	Syed Haider Naqvi	The Board of Directors	Drafted policy
v.2	19.04.2024	23.04.2024	Syed Haider Naqvi	The Board of Directors	Updates to policy
v.3	31.07.2024	02.08.2024	Syed Haider Naqvi	The Board of Directors	Updates to policy
v.4.	01.05.2025	06.05.2025	Syed Haider Naqvi	The Board of Directors	Updates align with regulatory updates
v.5	24.11.2025	25.11.2025	Akhil Ravi	The Board of Directors	Updates aligned with Curaçao law.

This policy shall be reviewed as needed and updated to ensure full alignment with Curaçao AML/CFT legislation.

LIST OF ABBREVIATIONS

4th AMLD	Directive (EU) 2015/849, the EU's 4 th Anti-Money Laundering Directive - on the prevention of the use of the financial system for the purposes of ML/FT
5th AMLD	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
BRA	Business Risk Assessment
CAP	Customer Acceptance Policy
CFATF	Caribbean Financial Action Task Force
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
ESA	European Supervisory Authority (European Banking Authority)
EU	European Union
FATF	Financial Action Task Force
FIU	The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT
GCB	Curacao Gaming Control Board
LID	National Ordinance on identification when rendering services
LMOT	National Ordinance on the reporting of unusual transactions
The Manual	This AML/CFT Policy & Procedures Manual
Material change	Examples of material change include: • Change of beneficial ownership (direct or indirect); • Change of principal place of business /tax residence; • Change of business industry or provision of new services; • Change of Director or Controlling persons with authorisation to sign financial documents of a company.
ML/FT	Money Laundering and/or Funding of Terrorism
MLRO	Money Laundering Reporting Officer
Non- reputable jurisdiction	A jurisdiction having:

	• significant deficiencies in its national AML/CFT regime; • inappropriate and ineffective measures to prevent ML/FT, taking into account any accreditation, declaration, public statement or report by FATF/MONEYVAL or any other FATF-style regional body; or • been identified by the European Commission in accordance with Article 9 of the 4th AMLD.
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person, a natural person with prominent public function and includes: • Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries; • members of Parliament or similar legislative bodies; • members of the governing bodies of political parties; • members of the superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; • members of courts of auditors, or of the boards of central banks; • ambassadors, and other high-ranking officers in the armed forces; • members of the administrative, management or supervisory boards of state-owned enterprises; and • anyone exercising a function equivalent to those set out in paragraphs (a)- • above within an institution of the EU or any other international body (incl. UN, World Bank). Family members of PEP: • the spouse, or a person considered to be equivalent to a spouse; • the children and their spouses, or persons considered to be equivalent to a spouse; and • the parents; Close associates of PEP: • a natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement, or any other close business relations, with that PEP; and • a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.
Sanctioned person	Designated persons, groups and entities, whose financial assets and economic resources are subject to freezing obligation under relevant anti-terrorism financing UN and EU Regulations
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report to the FIU
UN	The United Nations

Table of Contents

1. Preamble.....	6
2. The Purpose, Scope and Aim of the Policy.....	7
2.1 The Purpose of the policy:.....	7
2.2 The aims and objectives of the AML Policy.....	7
2.3 The Objectives and Goals of the AML Policy.....	7
3. Overview.....	8
3.1 What is ML?.....	8
3.2 Money Laundering in Practice.....	8
3.3 What is Funding of Terrorism?.....	9
3.4 What is Proliferation Finance?.....	10
4. The Risk-based Approach.....	10
4.1 What is the Risk-based Approach?.....	10
4.2 The Business and Customer Risk Assessments.....	11
5. Customer Acceptance Policy (CAP).....	13
6. Customer Due Diligence ('CDD').....	14
6.1 Introduction.....	14
6.2 CDD Measures.....	14
6.3 Identification and Verification.....	15
6.4 Sanctions screening and PEP status screening.....	16
6.5 Elev8 Customer Support.....	17
6.6 Identification of the beneficial owner & Business Relationship Purpose.....	18
6.7 Technological Risks and Non-Face-to-Face Models.....	18
6.8 On-Going Monitoring.....	19
6.9 Timing of CDD Measures.....	20
6.10 Application of CDD measures to existing customers.....	21
7. Simplified Due Diligence.....	21
8. Enhanced Due Diligence.....	21
9. Politically Exposed Persons.....	22
9.1 Who is PEP?.....	22
10. Restricted Persons.....	23
10.1 Restricted / High-Risk Jurisdictions.....	24
10.2 Suspicious of Stolen and Fraudulent Activity.....	25
11. The Termination of the Business Relationship.....	26
12. The Money Laundering Reporting Officer.....	26
13. Reporting Procedures.....	27
13.1 Recognition of unusual transactions.....	27
13.2 Reporting of unusual transactions.....	28
14. Training and Awareness.....	28
15. Anti-Money Laundering Compliance Program.....	29
16. Recordkeeping.....	30

1. Preamble

Aspera Operations B.V. (hereinafter referred to as the 'Company') attaches the highest importance to international and local efforts aimed at reducing financial crime.

This Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy and Procedures Manual (hereinafter referred to as the "Manual") provides a comprehensive framework to ensure the Company's compliance with the applicable laws and regulations of Curaçao, as mandated by the Curaçao Gaming Control Board (GCB) under the Regulations for the Combating of Money Laundering, the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction (January 2025).

- This Manual serves to fulfill the Company's obligations under the following Curaçao legislative instruments and related decrees:
- National Ordinance on Identification of Clients when Rendering Services (NOIS, N.G. 2017, no. 92);
- National Ordinance on the Reporting of Unusual Transactions (NORUT, 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 Sanctions Act (N.G. 2016, no. 54);
- National Decree entering into force of the Kingdom Sanction Law (N.G. 2017, no. 2);
- National Decree for general measures (July 10, 2015) implementing United Nations Security Council Resolutions concerning Al-Qaeda, the Taliban, ISIL, and related groups (N.G. 2015, no. 29);
- National Decree for general measures (July 10, 2015) implementing UN Sanctions related to Libya (N.G. 2015, no. 28);
- National Decree for general measures (July 10, 2015) implementing UN Security Council Resolutions 1695 (2006), 1718 (2006), 2087 (2013), and 2094 (2013) concerning the Democratic People's Republic of Korea (N.G. 2015, no. 30);
- National Ordinance extending the validity of sanction decrees (N.G. 2018, no. 34);
- The Code of Criminal Law (N.G. 2011, no. 48).

Together, these laws and regulations, along with any subsequent updates issued under the NOIS, NORUT, Sanctions National Ordinance, and the Kingdom Sanctions Act, form the cornerstone of Curaçao's legal and regulatory framework to prevent and mitigate the risks of money laundering, terrorist financing, and proliferation financing.

The Company's policy is to ensure full compliance with Curaçao's AML/CFT framework while also aligning with global best practices established by the Financial Action Task Force (FATF) and the Caribbean Financial Action Task Force (CFATF). Where relevant, international standards such as those issued by the European Union (EU) and the United Nations (UN) will also be considered to maintain global consistency in risk mitigation.

All officials within the Company are individually responsible for assisting in the efforts to detect, deter and prevent money laundering and other activities intended to facilitate the funding of terrorist or criminal activities. It is recognised that such efforts will help safeguard the integrity of the local financial services, gaming sectors and ancillary services as well as the good standing and reputation of the Company itself.

All officials, including Board Members and Senior Management, will be informed of and made familiar with the procedures outlined in this manual, together with the possible repercussions of non compliance.

2. The Purpose, Scope and Aim of the Policy

The Company has developed this Manual that sets out the procedures implemented by the Company, in order to comply with current AML/CFT rules and regulations.

2.1 The Purpose of the policy:

- A. Comply with the national Anti Money Laundering legislation as mentioned in section 1;
- B. Comply with CFATF;
- C. Comply with FATF;
- D. Comply with OFAC;
- E. Comply with any other legislation or recommendations, including those mentioned by the European Union ('EU') in relation to combatting ML and FT;
- F. to prevent the use of products or services promoted by the Company either for ML or FT purposes, and to prevent damage to the Company's name and reputation by association with ML and FT;
- G. to ensure that the Company complies with anti-money laundering legislations whenever it does business; and
- H. to document the procedures that are to be followed in order to detect and prevent ML.

2.2 The aims and objectives of the AML Policy

This policy will outline:

- A. the Objectives and Goals that are to be pursued by this policy;
- B. the tasks that are to be performed in fulfilling this policy and who is responsible for them;
- C. the processes and reporting procedures to be applied; and
- D. the obligation of the relevant organisational units to inform where applicable, the risk management and compliance of any facts that are relevant for the discharge of their duties.

2.3 The Objectives and Goals of the AML Policy

The Company must, on a continuing basis, assess its money laundering and terrorist financing risks and must implement its own prevention program as is most appropriate for the Company's particular circumstances. The purpose of this document is to set such a program.

The Company may choose to carry out the assessment in any manner it deems appropriate so long as it is reasonable under the circumstances. The assessment may be conducted in a highly

sophisticated manner (e.g. through the use of automated means), or it may be done in a simpler way as long as it is effective and adequate).

The Company's prevention of money laundering program must consider the customer base, the scope of business activities, and the product range that is offered in relation to the ML risk exposure.

At all times, the Company is obliged to understand who its customers are, what they do and whether or not they are likely to engage in ML or TF activities.

3. Overview

3.1 What is ML?

ML is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source. The Financial Actions Task Force ('FATF') described ML as the processing of 'criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source.'

Therefore, ML is a process by which criminals conceal, or attempt to conceal, the origin of the proceeds of their illegal activities and disguise or attempt to disguise the origin or the source of such proceeds to make them appear legitimate. This illegal process is of critical importance for criminals as it enables the perpetrators to make legitimate economic use of the criminal proceeds.

While the techniques for laundering funds vary considerably and are often highly intricate, there are generally three stages in the process:

- A. Placement - the stage when the proceeds of crime are placed in the financial system;
- B. Layering - the substantive stage of the process, which involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds (e.g. the buying and selling of property);
- C. Integration - the final stage when the laundered proceeds are re-introduced into the legitimate economy.

The definition of ML shall include also any of the following:

- I. Mere suspicion of criminal activity is sufficient (being, as it is termed a so-called 'suspicion-based regime') and there is no need to have knowledge;
- II. Criminalising money laundering irrespective of the crime that generates the proceeds - 'all crime regime'; and
- III. Covering property that may even be indirectly derived from criminal activity.

3.2 Money Laundering in Practice

A money launderer will seek to operate in and around the financial system in a manner that best fits the execution of the scheme to launder funds. As soon as many governments around the world enacted AML obligations, a shift in laundering activity occurred, involving non-financial activities such as dealers in high-value items, real estate, vehicle dealers and various gatekeepers like notaries, accountants, auditors and lawyers.

ML is an ever-evolving activity; it must be continuously monitored in all its various forms in order for measures against it to be timely and effective. The FATF and the CFATF publish periodic typology reports to 'monitor changes and better understand the underlying mechanism of money laundering and terrorist financing'. Their aim is to maintain the dynamism and timelines of efforts at combating ML/FT, precisely because of the ever-evolving nature of the crime of money laundering and the methods used by launderers to disguise the illicit origin/s of ill-gotten gains.

ML is frequently carried out in an international context, and therefore measures taken at the national level would be futile if it did not also take into account international coordination and cooperation. Particular account should be taken on the FATF Recommendations, as well as instruments of other international bodies active in the fight against ML/FT. A number of initiatives have been created to deal with the problem at an international level, such as the establishment of the Egmont Group of FIUs which is a worldwide group that promotes closer cooperation between FIUs and facilitates information sharing through a secure internet system known as the Egmont Secure Web.

3.3 What is Funding of Terrorism?

Funding of Terrorism is the process of making funds or other assets available to terrorist groups or individual terrorists to support them, even directly, in carrying out terrorist activities.

These include the use or possession of money or other property for the purposes of terrorist activities and the involvement in funding arrangements to support terrorist activities. The United Nations International Convention for the Suppression of the Financing of Terrorism 1999 defines the Financing of Terrorism as follows: Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

- A. an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
- B. any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population or to compel a government or an international organisation to do or to abstain from doing any act.

The funding of terrorist activity, terrorist organisations or individual terrorists may take place through funds derived from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organisations and traditional criminal organisations involved in money laundering operations.

While the funding of terrorism may thrive on funds derived from legitimate sources, money laundering necessarily involves funds from illegal sources.

Another difference is that, while the money launderer moves or conceals criminal proceeds to obscure the link between the crime and the generated funds, and avails himself of the profits of crime, the terrorist's ultimate aim is not to generate profit from the fund-raising mechanisms but to obtain resources to support terrorist operations.

¹ FATF, Guidance for Financial Institutions in Detecting Terrorist Financing, April 2002.

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is often a need for terrorists to obscure or disguise links between the organisation or the individual terrorist and their legitimate funding sources. Therefore, terrorists must similarly find ways to process these funds to be able to use them without drawing the authorities' attention.

Financing is required not only to fund specific terrorist acts but, more generally, to meet the operational costs of terrorist organisations, such as maintaining a terrorist network or cell, recruitment and training, sustaining an ideology of terrorism through propaganda, and maintaining an infrastructure or organisational support (even more so if this is to sustain an international network).

Terrorist organisations will vary from one organisation to another ranging from large, state-like organisations to small, decentralised and self-directed networks. Likewise, the nature of terrorist financing will vary depending on the size and scale of the organisation involved, if any, and the source from which funding is derived. Terrorist activities may be financed by states, companies or charities, as well as being self-financed by the terrorists themselves. Various methods of funding may be used at the same time.

In order to diminish terrorism, it is important to cut off financial support, in order to disrupt the operational activities of terrorist and terrorist organisations. This is what international anti-terrorism sanctions are aimed at. Not only do they enable terrorists' assets to be frozen globally but also, they also reduce terrorists' movement.

The UN Security Council obliges all states to freeze, without delay all funds and other financial assets or economic resources of any person, group or entity designated by the UN Security Council or a relevant UN Security Council Sanctions Committee.

²Resolutions 1267,1988,1989

3.4 What is Proliferation Finance?

Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes).

³ Dual-use goods are items that can be used both for civilian and military applications. These types of goods are heavily regulated because they can be classified for civilian use and then transformed for military purposes, or worse used for terrorism

4. The Risk-based Approach

4.1 What is the Risk-based Approach?

An anti-money laundering compliance program is an essential component of a Company's compliance regime. The primary goal of every good program is to protect the organization against

money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

Based on the FATF Recommendations, the Company is required to apply a Risk-based Approach when designing policies, procedures and controls to combat money laundering, financing of terrorism and financing of proliferation of weapons. By adopting a Risk-based Approach, it is possible for the Company to ensure that measures to prevent or mitigate money laundering, financing of terrorism and proliferation of weapons are commensurate with the risks identified. In drawing up the anti-money laundering compliance program, the Company takes a risk-based approach. That means the higher the risk, the more measures the Company will take to mitigate the risk. Where the risks are higher enhanced measures must be taken. Where the risks are lower they may take simplified measures, provided that this is consistent with the country's assessment of its money laundering/financing of terrorism risks.

Applying a Risk-based Approach means that the Company will:

- Assess the risks that money laundering or terrorist financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Document their risk assessments, including everything that has been done and the reason for this being done.

The risk assessment considers all relevant risk factors, including the player, countries or geographic areas, products and services (types of games of chance) that the Company offers and delivery channels, before determining the level of overall risk. Based on the risk assessment, the appropriate level and type of mitigation to be applied is determined. The Company will also take notice of the outcomes of the National Risk Assessment (NRA) of the jurisdictions where it operates and take these outcomes into account when conducting its risk assessment.

4.2 The Business and Customer Risk Assessments

The basis for the risk-based approach is the risk assessment which the Company has to carry out of its operation. This requires an understanding and assessment of the risk that one's business is in general exposed to, the so-called business risk assessment.

Also, each player exposes the Company to different risks. Therefore, a player-specific risk assessment must be carried out so the Company is able to identify the potential risks it faces when entering into a business relationship with, or carrying out an occasional transaction for a player, the so-called customer risk assessment. This assessment enables the operator to develop a risk profile for the customer and to categorize the ML/TF risk posed by such a player as low, medium or high.

a. Business Risk Assessment (BRA)

As indicated above, the Company is required to carry out a business risk assessment to identify the ML/TF risks they are exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. To strengthen consistency and comparability, To strengthen consistency and comparability, the Company applies a qualitative Low / Medium / High risk rating system across all key categories. This structured scoring framework ensures alignment with regulatory expectations and enables effective prioritization of mitigation measures.

The methodology for the risk classification involves assigning likelihood and impact scores (scale 1-5) to each risk factor, with a product of both determining the inherent risk. This is followed by the evaluation of existing controls and their effectiveness (on a 1-5 scale), resulting in a treated risk score. Sources of risk factor evaluation include FATF, UN, EU, OFAC lists, NRA publications, Internal data.

The risk assessment should address the ways in which the Company's products and services could be used to launder money, finance terrorism and finance proliferation and the extent of the risk that this will happen. All factors that may have an impact on the risks of money laundering, financing of terrorism and financing of proliferation must be taken into account in the risk assessment, but special consideration must be given to the type of customers, products and services offered, delivery channels and geographical risk factors.

The risk assessment evaluates exposure across the following categories:

- Customer Risk (e.g. PEPs, high-spending individuals, third-party involvement)
- Product/Service Risk (e.g. high-liquidity games, anonymous payment methods)
- Geographical Risk (e.g. high-risk jurisdictions per FATF, UN, EU, OFAC)
- Delivery Channel Risk (e.g. non-face-to-face onboarding, third-party agents)
- Technological Risk (e.g. virtual currencies, automation tools)

The Company also has to take into consideration and include outcomes and recommendations of the National Risk Assessment in their business risk assessment. The effectiveness of the implementation of these measures has to be monitored and improved where necessary.

The Business Risk Assessment shall be formally documented, reviewed and approved by the Board of Directors at least once per year or whenever a material change in business operations, products, services or the regulatory environment occurs.

b. Customer Risk Assessment (CRA)

The customer-specific risk assessment has to be carried out either prior to the carrying out of an occasional transaction or during the establishment of a business relationship. It is possible that this initial customer-specific risk assessment will have to be revised at a later stage of the business relationship and this may result in a customer's risk rating having to be adjusted.

CRA shall be reviewed on an ongoing basis, including:

- Whenever there is a material change in the customer's behavior, profile or transaction activity;
- Upon triggering alerts from the ongoing monitoring systems;
- At least annually for medium/high-risk customers as part of the periodic KYC refresh cycle.

The Customer Risk Assessment will assess the particular risks the Company will be exposed to when providing its services or products to players. The information collected to draw up the CRA will formulate the customer's risk profile. On the basis of the CRA, the proper level of CDD can then be applied as stipulated in the Customer Acceptance Policy (CAP).

Customers categorized as Low risk will be eligible for Simplified Due Diligence (SDD), while those flagged as High risk will be subject to Enhanced Due Diligence (EDD), including verification of source

of wealth/funds senior management approval for onboarding and increased transaction monitoring. Medium risk customers will undergo Standard CDD with periodic reviews

This policy has to provide:

- a description of the type of players that are likely to pose a higher than average risk of ML/FT/FP;
- the risk indicators presenting low, medium or high risk;
- Integration of sanctions and PEP screening into the customer onboarding and monitoring process , including automated checks against UN,EU,OFAC and any Local Curaçao sanctions lists;
- the level of Customer Due Diligence (CDD) measures, including ongoing monitoring to be applied;
- the circumstances under which service to someone is declined.

5. Customer Acceptance Policy (CAP)

The Company applies a Customer Acceptance Policy (CAP) to ensure that only customers aligned with its risk appetite are onboarded. This policy forms part of the overall risk-based approach and supports effective AML/CFT controls.

The CAP outlines the conditions under which a customer is accepted or rejected , based on the result of the CRA and other compliance checks.It serves as a key control mechanism to ensure that:

- All onboarding is conducted in line with Curaçao AML/CFT regulations.
- Risk-based decisions are taken to approve, restrict, or reject customer relationships.

Customers are accepted based on the outcome of the Customer Risk Assessment (CRA) and must:

- Have passed all identity verification (KYC) and sanctions/PEP screening requirements.
- Have provided a clear and legitimate source of funds and/or source of wealth, when required.
- Reside in jurisdictions with effective AML/CFT regimes (not listed as high-risk by FATF, OFAC, or CFATF).
- Exhibit transaction behavior that is consistent with their profile.
- Are not subject to any regulatory, legal, or law enforcement restrictions.

The Company does not accept customers who:

- Customers failing identity verification or providing false/incomplete documentation.
- Customers listed on international or local sanctions lists (e.g., UN, EU, OFAC, local GCB).
- Individuals identified as Prohibited PEPs, such as those under investigation or under sanctions.
- Customers from or residing in non-cooperative or sanctioned jurisdictions.
- Customers whose source of funds or wealth cannot be verified when required.
- Customers using third-party payment methods inconsistent with the verified account holder.
- Anonymous or fictitious users.

Based on risk classification (low/medium/high), customers are subject to Simplified, Standard, or Enhanced Due Diligence. Customers exceeding the Company's risk tolerance will be declined or offboarded, and FIU reporting will be considered where relevant.

6. Customer Due Diligence ('CDD')

6.1 Introduction

The Company is prohibited from keeping anonymous accounts or accounts in obviously fictitious names. The Company 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 Customer Due Diligence program is the best way to prevent money laundering, financing of terrorism and financing of proliferation.

The customer's risk profile is essential to allow the Company to apply a certain level of Customer Due Diligence commensurate to the identified ML/TF risk. The purpose of collecting information is to provide the Company with documentation to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship. Such an assessment is necessary in order to detect deviations from the expected behaviour. Any unusual behaviour needs to be reported to the FIU. If FIU Curaçao, after proper analysis of an unusual transaction, concludes that there is a suspicion of money laundering and/or terrorism financing, this transaction will be reported to the Public Prosecutor's Office as a suspicious transaction.

The Company has the obligation to undertake Customer Due Diligence measures when:

- a. When players engage in financial transactions equal to or above Naf. 4,0001;
- b. carrying out occasional transactions above the monetary equivalent of NAF. 4,000;
- c. there is a suspicion of money laundering or terrorist financing; or
- d. The Company has 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 NAF. 4,000.

In case the Company carries out an occasional transaction above the monetary equivalent of NAF. 4,000, it is still obliged to apply CDD measures. The Company is also subject to this obligation when they execute a series of linked transactions which, though individually below the applicable threshold, would cumulatively meet or exceed the NAF. 4,000 threshold. Transactions are considered as linked if for example they are carried out by the same player through the same game or in one gaming session. Whenever an occasional transaction presents a high risk of ML/TF, the enhanced due diligence measures must be applied.

6.2 CDD Measures

The CDD measures to be taken are as follows:

- A. Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- B. 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, the source of funds.

The Company, their directors, officers and employees are prohibited to disclose the fact that a UTR is being reported to the FIU. A risk exists that players could be unintentionally tipped off when the Company is seeking to perform its CDD obligations in these circumstances. Therefore, if the Company has a suspicion that transactions relate to ML or TF, it should take into account the risk of tipping off when performing the CDD process. If the Company reasonably believes that performing the CDD process will tip off the player, it may choose not to pursue that process and should file a UTR to the FIU.

6.3 Identification and Verification

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

a. Identification of the player

When identifying the player, at a minimum the following information will be collected:

- A. full name;
- B. permanent residential address;
- C. date of birth;
- D. place of birth;
- E. nationality; and
- F. identity number.

However, in low-risk scenarios, the Company 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 the Company considers the collection of additional personal details as necessary to mitigate the higher risk of ML/FT.

b. Carry out a Customer Risk Assessment

This is done to have sufficient information available to detect unusual activity in the course of the business relationship. At this stage, a provisional risk rating will be assigned based on the initially collected information. This is revised once questions are answered or additional information is received. On the basis of the CRA, the proper level of CDD can be applied as stipulated by the CAP.

c. Verification

Verification of identity refers to actions taken to verify that a person exists and is who he claims

to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.

As a rule, verification of identity will be carried out by making reference to an unexpired government-issued document containing photographic evidence of the customer's identity (e.g. passport, identity card). Where such a document does not allow verification of the player's residential address, the Company will obtain other documents like a bank statement, utility bill, letter from a public authority or rental agreement, which should not be more than six months old to verify the residential address. The Company will also contact the player by letter, e-mail or telephone to verify the information supplied. It will also send a verification code to the e-mail address to verify that the address is current and genuine. Verification will also be done by checking social media, telephone directories, companies registries or media and news sources. Biometric checks can also be used to confirm that the individual providing the document is the one described therein.

There will also be circumstances in which the Company is able to cross-reference the information in its possession with geo-location information, IP address data, funding method data etc. Verification is carried out for the Company to determine to its satisfaction that the player is who they declared themselves to be.

Where the Company does not have sufficient comfort that it knows its player, it will take additional measures to do so. Some of these measures include requesting additional identification documents, asking the player to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

If the Company is unable to satisfy the due diligence requirements outlined in this procedure, the Customer will not be allowed to begin or maintain any relationships or transactions.

6.4 Sanctions screening and PEP status screening

All players will be screened against sanctions lists. The Company will not do business with customers that are subject to international sanctions. Before doing business or performing an occasional transaction for the first time with a player, the Company will check published lists of known or suspected terrorists or other sanctioned persons or companies.

The Company has contracted with the industry-leading Swedish AML resource company, Devcode Identity AB (www.devcodeidentity.com). Devcode will provide the Company with identification, authentication, onboarding, KYC, fraud and data-source lookup services on a subscription basis. The Devcode suite of tools are integrated into the software platform being operated by the Company which will power the services provided to customers.

The suite of tools that Company will use from the Devcode stable will comprise:-

(1) SigninIQ:

This service allows the Company to verify its customers to ensure they are compliant with AML and KYC legislation. The identity verification will be performed at sign-up, check out and at any other event that demands a verified customer. Devcode Identity supports solutions such as eID, online ID verification and Open Banking. This tool will check if its customers are on a PEP or sanction list with

checks being conducted against EU, UN, OFAC, HKM etc. Customer source of funds, source of wealth, IBAN owner and player limits will be checked.

(2) GDC (Global Data Consortium)/LSEG:

GDC specialises in delivering high-speed electronic digital identity verification. GDC provides global name and address matching capabilities that enable them to accurately source and enhance data from over 300 data sources globally and to deliver high-quality identity data in near real-time for over 70 countries. Aspera will contract with GDC services through DevCode ID.

The Company will ensure that all sanctions and PEP screening tools are kept up-to-date by verifying that sanctions lists (UN, EU, OFAC, HKM, and any applicable Curaçao-published lists) are current and refreshed on a regular basis.

Sanctions and PEP screening will not be limited to onboarding but will also be conducted on an ongoing basis throughout the business relationship. Any customer identified as a sanctioned individual or high-risk PEP will be escalated to the MLRO and appropriate measures will be taken in line with Curaçao's AML laws and internal procedures.

6.5 Elev8 Customer Support

Ongoing checks will be carried out by the Company's specialist customer support service provider, Elev8 Solutions Limited (<https://elev8solutionsltd.com/>) who will also carry out manual checks of our customers' accounts.

These ongoing checks will include but are not limited to:

- a. maintain ongoing monitoring of the client's account activity, use of payment methods for balance refills and withdrawals, and review of transactions made during the course of these relationships to ensure that the transactions are consistent with the client's information, risk profile, and funding source provided by the company;
- b. to ensure that the records, data, or information the client provides for due diligence are accurate, current, appropriate, and subject to regular review.
- c. When a client deposits or withdraws money in amounts that are unusual for the client's past deposit and withdrawal activity, or when a compliance officer notices suspicious activity, source of funds verification will be done. While the source of the funds is verified, the transaction will be halted. It might also be necessary to validate the source of the funds used for the deposit.
- d. Check the legitimacy of documents by using document verification software and/or other resources, like contacting the document's issuing authorities or comparing it to known authentic examples of documents, to verify the document's authenticity.

While the Company utilizes third-party services such as Devcode Identity AB and Elev8 Solutions Ltd for technical onboarding and ongoing monitoring support, the ultimate responsibility for AML/CFT compliance remains with the Company.

The Company conducts due diligence on all third-party providers to confirm their competence, reliability, and alignment with Curaçao's AML/CFT legislation, including the National Ordinance on Identification (NOIS), Reporting of Unusual Transactions (NORUT), and relevant Sanctions Ordinances.

Contracts with these providers include compliance clauses that require full adherence to Curaçao AML laws, including the proper handling of personal data, escalation procedures, and red flag identification.

Responsibilities are clearly defined:

- Devcode Identity AB performs automated KYC, identity verification, sanctions/PEP screening, and source of funds checks.
- Elev8 Solutions Ltd conducts manual monitoring, document validation, and escalates any suspicious behavior or discrepancies to the internal Compliance Officer or MLRO.

All alerts and potential concerns identified by these third parties are logged and reviewed internally by the Compliance Team to determine whether further action or reporting to the FIU Curaçao is necessary.

6.6 Identification of the beneficial owner & Business Relationship Purpose

The Company is required to identify and verify the beneficial owner of a customer, where applicable. Customers must confirm during onboarding that they are acting on their own behalf through a declaration embedded in the terms and conditions. However, the company must not rely solely on such declarations and shall maintain systems to detect where third parties may be transacting on behalf of others.

In scenarios involving syndicates, pooled funds, or corporate structures, the Company shall identify and verify any individuals with 25% or more ownership or voting rights, or those who otherwise exercise ultimate control over the customer. Where no natural person can be identified, the senior managing official must be recorded as the beneficial owner. This is particularly relevant when dealing with corporate or business participants using accounts for commercial hedging or matchbook exposure.

Understanding the purpose and intended nature of the business relationship is an essential element of Customer Due Diligence. While the purpose of opening a gaming account is generally straightforward, the Company must collect enough information to create a customer risk profile that reflects expected transactional behavior. This enables detection of anomalies during the course of the relationship.

Where ML/FT risk is considered low, a basic declaration—such as the customer's occupation, industry, and estimated annual income—may suffice. However, for medium or high-risk cases, this information must be supported with reliable documentation and/or digital verification. Where appropriate, the Company may also reference statistical data (e.g. national income levels or historical platform trends) to understand a customer's typical wagering capacity, though this method shall not be used in high-risk cases.

6.7 Technological Risks and Non-Face-to-Face Models

The Company acknowledges that the use of technology in delivering remote gaming services introduces specific risks that may be exploited for money laundering or terrorist financing.

- a. Use of non-face-to-face onboarding methods
- b. Acceptance of anonymous or partially anonymous funding mechanisms, such as cryptocurrencies, virtual prepaid cards or electronic wallets

- c. The automation of transactions or activity patterns through the use of bots, scripts or proxy tools
- d. Geo-obfuscation tools, such as VPNs or anonymizers

To mitigate these risks, the company has implemented enhanced identity verification using biometric and document authentication tools via Devcode Identity AB. The company has also implemented detection of IP spoofing, mismatches in device/user behaviour and proxy/VPN use. Additionally, geolocation and browser fingerprinting are used to detect anomalies in customer activity. The company has implemented restrictions or additional reviews of customer activity. The Company has implemented restrictions or additional reviews of customers using crypto-based or high-risk payment instruments. Lastly, all non-face-to-face customers are classified as at least medium risk and are subject to additional monitoring.

All technology-driven controls are reviewed periodically as part of the Company's risk assessment framework, and the MLRO evaluates any new tools, channels or services prior to launch to assess the impact on the Company's risk profile.

6.8 On-Going Monitoring

The Company will conduct 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.

a. Ongoing monitoring of identity

In conducting ongoing due diligence on the business relationship, the Company will hold accurate and up-to-date identification data of its customers. Since identity may change due to circumstances, the Company will obtain evidence of identity periodically to detect any changes, refresh the data on key events (i.e. change of payment instrument) or will track expiry dates on evidence of identity and refresh it as it expires. The Company will determine on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

b. Ongoing monitoring of transactions

Transaction monitoring is executed to prevent the involvement of the Company with ML/TF and to safeguard the reputation of the Company. While conducting ongoing scrutiny of transactions, the Company notices that a customer's transactions are not consistent with what it knows or expects from the customer, the Company will question this unusual activity and, where necessary, establish the source of the funds used for that transaction. Source of funds refers to how the funds for a particular transaction were obtained by the player. The reason for inconsistency may lie in inconsistency, amongst others, with the source of funds or average profile or account activity noted to date). The Company will try to understand what the reason for this deviation is and obtain sufficient information and documentation with regard to the transaction. It is also one of the situations in which the risk profile of the customer may have to be revised.

After receiving this information, the Company will decide whether the transaction is an unusual transaction and needs to be reported to the FIU.

As with anything else, the level of ongoing monitoring will depend on the risk profile of the

customer, but even in low-risk situations, there will be a degree of oversight taking place to ensure that the business relationship still has to be considered as a low-risk one.

The frequency and intensity of ongoing monitoring shall be directly proportionate to the customer's risk profile as determined through Customer Risk assessment.

- High-risk customers will be subject to continuous or near real-time transaction monitoring and periodic identity refresh at least every 12 months.
- Medium -risk customers will be reviewed at least every 18-24 months with transaction patterns analyzed monthly or upon trigger events.
- Low-risk customers will be monitored periodically , with identity and transaction pattern checks performed at a maximum interval of 36 months.
- Ongoing monitoring will also be triggered by specific events or red flags, such as:
 -
 - Sudden or unexplained changes in transaction volume or frequency;
 -
 - Use of new or previously unverified payment methods;
 - Changes in customer location, declared occupation, or IP activity;
 - Failed KYC refresh or expiration of ID documents;
 - Attempts to use third-party funding sources or proxy users.

Monitoring is conducted through a combination of automated systems and manual reviews. The Company uses integrated compliance tools (such as Devcode Identity AB and manual oversight from Elev8 Solutions) to detect anomalies in real time, flag high-risk behavior, and escalate suspicious activity for internal review. Alerts from these systems are routed to the Compliance Team and MLRO for investigation.

6.9 Timing of CDD Measures

The Company provides services to a customer allowing for the wagering of a stake with monetary value in a game of chance. It does business with customers who are individuals and who act in their own name and on their own behalf. In doing so, the Company opens an account for their customers.

This is considered to be indicative of a relationship that is expected to have an element of duration and is therefore considered a business relationship between the Company and its customer. For the Company, verification of identity has to be conducted when engaging in financial transactions equal to or in excess of NAf. 4,000. This implies that all CDD measures must have been conducted at the time the threshold is reached. However, the Company will apply a minimum level of CDD measures prior to reaching the threshold. Thus, simultaneously with the opening of an account, the Company is able to identify the customer by collecting the minimum personal details, being: name and surname, permanent residential address and date of birth (set as the minimum applicable in case of low-risk business relationships) and conduct the sanctions screening. The threshold is to be calculated on a daily basis taking into account all deposits and withdrawals made by the player since the establishment of the business relationship. Once the threshold is reached, the Company will carry out a customer risk assessment and meet their remaining CDD obligation.

In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the casino obtains any necessary information from the customer concerned.

However If the Naf.4,000 threshold is reached, the player cannot deposit funds into the account or withdraw funds from the account.

Besides that, if the requested information and documentation is not received within 30 days from the moment the Naf.4,000 threshold was met in order for the Company to complete the CDD, the Company will terminate the relationship with the player and report the transaction to the FIU.

6.10 Application of CDD measures to existing customers

The Company will also apply the CDD measures to existing customers on the basis of materiality and risk and will conduct due diligence on such existing relationships at appropriate times. The Company will consider whether any procedures they have been applying are sufficient to meet their CDD obligations. If this is the case, The Company will continue applying these and pay special attention to their on-going monitoring obligations.

7. Simplified Due Diligence

Where the risks of money laundering or terrorist financing are lower, the Company will conduct simplified CDD measures, which will take into account the nature of the lower risk. Examples of possible measures:

- Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the casino to obtain the player's identity. In this case, casinos may limit identification to the first three personal details;
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the Company will also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low-risk situations, the Company will verify the basic identification details, as long as the Company has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

8. Enhanced Due Diligence

A risk-based approach will be taken, so more thorough checks should be undertaken for higher-risk customers. The Enhanced Due Diligence (EDD) measures will be consistent with the risks identified. In particular, it will increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual.

Enhanced Due Diligence will be conducted where the risks of money laundering or terrorist financing are higher. This concerns for example:

- Residents of higher-risk geographic areas;
- Political Exposed Persons (PEP's);
- Products or transactions that might favour anonymity;
- New products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.
- Examples of enhanced due diligence measures include:
- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player.
Examples of sources of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In situations presenting a higher risk of ML/TF, source of funds information will be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

9. Politically Exposed Persons

Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering offences and related predicate offences (including corruption and bribery), as well as conducting activity related to terrorist financing.

To address these risks the legislative provisions require subject persons to implement measures to prevent the misuse of the financial system and non-financial businesses and professions by PEPs, and to detect such potential abuse if and when it occurs.

9.1 Who is PEP?

These include but are not limited to:

- Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries;
- Members of Parliament or similar legislative bodies; Members of the governing bodies of political parties;
- Members of the superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

- Members of courts of auditors, or of the boards of central banks;
- Ambassadors, charge and other high-ranking officers in the armed forces;
- Members of the administrative, management or supervisory boards of state-owned enterprises;
- Anyone exercising a function equivalent to those set out in paragraphs (a) to (f) above within an institution of the European Union or any other international body.
- In terms of the PLMFTR, this also includes the 'immediate family members' of PEPs. Therefore, the terms includes:
 - The spouse, or any partner recognised by national law as equivalent to the spouse;
 - The children and their spouses or partners; and
 - The parents.
- Furthermore, the term includes "persons known to be close associates", a natural person known to have:
 - joint beneficial ownership of a body corporate or any other form of legal arrangement; or any other close business relations with that PEP.
 - a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.

9.2 Risk Posed

PEPs pose a high risk of ML/FT due to the position they occupy and the influence they exercise. PEPs may abuse their prominent public functions for private gain, such as by being involved in corrupt practices, accepting bribes or abusing or misappropriating public funds. Certain PEPs in certain positions may also be exposed to the possibility of being involved in FT.

In order for the Company to mitigate the potential risks of ML/FT that arise when dealing with PEPs or family members or persons known to be close associates of PEPs, the application of EDD measures is a must. The application of EDD measures should be commensurate and proportionate to the ML/FT risks envisaged.

The degree of scrutiny that the Company will apply will depend on various risk factors, including, but not limited to:

- a. proof that the clients source of funds or wealth do not emanate from criminal activity;
- b. whether the home jurisdiction of the PEP is one in which current or former political figures have been implicated in corruption; and
- c. the length of time that a former political figure has been in office.

If due diligence cannot be performed adequately, the Company will not open the account or will suspend the transaction activity, file a report with the MLRO and close the account.

10. Restricted Persons

The Company will not enter into any business relationship of financial transaction with a person or entity that:

- Is listed on any international or national trade or economic sanctions list, such as but not limited to
 - a. The United Nations Security Council Sanctions List;
 - b. The Specially Designated Nationals (SDN) list maintained by OFAC (Office of Foreign Assets Control of U.S. Treasury Department)

- c. Or the Denied Person List issued by the U.S. Commerce Department.
- Is a Government Official or Politically Exposed Person (PEP) as defined under the FATF's 40 Recommendations, and whose risk Cannot be effectively mitigated.
- Is from or transacting from jurisdictions that do not meet international AML- CFT standards and are designated by the FATF as high risk , non-corporative or strategically deficient jurisdictions;
- presents a risk of exposure to penalties, sanctions or reputational damage under applicable AML, CFT , anti-corruption , sanctions or tax laws;
- Fails to meet the company 's user due diligence standards , provided suspicious or unverifiable information or otherwise exhibits high-risk behavior inconsistent with the declared purpose of the relationship;
- is resident in a restricted or blocked jurisdiction, as assessed and maintained internally by the Company's Compliance Team, based on guidance from the Curaçao Gaming Control Board (GCB) and international bodies.
- In accordance with AML/CFT guidelines, the Company considers all relevant global and local sanctions sources including:
 - FATF high-risk and grey-listed jurisdictions
 - UN security Council Consolidated list
 - OFAC SDN list
 - UK OFSI consolidated list
 - Jurisdictions Restricted Based on Internal Risk Appetite

Any future lists issued by the Curaçao authorities.

10.1 Restricted / High-Risk Jurisdictions

Restricted / High-Risk Jurisdictions	
FATF High-Risk Jurisdictions (Black List)	OFAC/UN Sanctions
Iran DPRK (North Korea) Myanmar (Burma)	Russia Crimea, Donetsk, Luhansk (Ukraine) Sudan
FATF Jurisdictions Under Increased Monitoring (Grey List)	
Algeria Angola Bolivia Bulgaria Cameroon Côte d'Ivoire Democratic Republic of the Congo Haiti Kenya Lao PDR Lebanon	Monaco Namibia Nepal South Sudan Syria Venezuela Vietnam Virgin Islands (UK) Yemen

Jurisdictions Restricted Based on Internal Risk Appetite	
American Samoa	U.S. territory, restricted due to compliance complexity
Chad	Political Instability
China	restricted due to regulatory/censorship/operational reasons
Democratic Republic of the Congo (DRC)	FATF greylisted; restricted based on international AML/CFT deficiencies
Cuba	Not FATF listed; U.S. embargoed, historically high risk
Guinea-Bissau	Not FATF greylisted currently; past governance issues
Iraq	Not FATF greylisted; political/terrorism risk
Nicaragua	Not FATF-listed; potential political/reputational risks
Pakistan	Removed from FATF greylist (2022) Terror finance risks, corruption
Philippines	Removed from FATF greylist (2024); Internal risk
Uganda	Not FATF-listed; high internal ML/TF risk
Zimbabwe	Not FATF-listed; historically sanctioned/high corruption risk

10.2 Suspicious of Stolen and Fraudulent Activity

When there are a lot of similarities between one activity and another or there are strange activities which do not quite fit within the Customer's profile, the Fraud team will request from the Customer a Selfie, in order to verify that there has not been an identity fraud.

As soon as suspicion rises all documents must be screened, even though the account would be below threshold. Until such time as the due diligence is carried out, the Customer's account will be blocked and the Customer will not be in a position to withdraw any funds. Should the requested documents not be provided after 3 notifications, sent by email, then the Customer's account will be blocked definitely and the Money Laundering Reporting Officer ('MLRO') will be notified

accordingly, providing the MLRO with the transaction history and other information needed. It will be up to the MLRO as to whether a Suspicious Transaction Report ('STR') will be filed or not with the relevant authorities.

11. The Termination of the Business Relationship

In case the obligations arising from the customer's due diligence cannot be met, the Company will not establish the business relation or perform the transaction and will terminate the business relationship with the customer. The Company will also keep a record of all the attempts made to get the necessary information and documentation. To this end, the Company may decide to either close the account or keep it blocked and suspended in its entirety.

In the event that the customer makes the requested information and/or documentation available to the Company following the closure or the suspension and blocking of the gaming account, the Company will consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.

The Company will consider whether there are any grounds giving rise to suspicion of ML/TF/FP. The reluctance of the customer to provide CDD on its own will not be automatically equated to a suspicion of ML/TF/FP. The Company will consider all factors and information it has at its disposal to decide whether there are grounds to suspect ML/FT/FP. If, however, the presumption of ML/FT/FP exists the Company will submit an unusual transaction report to the FIU with regard to this player.

Where there is no reason for the retention of funds, the funds are to be remitted back to the player. This has to be done through the same channels used to receive the funds.

12. The Money Laundering Reporting Officer

The MLRO is responsible for the oversight of all aspects of the Company's AML/CFT activities and is the focal point for all activity relating to AML/CFT. As such he/she is tasked with monitoring the day-to-day operations and ensuring compliance with the Company's AML/CFT policies and procedures.

The MLRO is specifically responsible for the following:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;

- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

Additionally, the MLRO acts as a reference for any matters, enquiries or contact with the Regulatory Authority.

13. Reporting Procedures

The Company is not only required to adhere to the stipulations of the National Ordinance for Identification of Services but is also required to detect and report either intended or completed unusual transactions. The Company has adequate procedures in place that cover the following:

- a) The recognition of unusual transactions;
- b) The documentation of unusual transactions; and
- c) The reporting of unusual transactions.

13.1 Recognition of unusual transactions

An unusual transaction is a transaction inconsistent with the player's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the player. The purpose of collecting information is to provide the Company with documentation to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship.

Based on the NORUT legislation, objective and subjective indicators have been established by means of which the Company must assess whether a customer's transaction qualifies as an unusual transaction. Management will also provide its staff with specific guidance and training in recognizing and adequately documenting unusual transactions. All these unusual transactions must be reported to the compliance officer/MLRO in the format approved by management. All additional documents available, such as copies of identification documents, cash-out slips, and other records will also be submitted as supplements. The compliance officer/MLRO will keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU by the Company, the reason shall be adequately documented and signed off by the compliance officer/MLRO and/or management.

In order to implement FATF recommendation 11, the Company will pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

The following transactions or intended transactions are deemed unusual:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;

- Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- Transactions in the amount of NAf. 5,000 or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means. This includes but is not limited to:
 - a. A cashless transaction in the amount of NAf. 5,000 or more.
 - b. A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the client.
 - c. Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
 - d. Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but are not limited to tokens and credits.
 - e. A cash out in the amount of NAf. 5,000 or more;
 - f. Note: A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAf. 5,000.
- Presumed money laundering transactions or terrorist financing: Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

13.2 Reporting of unusual transactions

By virtue of article 11 of the NORUT, the Company will report unusual transactions or any intended unusual transaction to the FIU without delay. In order to do this, it has clear procedures for internal and external reporting of unusual transactions in place. These have been communicated to the personnel.

All unusual individual transactions or series of transactions, as mentioned in the Regulation Indicators Unusual Transactions, must be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting.

The documentation of unusual transactions. The Company has registered with the FIU and will get access to the goAML reporting portal after validation by the FIU.

The compliance officer/MLRO will also prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The Company will report to the FIU the details of the transactions by means of the goAML reporting portal. The reports and the submission of the thereto-related information (all supporting documents) will be done in English.

The Company and its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting to the FIU.

14. Training and Awareness

Each employee of the Company will be made aware of the policies and procedures listed here and will ensure that they understand the importance of adhering to these policies.

New employees

A general training of the nature and process of money laundering and terrorist financing, and the need to report any unusual transactions to the appropriate designated officer will be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority. They will be made aware of the existing internal policies, procedures and regulations concerning money laundering, terrorist financing, proliferation of weapons and the reporting requirements. They will also be trained on the money laundering methods and trends in the gambling sector. They will receive an explanation of customer due diligence and objective and subjective indicators for reporting unusual transactions.

Audit staff

Those charged with overseeing, monitoring and testing money laundering controls will also be trained about changes in regulation, money laundering methods and enforcement, and their impact on the organization.

AML Compliance staff

They will get specialized training to be able to stay on top of new trends or changes that impact the organization and the way it manages risk. This will require attending conferences or AML-specific presentations to go into greater detail.

Supervisors and Managers

A higher level of instruction covering all aspects of money laundering, terrorist financing policies, procedures and regulations will be provided to those with the responsibility to supervise or manage the staff.

Senior management and board of directors

Money laundering issues and dangers will be regularly and thoroughly communicated to the board. This is to keep board members aware of the reputational risk that money laundering poses to the institution.

Refreshment training will be arranged at regular intervals to ensure that staff members are kept informed of current and new developments regarding money laundering and terrorist financing techniques, methods and trends. To demonstrate compliance with the aforementioned staff training, the Company will maintain records that include:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

15. Anti-Money Laundering Compliance Program

The Company maintains a structured AML/CFT Compliance program in accordance with Curaçao's AML legislation and CGA guidance. The program integrates internal controls, third-party services, employee accountability, and oversight mechanisms to ensure effective prevention and detection of money laundering and terrorist financing.

The Company has appointed a Money Laundering Reporting Officer (MLRO) who is responsible for overseeing the implementation of the AML/CFT policy.

The MLRO:

- Reviews internal alerts and suspicious activity reports
- Coordinates with third-party monitoring teams and escalates cases when required;
- Acts as the point of contact with the FIU Curaçao and regulatory bodies
- Reports periodically to Senior Management and Board of Directors
- To support its compliance efforts the Company engages:
- Devcode Identity AB for customer onboarding, identity verification, sanctions and PEP screening and source of funds/wealth checks;
- Elev8 Solutions Ltd for manual transaction monitoring, document authentication and customer behaviour analysis

While these third parties conduct technical checks and monitoring, the company retains full accountability for all AML obligations. The MLRO maintains direct oversight and reviews all red flags or escalated cases identified by Devcode or Elev8.

All relevant employees undergo initial background screening and periodic rechecks where necessary. Staff involved in compliance, customer due diligence, or handling transactions must complete mandatory AML/CFT training, refreshed at least annually. Training included legal obligations, red flag detection, proper escalation, and data handling protocols.

The Company shall ensure that its AML/CFT Program undergoes an independent audit every year in accordance with the requirements of the Curaçao Gaming Control Board (GCB). The audit shall be conducted by an external, qualified, and independent auditor. The final audit report, including all findings and required corrective actions, shall be formally submitted to Senior Management and the Board of Directors. The Board retains full accountability for the Company's AML/CFT framework and is responsible for reviewing audit outcomes, approving all AML-related policies, and ensuring that sufficient resources and staffing are allocated to maintain effective compliance.

16. Recordkeeping

The Company shall maintain all records related to customer due diligence (CDD), transaction monitoring, unusual transaction reports (UTRs), and customer communications for a minimum period of five (5) years from the date of the last transaction or the termination of the business relationship, whichever is later.

This includes, but is not limited to:

- Copies of customer identification and verification documents,
- Records of transactions (including attempted transactions),
- Internal and external correspondence related to AML matters,
- Risk assessments and decisions made on customer onboarding or offboarding.

All records shall be stored securely and in a manner that ensures timely retrieval and full accessibility by competent authorities (e.g., the FIU Curaçao or the GCB) upon request, in accordance with Curaçao's AML legislation and data protection requirements.

Annex I - Customer High Risk Factors

- ★ Irregular and different types of credits
- ★ Cash Intensive Transactions
- ★ Players who stem out of an industry which is considered to be prone to ML/FT such as Arms trade, Defence, Mining and Petroleum Industry
- ★ Players using virtual currencies (such as Bitcoin)
- ★ Players gaining their revenue from Forex services
- ★ Charitable Organisations
- ★ Players benefitting from residence rights or citizenship in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities, e.g. the Citizenship scheme offered in Malta and Cyprus by investment.
- ★ PEPs
- ★ Individual having otherwise prominent public positions
- ★ Players who are considered celebrities deriving from international sports, such as football players, basketball players, tennis players, etc.
- ★ High Spenders - having a high level of spending
- ★ Disproportionate Spenders - having a high level of spending which is disproportionate to their level of income or source of wealth.
- ★ Casual customers - this includes tourists, participants in junkets and local customers who are infrequent visitors.
- ★ Customers who are not regularly employed
- ★ Customers with unusual spending patterns
- ★ Multiple Player Accounts - some customers may have multiple accounts
- ★ Junkets

Annex II - Customer High Risk Factors

A non-reputable jurisdiction is one that has deficiencies in its national AML/CFT regime or has inappropriate and ineffective measures for the prevention of ML/FT.

In assessing the aforementioned elements, the Company has to take into account any accreditation, declaration, public statement or report issued by an international organisation which lays down internationally accepted standards for the prevention of ML/FT, or which monitors adherence thereto, as well as whether the jurisdiction has been included in the list published by the European Commission.

A significant distinction needs to be made between High Risk Jurisdictions and Non-Reputable Jurisdiction. While a non-reputable jurisdiction is always to be regarded as a high-risk jurisdiction, a high-risk jurisdiction may not necessarily always be regarded as a non-reputable jurisdiction.

The FATF identifies three types of Categories:

Category 1: Jurisdictions that have strategic AML/CFT deficiencies and to which countermeasures apply.

Category 2: Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies

Category 3: Jurisdictions with strategic AML/CFT deficiencies that have developed an action plan with the FATF and have made a high-level political commitment to address their AML/CFT deficiencies.

The FATF and any FSRB have the power to issue statements and/or declarations against a particular country or jurisdiction whenever such action is merited. When such statements are issued, the Company has an obligation to regard such a country as non-reputable until such time and as long as such statement is kept in force by the FATF.

Determining High-Risk Jurisdiction

The concept of high-risk jurisdictions goes beyond that of non-reputable jurisdictions, due to the fact that other risk factors which go beyond AML/CFT issues and shortcomings are calculated. The Company, in order to assess whether a jurisdiction is high-risk or not must take into consideration a number of issues which are non-exhaustive. An indication of such factors, which nonetheless are non-exhaustive, are the following:

- Level of Transparency & Rule of Law;
- Level of Corruption;
- War-torn countries/Civil unrest;
- Significant level/s & type/s of crime/s (jurisdictions known for high level of different types of crimes, including drug trafficking, arms trafficking, human trafficking, jurisdictions known to be a hub for terrorist groups);
- Significant level of terror threat;
- Mutual Evaluation Report (MERs) issued by the FATF or any FSRB; and
- Other notable sources