

AML COMPLIANCE

POLICIES & PROCEDURES

Policy Owner:	Playvision Group B.V
Version:	3.0
Approved by:	The Board of Directors
Approval date:	30.10.2025

DOCUMENT REVISION HISTORY

Version	Date Updated	Date Approved	Drafted By	Approved By	Description of Changes
v.1	09.01.2024	09.01.2024	Dr Josianne Cardona Gatt	The Board Of Directors	Drafted policy
v.2	20.06.2025	20.06.2025	Dr Josianne Cardona Gatt	The Board of Directors	Reviewed AML Policy. Updated Black List & Gray List in accordance with FATF Regulations issued on the 13 th June 2025
V.3	09.09.2025	30.10.2025	Dr Josianne Cardona Gatt	The Board of Directors	Reviewed policy and procedures to be in line with the new regulations issued by GCB which came into effect in January 2025

LIST OF ABBREVIATIONS

4 th 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
5 th 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	Financial Investigation Unit
GCB	Curacao Gaming Control Board
KYCMATIC	A holistic and automated Customer Due Diligence software, built and maintained by Diligex Ltd., which consolidates the AML/CFT regulatory measures for subject persons
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
CO	Compliance Officer
Non-reputable jurisdiction	A jurisdiction having: a. significant deficiencies in its national AML/CFT regime; b. 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 c. been identified by the European Commission in accordance with Article 9 of the 4th AMLD.
PEP	Politically Exposed Person, a natural person with <i>prominent public function</i> and includes: a. Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries; b. members of Parliament or similar legislative bodies; c. members of the governing bodies of political parties; d. 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; e. members of courts of auditors, or of the boards of central banks;

	f. ambassadors, <i>chargé d'affaires</i> and other high-ranking officers in the armed forces; g. members of the administrative, management or supervisory boards of state-owned enterprises; and h. anyone exercising a function equivalent to those set out in paragraphs (a)-(f) above within an institution of the EU or any other international body (incl. UN, World Bank). Family members of PEP: a. the spouse, or a person considered to be equivalent to a spouse; b. the children and their spouses, or persons considered to be equivalent to a spouse; and c. the parents. Close associates of PEP: a. 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 b. 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

Contents

1. Preamble	7
2. The Purpose, Scope and Aim of the Policy	8
2.1 The Purpose of the policy:	8
2.2 The aims and objectives of the AML Policy	8
2.3 The Objectives and Goals of the AML Policy	9
3. Overview	9
3.1 What is ML?	9
3.2 Money Laundering in Practice	10
3.3 What is Funding of Terrorism?	10
3.4 What is Proliferation Finance?	11
3.5 Targeted Financial Sanctions	12
4. The Risk-Based Approach	12
4.1 Business Risk Assessment	13
4.2 Customer Risk Assessment	14
4.2.1 <i>Customer Risk</i>	15
4.2.2 <i>Geographical Risk</i>	16
Determining High-Risk Jurisdiction	16
4.2.3 <i>Product, Service and Transaction Risk</i>	17
4.2.4 <i>Delivery Channels Risk</i>	17
<i>Technological developments risk assessment</i>	17
4.2.5 <i>Additional Risk Factors</i>	17
5. Customer Due Diligence ('CDD')	18
5.1 The CDD Measures	18
5.2 Identification and Verification	19
5.2.1 <i>Identification</i>	19
5.2.2 <i>Carrying out Customer Risk Assessment ('CRA')</i>	19
<i>Fig. 1 Customer Due Diligence Obligations</i>	21
5.3 Source of Funds and Source of Wealth	22
5.4 On-Going Monitoring	23
6. Simplified Due Diligence	25
7. Enhanced Due Diligence	26
7.1 Politically Exposed Persons	26
7.1.1 <i>Who is a PEP?</i>	27
7.1.2 <i>Risk Posed</i>	27
7.2 Suspicious of Stolen and Fraudulent Activity	28

7.2.1	Procedure	28
	<i>Fig. 3 Political Exposed Persons – Timeline</i>	29
8.	The Termination of the Business Relationship	29
9.	Reliance on Third Parties to Perform Customer Due Diligence	30
10.	Reporting of Unusual Transactions	30
10.1	Reporting Obligations	30
10.1.1	Recognition of Unusual Transactions	31
10.2	Reporting an unusual transaction.....	32
10.3	Reporting Procedures	33
10.4	Documentation of Unusual Transactions.....	35
10.5	Prohibition of disclosure – Tipping Off	35
11.	Anti-Money Laundering Compliance Program	36
11.1	What is an Anti-Money Laundering Compliance Program?	36
11.2	A system of internal policies, procedures and controls	36
11.3	Employee Screening Program and Ongoing Employee Training Program	37
11.3.1	New Employees.....	37
11.3.2	Audit Staff.....	38
11.3.3	AML Compliance Staff	38
11.3.4	Supervisors and Managers.....	38
11.3.5	Senior management and board of directors.....	38
11.4	An individual audit function to test the AML program.....	38
11.5	Examination by the Gaming Control Board	39
12.	The Appointment of a Compliance Officer	40
	Annex I – Geographical Risk	41
	Annex II – High Risk Products, Services and Transactional Risk	42
	Annex III – High Risk Interface/Delivery Channels	43

1. Preamble

As from February 2019 the Curacao Gaming Control Board ('GCB') was officially appointed the supervisory authority for AML/CFT compliance for the whole gaming sector. The **NOIS**, the **NORUT**, the **Sanction National Ordinance** and the **Kingdom Sanction Act** contain provisions for service providers to prevent such entities for being used for money laundering, financing of terrorism and the proliferation of weapons. These laws together with other international legislations and regulations are an integral part of the land-based and the online gambling licence requirements for the Curacao jurisdiction. **Playvision Group B.V** (hereinafter referred to as the '**Company**') attaches the highest importance to international and local efforts aimed at reducing financial crime.

The Company is committed to following the requirements of the money laundering legislation, including but not limited to:

- **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 Nation's Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s., and persons and organisations 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 Resolutions 1695 (2006t), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nation's 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)**

These laws and regulations and any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law form the main legal basis for the Curacao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons.

The Company responds to the Curaçao Gaming Control Board ('GCB') for any matters in relation to the any AML/CFT matters. The Company is obliged to report to the GCB any matter which involves or is suspected of involving any ML/FT.

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 an AML/CFT Policy and Procedures 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:

- i. Comply with the Anti Money Laundering legislations as mentioned here above;
- ii. Comply with CFATF;
- iii. Comply with any other legislation or recommendations, including those mentioned by the European Union ('EU') in relation to combatting ML and FT;
- iv. 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;
- v. to ensure that the Company complies with anti-money laundering legislations whenever it does business; and
- vi. 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:

- i. the Objectives and Goals that are to be pursued by this policy;
- ii. the tasks that are to be performed in fulfilling this policy and who is responsible for them;
- iii. the processes and reporting procedures to be applied; and

- iv. 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 criminal 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:

- Placement – the stage when the proceeds of crime are placed in the financial system;
- 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);
- 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 publishes 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 national level would be futile if it did not also take into account international coordination and co-operation. 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 co-operation 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 crim 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 operations¹.

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 terrorists 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 organisation to small, decentralise 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 cutting-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 they enable terrorists' assets to be frozen globally but also, they reduce terrorists' movement.

UN Security Council² oblige 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.

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,

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

² Resolutions 1267,1988,1989

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 goods³ used for non-legitimate purposes).

3.5 Targeted Financial Sanctions

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities. All natural and legal persons in Curacao are required to freeze without delay and without prior notice, the funds or other assets of designated persons and entities. This to comply with the United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. EU sanctions are binding for Curacao on the basis of the Kingdom Sanctions Act.

4. The Risk-Based Approach

The Company is obliged to implement a series of measures, policies, controls and procedures to prevent the financial system or other systems from being abused for ML/FT/FP. The risk of ML/FT/FP may vary from one sector to another, from one subject person to another, as well as from one business relationship, or occasional transaction, to the other.

The effectiveness of the risk-based approach depends on the proper understanding of the ML/FT/FP risk to which the Company is exposed. When speaking of Risk, it is intended the **inherent risk**, i.e. the risk that the Company is exposed to prior to adopting and applying any measures, policies, controls and procedures to mitigate the same.

To assess the risk, the Company is to identify and understand how the risk can manifest itself, giving the importance to the:

- i. **Vulnerabilities** – i.e. the weakness that may be exploited for ML/FT/FP purposes; and
- ii. **Threats** – i.e. the external elements that seek to exploit the Company's possible vulnerabilities.

In order to adopt a Risk-Based Approach the Company needs to take appropriate steps (in proportion to the nature and size of its business) to identify and assess the risks of ML/FT/FP, and to adopt controls, policies, measures and procedures to mitigate the risks identified. This calls for a **Business Risk Assessment** (hereinafter called the '**BRA**') to understand and assess the ML/FT/FP risks the Company is exposed to and **Customer Risk Assessment** (hereinafter called the '**CRA**') to assess the risks which the business will be exposing itself to when establishing business relationships with clients.

Applying the Risk-Based Approach means that the Company has to:

- Assess the risks that money laundering or terrorist financing may occur within its organisation beforehand
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks.

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.

- Monitor and improve the effective operation of these policies, procedures and controls
- Document the 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 casino offers and delivery channels, before determining what the level of overall risk is. Based on the risk assessment, the appropriate level and type of mitigation not be applied is determined. The Company will also take into consideration the outcomes of the National Risk Assessment (**NRA**) of the jurisdictions where it operates when it is to conduct a risk assessment.

4.1 Business Risk Assessment

Appropriate regards must be had to the **risk factors**, i.e. those variables that either on their own or in combination with each other may increase or decrease the ML/FT/FP risk posed by the Company.

The BRA is seen as the foundation of a risk-based approach. The BRA is the process whereby the Company identifies the threats and vulnerabilities that it is exposed to and assesses the likelihood and impact of ML/FT/FP risks. Based on this assessment, the Company will determine which areas to priorities in terms of AML/CFT/CFP and ensure that its AML/CFT/CFP measures, policies, controls and procedures are commensurate with the ML/FT/FP risks it faces to mitigate the same. Identification of ML/FT/FP risk is to be followed by an assessment of the same. Identification of ML/FT/FP risk is to be followed by an assessment of the same in considering the **likelihood** of risk manifesting itself and the **impact** that such manifestation would have on the Company.

The impact consists in the nature of seriousness of the resultant damage if a threat manages to exploit one or more vulnerabilities, and it can take a number of forms, including *reputational risk, business risk, regulatory risk, legal risk, financial loss and others*. **Likelihood** and **Impact** will lead to the determination of the level of **inherent risk**, the Company is subject too.

In determining the likelihood and impact of the risk(s), the Company will highlight the areas where the mitigating measures, i.e. its AML/CFT measures, policies, controls and procedures need to be the strongest to mitigate the level of inherent risk identified. After the Company's evaluation of what risks remains, following the application of the mitigating measures, then the Company will be in a position to quantify the **residual risks**.

Thus the:

$$\text{Level of Inherent Risk} - \text{Mitigating Measures} = \text{Residual Risk}$$

It is understood that after taking into consideration the residual risks, there still will be an amount of risk which cannot be addressed, avoided or controlled.

At this stage the Company has to consider whether the residual risk fall within the Company's **risk appetite**, i.e. whether the Company is prepared to accept that level of residual risk in the pursuit of its business objectives. Where the residual risk falls outside the risk appetite, the Company will need to revisit its mitigating measures to strengthen their efficacy and desist from pursuing that particular activity which falls outside the risk appetite.

The Company's risk appetite should never be more than what can effectively be mitigated through the mitigating measures of the Company.

The BRA will be carried out whenever there are any changes that warrant the carrying out of a revision/updating of the BRA. The methodology of the BRA and the scope will be described within the BRA itself as part of the literature needed to accompany the BRA.

4.2 Customer Risk Assessment

The CRA is an assessment of the risks that the Company will be exposed to in providing the services, either as one-off event (i.e. occasional transaction) or as a business relationship in the case of a repeat customer. The information collected to draw up the CRA is the customer's risk profile.

Based on the overall risk assessment of a customer, different risk mitigating measure, including Simplified Due Diligence ('SDD') and Enhanced Due Diligence ('EDD') measures can then be applied, in a manner that addresses the identified risks effectively. This is the reason why the CRA is to be carried out prior to entering any business relationship or carrying out an occasional transaction.

For ML/FT/FP purposes, the Company shall consider various risk factors when evaluating and verifying the information and documentation provided by customers and, depending on these, the Company will classify its customers as **Low, Medium, High** and **Critical**.

The risk factors which will be taken into consideration in carrying out a customer risk assessment are the following:

- **Customer risk** – i.e. the type of customer that the Company is engaging with.
- **Geographical risk** – i.e. the risk which the country where the customer resides or where he has any ties with, including but not limited to, business, place of habitual abode and family.
- **Products Risk** – this relates to the product that the Customer would have requested from the Company.
- **Interface Risk** – this relates how did the Customer came to know about the Company, i.e. through the internet, introducer, or agent.
- **Other Risk Factors** – these are any other risk factors which may have an influence on the Customer, such as *human error, transaction error, calamities, etc.*

The CRA 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.

The information collected to draw up the CRA will formulate the customer's risk profile. On the bases of the CRA, the proper level of Customer Due Diligence (**CDD**) can then be applied as stipulated in the Customer Acceptancy Policy (**CAP**). For this reason, it is important that the Company adopts a CAP. 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 level of customer due diligence measures, including ongoing monitoring, to be applied
- The circumstances under which service to someone is declined.

The Company will establish and maintain policies, procedures and controls to mitigate and manage effectively the risks identified in the operator's risk assessment of money laundering, terrorist financing and proliferation of weapons. The measures, policies, controls and procedures to mitigate ML/FT/FP risk shall include:

- i. CDD
- ii. Record keeping procedures
- iii. Reporting procedures
- iv. Risk management measures including Customer Acceptance Policies (CAP), Customer Risk Assessment (CRA) procedures, internal control, compliance management and communications of such policies, procedures and controls, employee training and employee screening policies and procedures.

It is important that these measures be clearly documented and approved by the Board of Directors. The Company will monitor the implementation of these controls and enhance them as needed. Enhanced measures will be taken in order to mitigate the risks where higher risks are identified.

The risk assessment will need to be documented and approved by the Board of Directors of the Company. It should also be made available to the GCB upon request. All aspects of the Business Risk Assessment should be covered, including:

- The methodology adopted
- The reasons for considering a risk factor as presenting a low, medium or high risk
- The outcome of the BRA
- Any information sources used

4.2.1 Customer Risk

Customer Risk is the risk of ML/FT/FP associated with entertaining relations with a given person or entity due to:

- a. the business or professional activity;
- b. the reputation; and
- c. the nature of the entity and the behaviour of the said person or, where applicable, of its beneficial owner.

Some activities may be considered as High Risk. These include cases when:

- i. Customers who have multiple sources of income;
- ii. Customers with irregular income streams;
- iii. PEPs;
- iv. High Spenders (money can be derived from illegal activities)
- v. Disproportionate spenders (inconsistent with the information given to the Company about the customer's known source of income/assets;
- vi. Casual customers like locals/tourists, especially when spending pattern changes
- vii. Improper use of third parties – criminal used third parties to gamble and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid CDD measures
- viii. Customers using multiple casino player rating accounts to hinder a casino to track their gambling activities.
- ix. Unknown customers (redeeming large amounts of chips/tokens)
- x. Junkets (junket operators monitor player activity and issue and collect credit)

4.2.2 *Geographical Risk*

The geographical risk is the risk posed to the Company by the geographical location of the player and the source of wealth of the business relationship. The nationality, residence and place of birth of the player are to be taken into consideration, as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organisations operating, are to be considered as high risk.

It is being recommended that the Company takes into recommendations a variety of sources of information produced by the FATF and well-known non-governmental well-known bodies. Some of these sources are listed in Annex I.

The FATF identifies three types of Categories:

Category 1: Jurisdictions that have strategic AML/CFT deficiencies and to which countermeasure 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 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 none the less 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

4.2.3 Product, Service and Transaction Risk

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation. The use by customers and the acceptance by casinos, whether land based or online casinos, of specific payment methods, which are considered to present a higher risk of ML/FT, can be looked at as high risk factors.

Annex II provides a non-exhaustive list of what is considered High Risk.

4.2.4 Delivery Channels Risk

The delivery channel, or interface risk, is the risk arising from how the Company interacts with the Customer and the channels it uses to provide a given product or service.

The channels through which a casino establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction. The following are examples of the channels which may impose a risk:

- Channels that favour anonymity
- Non-face-to-face business relationship
- Involvement of a third party in the interactions between the customer and the casino, especially in third parties that are not themselves subject to any from AML/CFT obligations.

Most customers are not met face-to-face. Therefore, other matters need to be looked at in order to identify whether a Customer is considered a high risk or not. **Annex III** provides a list of instances where the interface is considered High Risk.

Technological developments risk assessment

The casino will maintain appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing risks that may arise whenever:

- A new product is developed
- A new business practice emerges
- A new delivery mechanism becomes available
- A new or developing technology is used for both new and pre-existing products.

In these cases, a risk assessment needs to take place prior to the launch of the new products, business practices, delivery mechanisms or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism. Such risk assessment must be documented. Where risks are identified, measures will be taken to mitigate these risks.

4.2.5 Additional Risk Factors

The Company needs also to look at other factors which may substantiate a risk for the Company in accepting a client, which may vary in accordance to the client's circumstances.

The Company is aware that risk factors are not static and it is possible that the Company will have to consider additional or new risk factors over time, especially if it explores new products and markets.

5. Customer Due Diligence ('CDD')

The Company is prohibited from keeping anonymous accounts or accounts in obviously fictitious names. The casino is to identify the player and ask for the player's details and other relevant information to determine the purpose and nature of the business relationship. Without sufficient information, the casino will not be able to 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 casino 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 casino 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 to detect deviations from expected behaviour.

The extent and timing of CDD measures to be applied in relation to the customer, depends on the type of customer, product, service, transaction, delivery channels and geographical connections. The risk assessment undertaken at the beginning of the business relationship will determine the extent and timing of CDD measures which are to be applied by the Company, including the CDD information and the nature and frequency of ongoing monitoring.

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

- i. players engage in financial transactions equal to or above Naf. 4,000;
- ii. carrying out occasional transactions⁴ above the monetary equivalent of Naf. 4,000⁵;
- iii. there is a suspicion of money laundering or terrorist financing; or
- iv. they have doubts about the veracity or adequacy of previously obtained customer identification data.

Whenever an occasional transaction presents a high risk of ML/TF, the enhanced due diligence measures must be applied.

5.1 The CDD Measures

The CDD Measures to be taken are as follows:

- a. identifying the player and verifying the 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 will include understanding the ownership and control of structure of the customer;

⁴ An occasional transaction refers to a transaction with a one-off customer, that at the point, is not expected to return. This applies typically to land-based casinos, where no opening of an account is required to play.

⁵ 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.

- c. obtaining information on the purposes 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.

5.2 Identification and Verification

The Company requires to implement CDD policies and measures that include customer identification and verification procedures. **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 risk⁶.

5.2.1 Identification

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

- Name and surname of Customer
- Permanent residential address
- Date of birth
- Place of birth
- Nationality and
- Identity reference number where applicable.

However, in **low-risk** scenarios, the casino may limit identification to the information required under points (i) to (iii) above. On the other hand, in **high risk** situations, the casino may consider the collection of additional personal details as it might be necessary to mitigate the higher risk of ML/FT.

5.2.2 Carrying out Customer Risk Assessment ('CRA')

This is the evaluation of the customer in order 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 Customer Acceptance Policy ('CAP').

5.2.3 Verification This is requesting information and documentation to verify that a person really exists and that that person is the individual whom 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 must 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 document does not allow verification of the player's residential address, other documents like a bank statement, utility bill⁷, letter from a public authority or rental agreement, **not older than six months**, to verify the residential address. The player can also be contacted to verify the

⁶ If the player is required to open an account for playing demo games and that account can be used for paid games as well, the casino will need to collect personal information of the player at such stage.

⁷ For phone bills, only fixed line telephone bills are accepted as proof of address.

information supplied. Verification can also be done by checking social media, telephone directories, companies registries or media and news sources. Biometrics checks can also be used to confirm that the individual providing the document is the one described therein.

There are also circumstances in which the casino may do cross references to verify the information in its possession. This can be done with geo-location information, IP address data, funding method, etc.

Verification is carried out to determine that the player is who he declares himself to be. It is important that the documents are clear, legible and of good quality. Verification of evidence of identity implies a check whether the document presented is legitimate and that it has not been stolen from the true owner. If foreign documents are presented, extra care should be taken with regards to verifying its authenticity, particularly, when the type of document is unfamiliar.

When there isn't sufficient comfort that the identity of the player has been confirmed, additional measures need to be taken⁸.

5.2.4 Sanctions screening and PEP⁹ status screening

All players should be screened against sanctions lists of the United Nations and European Union. Should Curacao, in future, publish a local list with designated persons and organisations, this list should be taken into account along with the other international lists. No business cannot be carried out with customers that are subject to international sanctions. Before doing business or performing an occasional transaction for the first time with a player, the casino should check published lists of known or suspected terrorists or other sanctioned person or companies through:

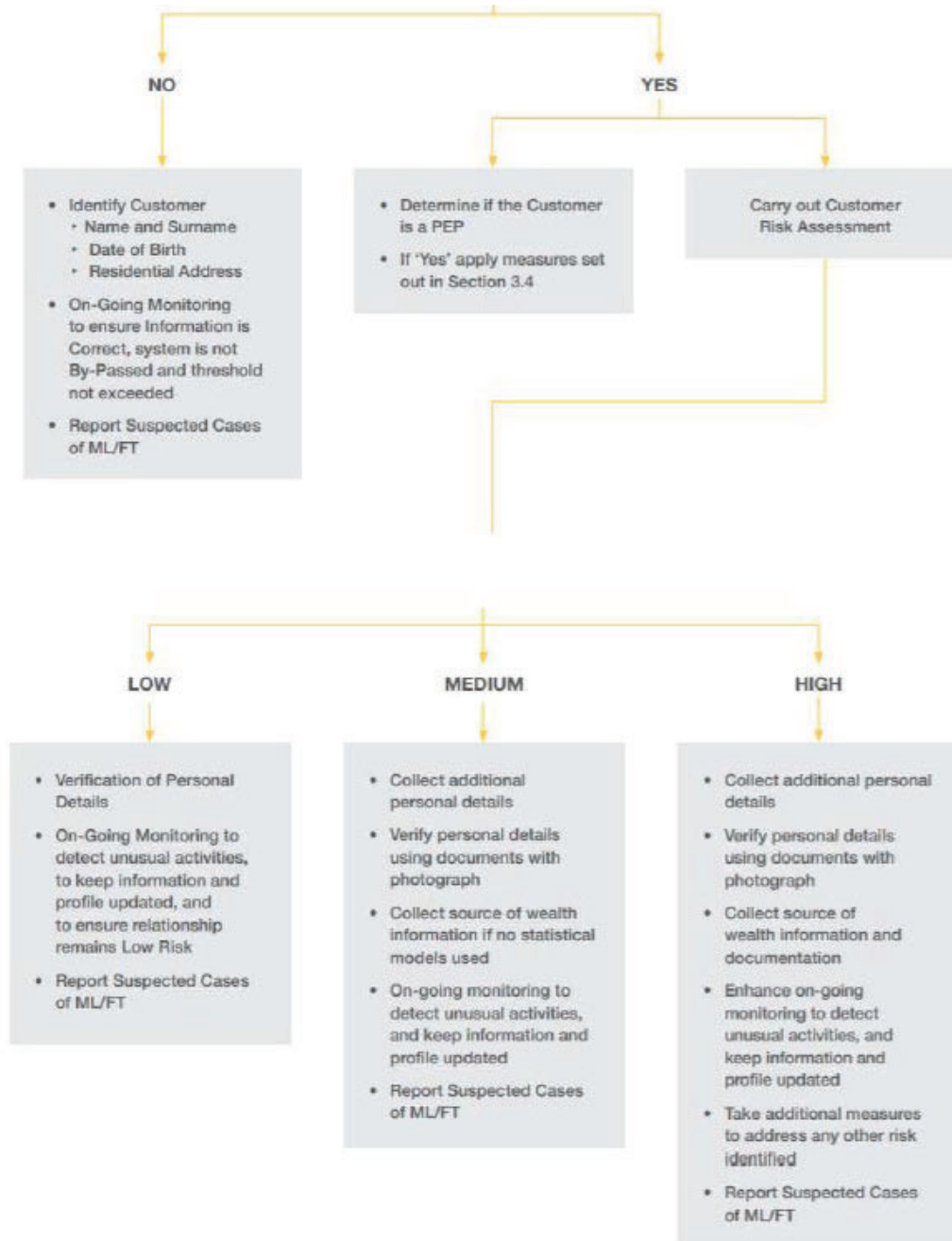
- UN Sanctions list
- EU Sanctions List

For PEP status screening, the casino can rely on internet search or consult reports and databases on corruption risk, like the Transparency International Corruption Perceptions Index, or on www.knowyourcountry.com. For local PEPs, the PEP Caribbean list can be consulted.

⁸ 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.

⁹ Political Exposed Persons

Fig. 1 Customer Due Diligence Obligations



5.2.5 Identification and Verification of the Beneficial Owner

The casino is obliged to require to identify and verify the identity of the beneficial owner. As a general rule, the casino should make sure that the customers have a registered account to play and transact on their behalf. This shall be achieved by including specific wording in the terms and conditions that the registered player must explicitly accept, together with a declaration form of a tick box that the player is registering in his own name, and not behalf of third parties. However, the sole declaration should not be sufficient to proof the veracity of what is being declared by the player, but the Company

has to ensure that there are enough ongoing procedures allowing for the detection of possible instances where the player is actually playing on behalf of third parties.

Even though the situation of a beneficial owner, is not so common with casinos, still such a scenario cannot be left unnoticed, as there could be instances where business relations are funded by syndicates.¹⁰ In such case syndicates will be considered as beneficial owners and therefore, their identity must be verified.

Where the player accounts used by companies (corporate accounts) to hedge matchbook exposure, the applicable beneficial ownership requirements relate to the beneficial owners of the companies/operators registering those accounts. It is necessary to distinguish between an ordinary gaming account belonging to a consumer, and such other accounts being of a different nature.

In case of business participants satisfactory evidence must be obtained to identify these business participants. Reasonable steps need to be taken to verify the identity of the beneficial owner, using information or data that was obtained from a reliable source. At the minimum identification information, verification evidence must be gathered for all persons holding 25% or more of the customer. Where no natural person is identified, the natural person who holds the position of senior managing official needs to be identified.

Obtaining information on the Purpose and Intended Nature of the Business Relationship

One of the requirements of CDD is to understand why a prospective customer is seeking to acquire a specific service or product from them. In the gambling sector, the reason why an account has been opened, it is very self-evident, and therefore, there is no need to obtain any further information about this.

A customer risk profile needs to be carried out in order to have sufficient information available to allow the detection of unusual activity during the business relationship. Sufficient information and necessary documentation needs to be collected in order to establish a customer's source of wealth and expected level of activity.

5.3 Source of Funds and Source of Wealth

Source of Wealth ('SOW') consists of determining the activities which generate the customer's net worth and whether this justifies the projected and actual level of account activity. As to the extent of the information needed, it is essential that this reflects the level of ML/FT risk identified through the customer risk assessment.

Where the risk is not high, a declaration from the customer with details describing the nature of employment/business/income is sufficient. Social media information can also be used as a source of information.

¹⁰ In the case of syndicates, the funds being wagered are collected from multiple persons who will eventually share in any winnings. In such instance the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding.

However, where the risk of ML/FT is higher or there are doubts as to the veracity of the information collected, the information obtained will need to be substantiated by independent and reliable information and documentation.

In developing the customer risk profile, statistical data may also be used to develop behavioural models against which to eventually gauge customer's activity rather than collect source of wealth information. Should this method be adopted, then the data collected by the Central Statistics Department, such as average national income, average disposable income, etc. can be used. These indicators will provide the necessary information to determine the average wagering power of players from a given jurisdiction.

Furthermore, taking into consideration the data collected over a period of time by the Company, can be used in order to create a profile of an average player. It is important to understand that the statistical data is not of the individual player, but to statistical data obtained from a range of players.

Statistical data cannot be used when the customer is considered as a high risk client. This is due to the fact that the transactional pattern will deviate from the average behavioural model. In such circumstances, the normal source of wealth information must be collected, i.e. supportive documents proving the source of wealth.

Source of Funds ('SOF') refers to the origin of the funds used in a particular transaction or to be used in future transactions. This should not simply be restricted to knowing from which Bank or Investment Firm the funds may have been received. The information obtained should be relevant and should be able to establish the fund's origin and the method/circumstances under which the funds were acquired.

5.4 On-Going Monitoring

Ongoing due diligence on the business relationship and scrutinising the transactions undertaken throughout the course of the business relationship is a must in order to understand the customer, the customer's business and risk profile.

5.4.1 Ongoing Monitoring of Identity

In conducting ongoing due diligence on the business relationship, it is important to hold accurate and up-to-date identification data of the customers. Since identity may change due to circumstances, there needs to be in place enough control to understand whether there is a change of identification and that such change is detected and re-evidenced in a timely manner. Evidence of identity will be obtained periodically to detect any changes, refresh the data on key events (i.e. change of payment instrument). Also, there needs to be enough control tracking the expiry dates, by refreshing the evidence upon expiration of the identity document. Should there be substantial changes, which award a reassessment of the business relationship, then should there be a change in the risk factor, the appropriate due diligence needs to be requested.

5.4.2 Ongoing Monitoring of Transactions

Transaction monitoring is executed to prevent involvement with ML/FT and to safeguard the reputation of the Casino. Should it be discovered that a customer's transactions are not consistent with what is known to be the usual customer's behaviour, those transactions need to be questioned,

and where necessary the source of funds used for those transactions, need to be established. There should be an understanding what the reason for this deviation is and obtain sufficient information and documentation regarding the transaction. Upon gaining more information, the relationship has to be re-evaluated and should the transaction result in being a suspicious one, a report to the FIU should be filed by the Compliance Officer.

The level of on-going monitoring will depend on the risk profile of the customer, but even in low-risk situations there should always be a degree of oversight taking place to ensure that the business relationship still maintains the same low risk profile.

5.4.3 Timing of CDD Measures

Verification and identity is to be conducted when engaging in financial transactions equal to or in excess of **Naf. 4,000** (equivalent to EUR 1,904). This implies that all CDD measures must be conducted at the time that the threshold is reached. However, a minimum amount of CDD measure must be applied prior to reaching the threshold. Thus simultaneously with the opening of an account, the identification of the customer must be obtained. This is done by collecting the minimum personal details, being:

- Name and Surname
- Permanent Residential Address
- Date of Birth

Along with this minimal information, the PEP status screening and sanctions screening must be conducted.

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, including any peer-to-peer transfers. Once the threshold is reached, a customer risk assessment must be conducted and decide what further information needs to be obtained from the customer, in order to decide whether the simplified or enhanced due diligence is needed.

In carrying out the CDD measures, the customers will still be allowed to continue using their gaming account, while all the necessary information is being obtained. However, if the threshold is reached because of a deposit of the players, the player won't be able to make further deposits, until such time that the CDD measures have been completed satisfactorily.

On the other hand, if whilst conducting the due diligence, the players wishes to withdraw funds and such withdrawals reach the threshold mentioned here-above, then the player's account will be completely frozen, and the player will be prohibited from playing any further, until such time that the Due Diligence process is completely and satisfactorily completed.

Should the requested information not be provided within **30 days** from the initial request, i.e. from when the player would have reached the NAF. 4,000 thresholds, the relationship with the player will

have to be terminated and a report with the FIU needs to be filed if a presumption of ML/FT exists. If no presumption of ML/FT exists, the funds will be transferred to the same bank account or wallet it was deposited from. If presumption of money laundering or terrorist financing exists, a mechanism will be imposed, whereby the funds are blocked or not, keeping in consideration, that by blocking the funds, the customer could be tipped off¹¹.

6. Simplified Due Diligence

Where the risks of money laundering or terrorist financing are lower, the Casino is allowed to conduct simplified CDD measures, which should take into consideration the nature of the lower risk into account. The application of SDD is **not an exemption** from carrying out CDD but rather a variation of the extent and timing of CDD to be applied in view of the lower risk of ML/FT that the circumstances present. When applying CDD measures the following may be adjusted:

- i. The timing of CDD – postponement of the verification of identity or other CDD measures until a pre-determined threshold or other triggering event is reached;
- ii. The quantity and quality of information and/or documentation obtained for verification of identity and other CDD measures.
- iii. The frequency and intensity of ongoing monitoring. The level of ongoing monitoring should always be sufficient to a degree that can determine whether the circumstances on the basis of which it was decided to apply SDD are still current.

The following are examples of possible measures to be undertaken when conducting simplified due diligence:

- Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary to obtain the player's identity. Therefore getting the name and surname, address and date of birth.
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship.
- Adapting verification to perceived risk. The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low risk situation, the Casino can 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).
- Limiting the extent of personal details to be verified. In low risk situations, the Casino must verify the basic identification details, and not any other information is necessary. However, such documentation/verification shall be that the Casino is comfortable with the amount of information collated.
- 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.

¹¹ Tipping Off means to illegally disclose information about a money laundering or terrorist financing investigation, which could compromise the investigation itself.

7. Enhanced Due Diligence

Enhanced Due Diligence (EDD) needs to be applied on a risk-sensitive basis, in those situations that, by their nature, represent a higher risk of ML/FT. In essence, EDD measures are additional measures to CDD measures, which are to be applied to ensure that the higher risks represented by certain customers, products, services or transactions are better monitored and managed to avoid any involvement in ML/FT. EDD must be consistent with the business relationship, in order to determine whether transactions or activities appear unusual. EDD must be conducted where the risk of money laundering or terrorist financing are higher. This concerns for example:

- Residents of higher risk geographic areas
- Political Exposed Persons (PEP)
- Products or transactions that might favour anonymity
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

Whereas the Company may choose as to when apply SDD or not, EDD measures are mandatory to be applied in any situation that presents a higher risk of ML/FT and in any other scenario when the application of these measures is mandated by law.

The applied measures must be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether transactions or activities appear unusual or suspicious. Examples of EDD 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 source 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 has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

7.1 Politically Exposed Persons

Politically Exposed Persons ("PEPs") are individuals who are or have been entrusted with prominent public functions.

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.

7.1.1 Who is a 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 d'affaires* 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 PMLFTR, 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.

7.1.2 Risk Posed

PEPs pose a high risk of ML/FT due to the position they occupy and the influence they exercise. PEPs may abuse of 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. However the Company is not required to turn away any prospective customers or close a business relationship on the basis that the prospective customer or the customer or beneficial owner is a PEP or a family member or a close associate.

However, if after evaluating the customer and carrying out a Customer Risk Assessment of the customer or the potential customer, it results that the prospective business relationship falls outside its risk appetite, then the Company has to decline or close the business relationship.

The Company when establishing or continuing a business relationship with a PEP shall:

- Require the approval of senior management;

- Take adequate measures to establish the source of wealth and source of funds; and
- Conduct the necessary enhanced ongoing monitoring of such business relationship

Furthermore, in addition to the above mentioned requirements, due to the nature of business, being long-term insurance, the Company shall take reasonable measures to determine whether the beneficiaries of a policy and where applicable, the beneficial owner of the beneficiary are PEPs, which measures shall be taken no later than the time of pay-out or the time of the assignment, in whole or in part, of the policy.

Provided that where the beneficiaries of the policy or where applicable the beneficial owner of the beneficiary are PEPs, senior management should be informed before proceeding with the pay-out under the policy and enhanced scrutiny shall be conducted of the entire business relationship with policy holder.

Should the Company suspect a degree of higher risk of money laundering or funding of terrorism, the MLRO of the Company should be informed and the MLRO of the Company should consider as whether such suspicion is sufficient to warrant a report to the FIAU or not.

In line with the above, the Company is required to ensure that:

- The PEP declaration is duly completed; and
- All identification details on natural persons (whether individual customers or beneficial owners) are collected to ensure proper screening through KYCMATIC.

7.2 Suspicious of Stolen and Fraudulent Activity

When there is 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.

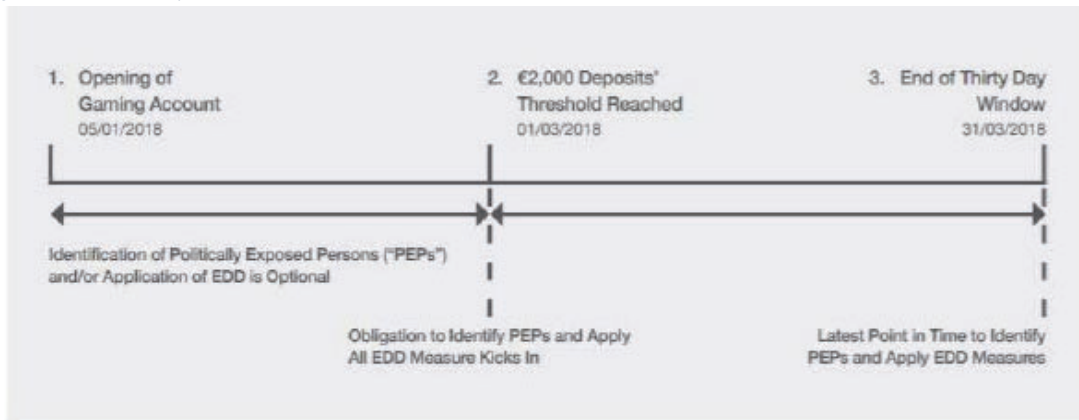
As soon as suspicion rises all documents must be screened, even though the account would be below threshold. Until such time as the due diligence is carried out, Customer's account will be blocked and the Customer will not be in a position to withdraw any funds. Should the requested documents not be 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 whether a Suspicious Transaction Report ('**STR**') will be filed or not with the relevant authorities.

7.2.1 Procedure

- Timeframe when clients meet the EUR 2,000 threshold – the Company implements the above mentioned measures and the once mentioned in Annex I at any point in time between the establishment of the business relationship and the point in time when the EUR 2,000 threshold is met, but **not later than 7 days from when the said threshold is met.**
- If the player has money on the account, the account will be blocked and amount will be returned to the player upon due checks have been finalised.
- If the player has bonus, bonus will be cancelled and deposit amount will be returned to player.
- Players who reach the EUR 2000 threshold need to be screened through KYCMatic.
- PEPs are not accepted.
- Should a PEP be identified, managerial personnel needs to be informed.

- PEP accounts must be closed immediately as soon as through checks it results that the account belongs to a PEP.

Fig. 3 Political Exposed Persons – Timeline



8. The Termination of the Business Relationship

In case the obligations arising from the CDD's requirements cannot be met, the Casino cannot establish a business relationship with that customer or perform the transaction and is obliged to terminate the business relationship with the customer. A record of all the attempts made to get the necessary information and documentation must be kept by the Casino. In such an instance the Casino has two (2) options, either to:

- close the account belonging to that particular customer; or
- block and suspend the account in its entirety.

In the event that the customer makes the requested information and/or documentation available to the Casino, following the closure or the suspension and blocking of the gaming account, the Casino has to 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 Casino is to 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 should be automatically equated to a suspicion of ML/TF/FP. The Casino needs to 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 Casino will need to submit an unusual transaction report to the FIU with regard to that particular customer.

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

9. Reliance on Third Parties to Perform Customer Due Diligence

The Casino may rely on third parties when performing elements of Due Diligence (name, date of birth and nationality), providing that the criteria mentioned here below are adhered to:

- i. the third party should be subject to CDD and record-keeping requirements as those that the Casino is subjected to.
- ii. the third party has to have an ongoing business relationship with the customer, which is independent from the relationship to be formed by the customer with the Casino.

Where such reliance is possible, the ultimate responsibilities for CDD measures remain with the Casino. The criteria to be met are as follows:

- a. the Casino has to obtain the information concerning the elements mentioned above immediately from the third party it is relying upon.
- b. The Casino has to have an agreement with the third party being relied upon that copies identification data or other relevant documentation relating to CDD requirements will be made available upon request.
- c. This arrangement of reliance between the Casino and the third party has to be tested from time to time to ensure that it functions as set out in the agreement. However, the Casino remains ultimately responsible for the carrying out of a customer-based risk assessment, determining whether the customer is a PEP and conducting on-going due diligence.
- d. The Casino needs to satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with CDD and record keeping requirements.
- e. The third party must have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution and would apply its own procedures to perform CDD measures.
- f. When determining in which countries the third party that meets the conditions can be based, the Casino needs to have regards to information available on the level of country risk.

10. Reporting of Unusual Transactions

10.1 Reporting Obligations

The Casino 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. It is important that the Casino 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.

10.1.1 Recognition of Unusual Transactions

An unusual transaction is a transaction inconsistent with the player's profile. Therefore, the first key to recognise that a transaction or series of transactions is unusual is to know enough about the player. The purpose of collecting player information is to provide the casino 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 of which the Casino needs to assess whether a customer's transaction qualifies as an unusual transaction. All the unusual transactions should be reported to the **Compliance Officer**. All documentation relating to such unusual transactions should be provided to the Compliance Officer together with the reporting form for the unusual transactions form¹².

The Compliance Officer is to keep an appropriate record of the transactions reported. Should the unusual transactions be not reported to the FIU, then the Compliance Officer needs to enter in the Unusual Transaction Reporting form the reason why such transaction was not reported to the FIU and signed off by the Compliance Officer or Management.

Special attention needs to be given to all complex, unusually large transactions, and all unusual patterns of transaction, which have no apparent economic or visible lawful purpose.¹³

The following transactions or intended transactions are deemed unusual¹⁴:

- i. transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice.
- ii. 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 Ordinance¹⁵.
- iii. Transactions in the amount of Naf. 5,000 or more, regardless 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 cashless transaction in the amount of Naf. 5,000 or more¹⁶
 - Accepting or releasing a deposit in the amount of Naf. 5,000 or more¹⁷

¹² See Annex II for the Unusual Transaction Report Form

¹³ This is to reflect the FATF recommendation 11

¹⁴ Ministerial Decree with general operation of December 1, 2015, laying down the indicators as mentioned in Article 10 of the NORUT (Decree Indicators Unusual Transactions)

¹⁵ N.G. 2014 no. 55

¹⁶ A cashless transaction is a transfer from a bank account of the Casino to a local or international bank account, at the request of the client.

¹⁷ Chips include but is not limited to tokens and credits

- A cashout in the amount of NAf. 5,000 or more¹⁸

It is to be noted that 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 or more and is considered per gaming day.

iv. 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.

10.2 Reporting an unusual transaction

By virtue of Article 11 of the NORUT, the Casino must report unusual transactions or any intended unusual transactions to the FIU without delay. To be able to do this, the Casino needs clear procedures for internal and external reporting of unusual transactions in place.

In order to be able to report any unusual transactions, the Casino shall apply the following systems:

i. Customer Due Diligence:

Before monitoring can begin the Casino must have a robust Customer Due Diligence practice, in order to verify who the customer is:

- **Identity verification** – The Casino has to obtain and verify government-issued ID, proof of address and date of birth.
- **Enhanced Due Diligence (EDD)** – For High-Risk customers or large transactions (e.g. politically exposes persons) a stricter requirement for Due Diligence is needed.
- **Ongoing Monitoring** – The Casino must continuously assess player activity for consistency with their known profile.

ii. Automated Transaction Monitoring Systems:

The Casino will implement automated systems that:

- Track all deposits, withdrawals, and bet sizes in real time
- Flag unusual or suspicious activity, such as:
 - Rapid deposit and withdrawal cycles (possible money laundering)
 - Use of multiple accounts or payment methods
 - Sudden changes in betting behaviour or spending limits
 - Structuring transactions to avoid reporting thresholds.

The system will also generate alerts for manual review by the compliance officer.

iii. Risk Based Approach

Transactions will be monitored based on risk levels:

- Low risk – Small, consistent amounts within normal gaming activity

¹⁸ The indicated examples are not limited, also credit card transactions and e-wallet transactions are to be reported to the FIU.

- Medium risk – Moderate increases in betting or frequent deposits
- High risk – Large or irregular transactions, cross-border payments, or use of third-party payment methods.
- The Casino has implemented the trigger that when a threshold reaches the NAF. 5,000, then an automated notification will be issued to the transaction monitoring team and following that the transaction monitoring team will review whether such transaction is suspicious or not.

iv. **Record Keeping and Audit Trail**

- The Casino will maintain records of all transactions, including date, amount, method and linked player accounts.
- Customer identification documents and transaction logs are retained by the Casino for at least five (5) years.
- The Casino will keep detailed logs of alerts, investigations and actions taken.

v. **Compliance Oversight**

The designated Compliance Officer must oversee;

- The monitoring system setup and tuning
- Review flagged transactions
- Report to regulators any irregularities
- Will train staff on AML/CTF.

Also the Casino will be subject to regular reviews and audits by independent auditors.

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

10.3 Reporting Procedures

In cases where an employee of the Company knows, suspects or has reasonable grounds to suspect that:

- funds are the proceed of criminal activity; or
- a transaction may be related to money laundering or the funding of terrorism; or
- a person may have been, is, or may be connected with money laundering or the funding of terrorism; or
- money laundering or the funding of terrorism has been, is being, or may be committed or attempted, he/she is required to submit an Internal Report to the Compliance Officer, within 1 working day of becoming aware of such suspicion or action. The information provided to the Compliance Officer shall be as follows:
 - a. Name of the Person Compiling the Report;
 - b. Date when the report is being compiled
 - c. What kind of incident it relates to, i.e. ML, FT, Bribery, Tax Evasion; Financing Proliferation;
 - d. The Customer's name;

- e. The Customer's account number;
- f. A detailed description of the incident which has occurred;
- g. Whether it is mere suspicion or whether an actual act has been done;
- h. Date when the official has become aware of the incident;
- i. What actions had been taken;
- j. Date.

In order for the Compliance Officer to consider all relevant material in respect of an internal report the following should be made available to the Compliance Officer:

- Previous transactions, transaction patterns and volumes, previous patterns of instructions, the length of the business relationship and CDD information;
- Where possible, other connected accounts and the existence of other relationships including where the person is suspected of ML/FT;
- Situations where there is no commercial rationale for the customer buying the product he seeks;
- Requests for any complex or unusually large transaction which has no apparent economic or lawful purpose;
- Requests to associate undue levels of secrecy with a transaction;
- Situations where the origin of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broker and/or unnecessarily layered;
- The unwillingness of customers who are not private individuals to give the names of their real owners and controllers.

The Compliance Officer will then consider, without delay, every internal report he/she receives in order to determine whether or not the information contained in the report:

- does give rise to the knowledge or suspicion of ML/FT or
- whether additional information is necessary to reach such a determination.

Should the Compliance Officer conclude that it has enough information to file a report to the FIU through the goAML systems, without any delay, when the knowledge or suspicion subsists. STRs should be submitted through the goAML platform and should include all the relevant identification and other supporting documentation. An STR log should be retained by the Compliance Officer whereby all information as to the STR being filed is registered and the documents submitted in relation to that particular STR is to be retained on file. The STR log will only be accessible to the Compliance Officer. A report of the number of STRs filed should be presented to the Board of Directors on a periodical basis, without disclosing any of the details in relation to the specific STRs filed. In the case where an incidence report is provided to the Compliance Officer for assessment as whether to proceed to file an STR, but the Compliance Officers considers that there is not sufficient evidence to substantiate the filing of an STR, then the Compliance Officer is under obligation to record such decision in a log whereby it provides information as to why the STR was not filed and what action was taken in that regards.

Note: A customer should automatically be classified as a high-risk customer if he is subject to sanctions or other economic measures. In these instances, caution should be exercised in providing services depending on the measures that the person is subject to.

10.4 Documentation of Unusual Transactions

As part of the new regulations, each Casino needs to register with the FIU and obtain access to the goAML reporting portal after validation by the FIU.

The Compliance Officer will prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The Casino will report to the FIU the details of these transactions by means of the goAML reporting portal. The reports and the submission of the thereto related information (all supporting documents) should be done in English.

The Casino 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. This is done in order not to jeopardise any investigation being done. This is also the reason

10.5 Prohibition of disclosure – Tipping Off

The Casino and its senior management and employees shall not disclose any details or information in connection with a report filled to the FIU or a request for information made by the FIU. Disclosing information and other information is not permitted by the Casino or any of its officers to third parties. The same caution needs to be exercised when terminating a relationship or otherwise block additional transactions following reporting to the FIU. Drastic action should only be taken when there is no other way out since any unjustified action may alert the player. In such circumstances, it would be more advisable to increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/TF.

10.6 Record Keeping

The Casino shall maintain for at least five (5) years, all necessary records on transactions (both domestic and international), to enable them to comply with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

All records obtained through CDD measures (e.g. copies of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five (5) years after the business relationship is ended, or, after the date of the occasional transaction.

The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority.

11. Anti-Money Laundering Compliance Program

11.1 What is an Anti-Money Laundering Compliance Program?

An Anti-Money laundering program is an essential component of the Casino's compliance regime. The primary goal of every good program is to protect the organisation against money laundering and to ensure that the organisation is in full compliance with relevant laws and regulations. For this reason, designing, structuring and implementing this program should be a priority in order to safeguard the interests of the Casino.

Thus the Company together with the Director and the Compliance Officer designed the AML program, establishing the minimum standards of organisation that are reasonably designed to comply with applicable laws and regulations. The organisation-wide program is to be implemented by the policies and procedures related here to.

Before designing the AML program, it was imperative to understand what was required of the institution, its employees and customers in accordance with the laws and regulations of Curacao.

The basic elements that the Casino is trying to address, in implementing the AML Program, are the following:

- A system of internal policies, procedures and controls;
- A designated compliance office with day-to-day oversight over the AML program;
- An employee screening program and ongoing employee training program; and
- An independent audit function to test the AML Program.

The AML Program also ensures that the obligations regarding customer due diligence, reporting unusual transactions, retention periods, data protection and training are met. The Casino must on a continuous basis test the AML Program and adapt such program to the current risks that might arise within the company's own organisation. The AML program must be presented to the Board of Directors and Senior Management for their approval.

11.2 A system of internal policies, procedures and controls

The Casino has policies and procedures, including a policy statement that clearly expresses the Casino Senior Management's commitment to combat the abuse of its facilities, products and services for the purpose of Money Laundering, terrorist financing and the proliferation of weapons of mass destruction purposes. The policies state the Casino's intention to comply with current AML, CFT and the financing of proliferation legislation as well as regulations, in particular the laws and regulations regarding customer due diligence¹⁹. Such policies are there to offer guidelines upon which the Company needs to act in order to combat ML/FT/FP and safeguard its operations.

¹⁹ NOIS, NORUT, Sanctions National Ordinance, Kingdom Sanction Act

The Casino must be updated on the changes in regulations, both internationally and nationally. The policies and procedures will need to be updated with the amendments issues in the local and international legislations.

Whilst policies and procedures provide important guidance, the AML program also relies on a variety of internal controls. These internal controls should enable the compliance officer to recognise deviations from standard procedures and protocols.

The AML policies and procedures should always be kept in writing and shall always be presented to the Board of Directors for their approval. Any changes which effect the employees' knowledge, the employees should be informed about these said changes. The AML program also relies on a variety of internal controls. These Internal controls, enable the Compliance Officer to recognise deviations from standard procedures and protocols.

The AML Program will be in a written format and shall be approved by senior management or the Board of Directors. All employees should be made aware of all the policies and procedures related to AML/CFT.

11.3 Employee Screening Program and Ongoing Employee Training Program

The Casino has to ensure that its business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. The Casino must establish and adhere to proper policies and procedures in screening its employees for criminal records.

A training program will be developed and provided to all personnel who handle transactions that may be qualified as unusual based on the indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions²⁰.

Training includes setting out rules of conduct governing employees' behaviour and their ongoing education to create awareness of the Casino's policies against money laundering and terrorist financing. Most areas of the institution will receive training, and the target audience will include most employees. However, each segment should be trained on topics and issues that are relevant to them. Training will at least address the following topics:

11.3.1 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 office must be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority. New employees will be made aware of the existing internal policies, procedures and regulations concerning

²⁰ N.G. 2015 No. 73

money laundering, terrorist financing, proliferation of weapons and the reporting requirements. The new entries will be trained on the money laundering methods and trends in the gambling sector. They will receive an explanation on customer due diligence and objective and subjective indicators for reporting unusual transactions.

11.3.2 Audit Staff

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

11.3.3 AML Compliance Staff

These are the people who run the AML program. They will need specialised training to be able to stay on top of new trends or changes that impact the organisation and the way it manages risk. This will require attending conferences and training courses.

11.3.4 Supervisors and Managers

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

11.3.5 Senior management and board of directors

Money laundering issues and dangers should 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 is to 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 aforementioned staff training guidelines, the Casino has to 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.

11.4 An individual audit function to test the AML program

The AML compliance program is to be monitored and evaluated at least **annually** by an adequately resourced internal audit department or an outside independent party. The audit must be independent, thus performed by people not involved with the organisation's AML compliance staff.

Those performing the audit must be sufficiently qualified²¹ to ensure that their findings and conclusions are reliable. These tests must include at least:

- An evaluation of the institution's anti-money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The audit team will also consider whether the board was responsive to earlier audit findings. The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or the Board of Supervisory Directors, and to the designated officers with a request to take prompt corrective actions by a certain deadline. These corrective actions could also include enhancement of controls and procedures.

11.5 Examination by the Gaming Control Board

The Casino shall provide all information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the GCB in preparation of or during an examination and upon GCB request during the year. The following items should be made readily available:

- The written and approved AML Compliance Program on money laundering, terrorist financing and financing of proliferation;
- Records of its Business Risk Assessment;
- The name of each Compliance Officer responsible for the casino's overall money laundering and terrorist financing policies and procedures and his/her designated job description;
- Records of reported unusual transactions;
- Records of unusual transactions which required closer investigations;
- Records of frozen accounts
- Schedule of the training provided to the casino's personnel regarding money laundering, terrorist financing and proliferation of weapons;
- The assessment report on the casino's policies and procedures on money laundering, terrorist financing and financing of proliferation by the internal audit department or an external auditor; and

²¹ The auditor must have at least two years of experience in AML/CFT compliance along with a bachelor's degree and a relevant AML certification. Recognised certifications include the CAMS or CAMS-Audit certification from the ACAMS or AMLFC certification from the AML Foundation and Compliance Institution

- The customer's files including customer risk assessment, CDD, customer acceptance and transaction information.

12. The Appointment of a Compliance Officer

A person designated by the Casino as Compliance Officer shall officially be chosen and such person shall be considered as a Senior Officer, who shall be independent and of sufficient authority to make the necessary decisions to safeguard the Casino. The Compliance Officer ('CO') shall be responsible for the detection and deterrence of money laundering and terrorist financing. The AML/CFT CO must have timely access to customer identification data and other CDD information, transaction records and other relevant information. The Compliance Officer must be able to act independently. The CO shall be assigned the following responsibilities:

- 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 organise training sessions for the staff on various compliance-related issues;
- To analyse 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 design an internal procedure about when reporting of unusual transactions will lead to blocking/freezing of user accounts, taking into account the risk of tipping off the player;
- 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.

Annex I – Geographical Risk

A non-exhaustive list of sources of information produced by the FATF and well-known non-governmental bodies which indicate which countries have deficiencies in AML/CFT:

- Countries on the FATF list of High-Risk Jurisdictions subject to a Call for Action
- Countries on the FATF list of Jurisdictions under Increased Monitoring
- Countries on the CFATF Public Statement
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR)
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime
- Countries sanctioned by the OFAC
- Countries identified by credible sources providing funding or support for terrorist activities or having terrorist organisation operating with them
- Countries on the Corruption Perception Index compiled by Transparency International.

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.

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 Company does not accept any player from FATF's Blacklisted and Gray Listed Countries. Such list has been updated as at the 13th June 2025.

Black Listed Countries:

- Myanmar
- Iran
- Democratic Republic of Korea

Gray Listed Countries:

- Algeria
- Angola
- Bolivia
- Bulgaria
- Burkina Faso
- Cameroon
- Cote d'Ivoire
- Democratic Republic of the Congo
- Haiti
- Kenya
- LAO PDR
- Lebanon
- Monaco
- Mozambique
- Namibia
- Nepal
- Nigeria
- South Africa
- South Sudan
- Syria
- Venezuela
- Vietnam
- Virgin Islands (UK)
- Yemen

Annex II – High Risk Products, Services and Transactional Risk

These may include:

- Proceeds of crime – risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer.
- Anonymous payment methods, such as pre-paid cards and virtual assets
- Use of casino accounts – this should only be done for gambling purposes and not to deposit and withdraw without gambling or after minimal play.
- Types of specific games (e.g. roulette, craps, bets)
- Peer to Peer gaming
- The use by customer of accounts held or cards issued in the name of third parties
- The transfer of funds from one gaming account to another
- Types of financial services (cred/marker, currency exchange)
- Multiple casino accounts or wallets (internet operator may own and control multiple websites)
- Changes to financial institution accounts to fund casino account
- Identity fraud. Details of financial institution accounts stolen and used on websites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on websites

- Games involving multiple operators (poker on platforms shared by multiple operators)
- Electronic wallets (e-wallets). Not all e-wallets are licensed in reputable countries, and several e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction issued statements may only record the payment to the e-wallet, not the transaction to the casino. This may be useful for dishonest customers who wish to disguise their gambling.

Annex III – High Risk Interface/Delivery Channels

In establishing a Customer relationship, the business partner is to be taken into consideration:

- Affiliates who brought high risk clients in the past
- Unlicensed affiliates
- Not effective and out of date partner tool and system.