

Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) Policy (Curacao)

Document information			
Document name:	Zoomba B.V. - AML & ATF Policy (Curacao)		
Document version:	1.2	Date of approval:	09.01.2024
Approved by:	Head of Compliance	Revision interval:	At least annually
Document owner:	CEO	Information classification:	Internal
Market	South America		
Revision history			
Author:	Version:	Date:	Change history:

Head of Compliance	1.0	01.09.2024	Initial release
Head of Compliance	1.1	01.09.2024	Approved version
Head of Compliance	1.1	01.09.2025 01.09.2026 01.09.2027	Annual review
Head of Compliance	1.2	01.09.2024	Proposed changes before 01.09 AML update

1. General	4
1.1. Introduction	4
1.2. List of relevant documentation	6
1.3. Definition	6
1.3.1. Money Laundering	7
1.3.2. Terrorist Financing	8
1.3.3. Financing of Proliferation of Weapons	9
1.3.4. Similarities and Differences of ML & TF	9
1.3.4.1. Similarities	9
1.3.4.2. Differences	9
2. Legislation and Guidelines	10
2.1. Relevant Legislation	10
2.2. Guidelines	10
3. Responsibilities	12

3.1. Senior Management	12
3.2. Verification Department	12
3.3. Compliance Officer	13
3.4. Company's Employee's Responsibilities	13
4. Customer acceptance	14
4.1. Player Identification - Know Your Client ("KYC")	14
4.2. Politically Exposed Person ("PEP")	15
4.3. Sanctions Screening	15
5. Customer relationship	16
5.1. Structure of the customer relationship	16
5.2. Identification & verification	17
5.2.1. Player risk assessment	17
5.2.2. Simplified Due Diligence	17
5.2.3. Enhanced Due Diligence	18
5.3. Ongoing Monitoring	19
5.4. Termination of a business relationship	20
6. Risk-Based Approach	21
6.1. Objectives	21
7. Regulatory Reporting	22
8. Protection of employees and whistleblowing	22
9. Training	22
10. Record keeping	23

1. General

1.1. Introduction

Zoomba B.V. (“Company”), is a remote gambling operator offering casino and sportsbook services and have sublicense granted on May 1st, 2024 by Cyberluck Curaçao N.V. pursuant to Master Gaming License #1667/JAZ. As The Curacao Gaming Control Board (“GCB”) introduced new licensing regime, Zoomba B.V. filed its application on March 24th, 2024 with reference number OGL/2024/1197/0563 to be granted a new type of license.

The Company is obliged to respect rules indicated in Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction.

The gaming industry operating in and from Curaçao is held to compliance with the National Ordinance on identification when rendering services (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92), and the National Ordinance on the reporting of unusual transactions (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99).

With the publication of the National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector, LB van 28 januari 2019, no. 19/0282) and the National Decree supervisor unusual transactions gaming sector (Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector, LB van 28 januari 2019, no. 19/0283), the Curaçao Gaming Control Board (GCB) is tasked with the AML/CFT supervision of the gaming sector operating in and from Curaçao.

Curacao's financial intelligence unit is Financial Intelligence Unit Curacao ("FIU Curacao").

The objectives of this policy are, amongst others:

- ensuring Company's compliance with all applicable laws, statutory instruments of regulation, and requirements of the relevant supervisory body;
- protecting the Company and all its staff as individuals from risks associated with breaches of laws, regulations and supervisory requirements;
- preserving the good name of Company against the risk of reputational damage presented by implication of money laundering and terrorist financing activities;
- making a positive contribution to the fight against crime and terrorism.

To achieve these objectives, **it is our policy to ensure** that:

- every staff member shall meet their personal obligations as appropriate to their role and position within the Company;
- commercial considerations shall never be permitted to take precedence over the Company's AML & ATF commitments;

Any failure to follow this Policy (and its associated Compliance Procedures) could severely harm Zoomba B.V., its reputation, financial standing and possibly breach the terms of the licenses and registrations necessary to operate our businesses. Such a failure may result in disciplinary action or termination for any employee found to have breached this Policy and may constitute a criminal offence. It should also be remembered that our compliance obligations include all our Policies and Procedures as well as those requirements that arise from the numerous contractual relationships with card schemes, banks and other payment related partners that we have entered into business relationship with.

1.2. List of relevant documentation

The whole Company AML program consist of this Policy and AML relevant documentation such as:

- Know Your Client Procedure
- Player Account and Fund Management Policy
- Account Closure, Reopen and Suspension Procedure
- Internal Reporting Policy
- External Reporting Policy
- Player Risk Management Policy

1.3. Definition

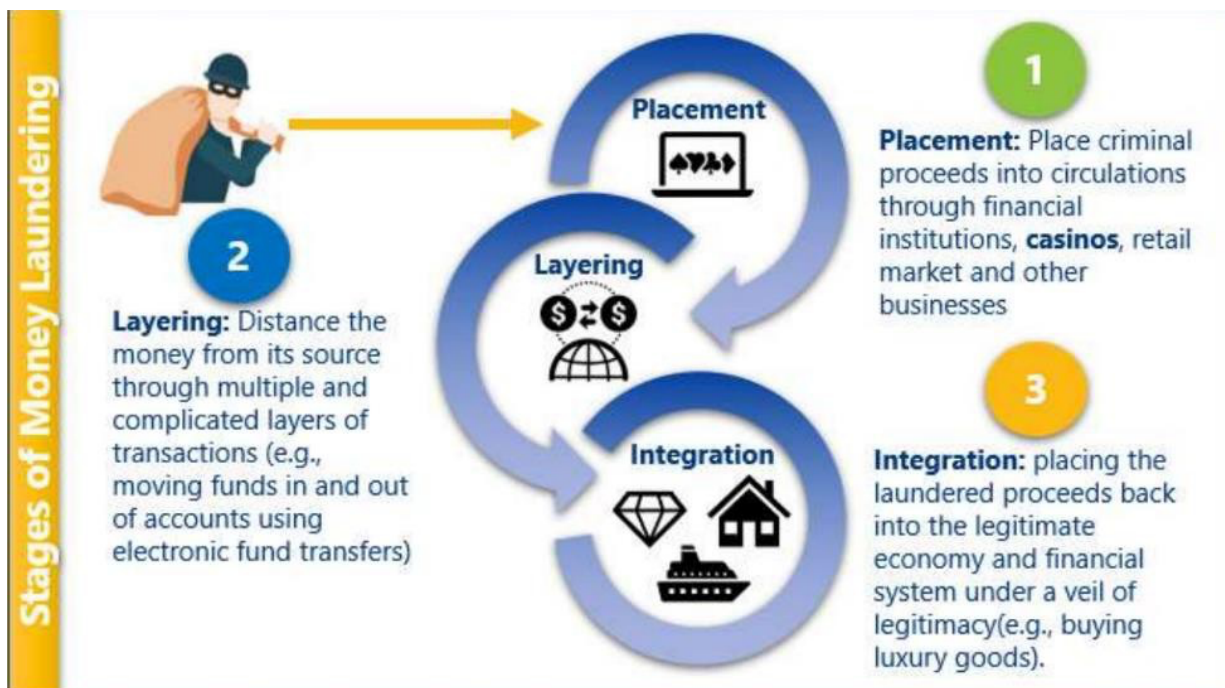
We believe that prior to implementing the AML&ATF Policy, it is essential for it to identify what is, on the one hand, money laundering, and what, on the other hand, constitutes financing of terrorism.

1.3.1. Money Laundering

Money laundering is the process used to disguise the source of money or assets derived from criminal activity. Essentially, money laundering is the process whereby “dirty money” – produced through criminal activity – is transformed into “clean money”, the criminal origin of which is difficult to trace. Profit-motivated crimes span a variety of illegal activities from drug/weapon/human trafficking and smuggling to fraud, extortion and corruption.

Money laundering facilitates corruption and can destabilize the economies of susceptible countries. It also compromises the integrity of legitimate financial systems and institutions and gives organized crime the funds it needs to conduct further criminal activities. It is a global problem, and there are numerous different techniques that can be very sophisticated. Technological advances provide further opportunities to launder illegal profit and obscure the money trail leading back to the underlying crime.

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



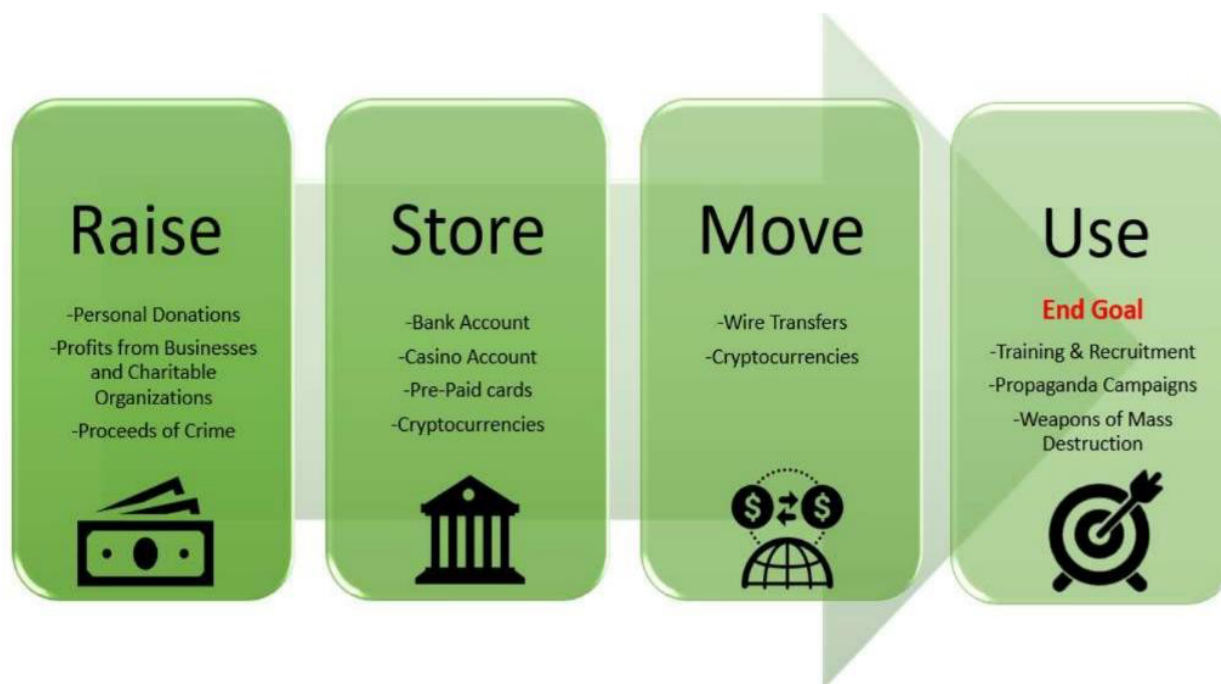
1.3.2. Terrorist Financing

Terrorist financing provides funds for terrorist activity which has as its main objective to intimidate a population or compel a government to do something. This is done by seriously interfering with or causing damage to essential services, facilities, or systems, or by endangering, harming or killing people.

Terrorist financing may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. However, financial transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering, and when terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult. To move their funds, terrorists use the formal banking system, informal value-transfer systems, Hawalas and Hundis and, the oldest method of asset-transfer, the physical transportation of cash, gold and other valuables through smuggling routes.

The funding flow usually follows a linear pattern: collection of funds, storage of funds, movement of funds, usage of funds.



1.3.3. Financing of Proliferation of Weapons

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

1.3.4. Similarities and Differences of ML & TF

1.3.4.1. Similarities

Money laundering and terrorist financing offences can be committed in connection with each other. For example, the funds for terrorist activity can be 'laundered' funds.

1.3.4.2. Differences

While they may share similar typologies, the difference lies in the timing and direction of the flow of funds and transactions.

Criteria	Money Laundering	Terrorist Financing
Motivation	Profit making	Ideological purposes
Intention	Disguise the origin of the resources	Intimidate through violence
Source of Financing	Illegal Resources Extortion Kidnapping Drug-trafficking Smuggling Fraud Theft	Illegal Resources Extortion Kidnapping Drug-trafficking Smuggling Fraud Theft Legal Resources Donations Government sponsorship Controlled companies
Methods	Placement Layering Integration	Placement Layering Integration
Life Cycle	Circular	Linear

2. Legislation and Guidelines

2.1. Relevant Legislation

The Regulations for Combating Money Laundering, the Financing of Terrorism and Proliferation of weapons of Mass Destruction are an integral part of the land-based and the online gambling license requirements for the Curaçao jurisdiction. These Regulations are issued in implementation of:

- article 2 paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 no. 92);
- article 22mm, paragraph 3, of the National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2017 no.99);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54).

2.2. Guidelines

With above Regulations the GCB offers the casinos a guideline to promote compliance with the laws and decrees with regard to money laundering, financing of terrorism and financing of proliferation and to implement sound internal policies and procedures to combat Money Laundering and the Financing of Terrorism. These include among others:

- 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); 4
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

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 Curaçao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons.

3. Responsibilities

3.1. Senior Management

For the AML & ATF purposes the Senior Management in the Company are Company Directors.

Senior Management is fully engaged in the process around the Company's assessment of risks for money laundering and terrorist financing and is involved in the process of decision making, to develop the appropriate policies and processes to comply with relevant legislation.

Senior Management fully supports the Compliance Team and ensures appropriate standards are implemented within their field of interest, for example by clear communication of applicable procedures to their staff members. Further, they will ensure robust mechanisms are in place to make sure that all policies and procedures are carried out effectively, weaknesses are identified, and improvements are made where necessary.

3.2. Verification Department

The Verification Department is responsible for conducting customer due diligence checks (standard and enhanced) and applying any required measures in line with the implemented approach. This Department is also responsible for ongoing customer monitoring of all related transactions and applying any measures that are necessary.

The company has developed internal systems, procedures and controls suitable for the remote gaming environment and provided the team with appropriate tools and training to perform the required checks.

3.3. Compliance Officer

The Company has appointed a Compliance Officer (“CO”). The CO’s main responsibility is that of considering any internal reports of unusual or suspicious transactions that are made within the company, following up on these reports and also filing them.

The Company ensures that the individual appointed as the CO enjoys sufficient seniority and command to be able to act independently of its management. The CO shall have access to all necessary information/documentation and company employees to effectively carry out their obligations.

3.4. Company’s Employee’s Responsibilities

All staff communicating with the customers, or having access to information about clients’ affairs, receive anti-money laundering training. In this manner, they are able to identify which player’s actions should reasonably lead them to suspect money laundering or terrorism financing risk.

They are expected to recognize and understand any gaming or transaction behavior which might indicate the customer being involved in money laundering or terrorism financing.

Where they know, suspect or have reasonable grounds to know or suspect that they are dealing with the proceeds of crime, that person must submit an internal report to the CO, according to the Reporting Procedure. In this manner, the employee’s legal obligation to report will be considered to have been fulfilled. Employees are also made aware that, if

they do not make an internal report to the MLRO when necessary, they may also face criminal sanctions.

4. Customer acceptance

The Company shall only accept customers who intend to use our website according to its purpose. Individuals with different intentions or ulterior motives shall not be accepted by the Company. Every customer must register their account personally, the Company does not accept customers registering an account for 3rd parties. The Company will terminate the business relationship if there is a reason to believe that a customer's account is being used by or on behalf of another person. This includes any customers operating an account funded by an Organized Crime Group.

Anonymous accounts are prohibited.

4.1. Player Identification - Know Your Client ("KYC")

The company accepts only players who will successfully fill registration page with:

- Name
- Surname
- Gender
- Date of Birth
- Phone Number
- Permanent Address

FROM 1ST SEPTEMBER:

Data entered at the registration form shall be automatically checked by AgeChecked software against independent data to verify the player's identity. Additionally PEPs and Sanction check also shall happen at this stage. Depending on the outcome, player can be verified and allowed to deposit and play or shall be sent for further manual verification.

Every player is also asked to upload additional documentation (if needed) before first withdrawal is processed. Only identified and successfully verified player are able to withdraw their balance.

More information about the process can be found in the Know Your Client (KYC) Policy.

4.2. Politically Exposed Person (“PEP”)

A PEP is an individual who is or has been entrusted with a prominent public function, such as serving in a prescribed government office or a political position, which can make them vulnerable to corruption and potential target of criminals who could exploit their status and use them knowingly or unknowingly to carry out ML/TF activities.

At the moment of registration, the Company is gathering attestation from players whether they are a PEP. FROM 1ST OF SEPTEMBER] Additionally, an automatic system checks registration details (name screening) across several databases and further assesses trigger risk during the ongoing monitoring process. This approach allows to identify PEPs at a very early stage of the relationship and minimizes the risk of being exposed to money laundering, bribery, and usage of illegally obtained funds.

4.3. Sanctions Screening

The imposition of economic sanctions against foreign countries remains an important instrument for the international community in the enforcement of laws relating to the financing of terrorist activity, money laundering, and fraud. Sanctions can encompass a wide variety of measures, which include limitations on official and diplomatic contacts or travel, and the imposition of legal measures to restrict or prohibit trade or other economic activity.

The Company does not accept any individuals who are listed on sanction lists. **FROM 1ST SEPTEMBER** Name screening against sanctions is being done during the registration process by an automatic system. More details can be found in the Player Identification - Know Your Client (KYC) Policy.

5. Customer relationship

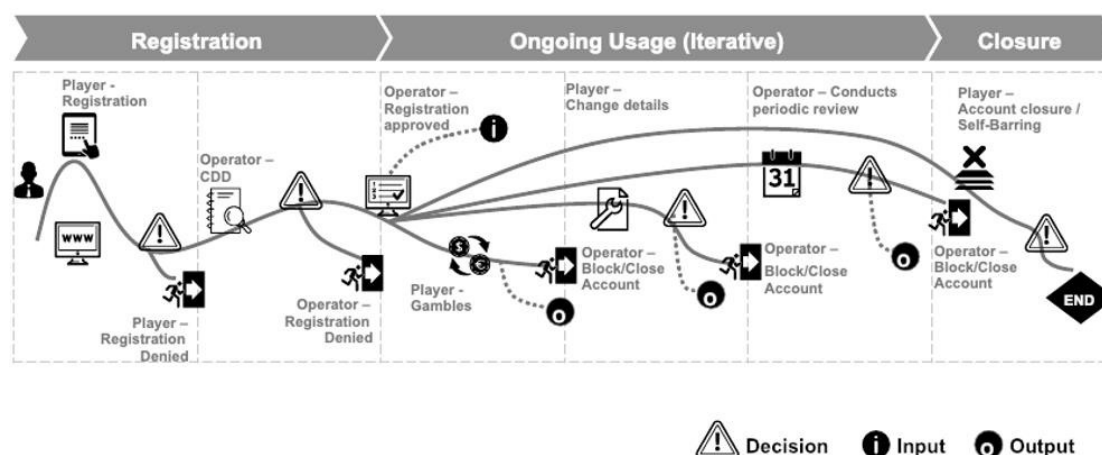
5.1. Structure of the customer relationship

In light of anti-money laundering and anti-terrorist financing policies, a customer's relationship with the Company consists of three elements:

- **registration** - the establishment of the business relationship, including customer verification and entering into a business relationship;
- **ongoing usage** - monitoring of the player's account, followed by ongoing monitoring, including account deposits and withdrawals;
- **account closure** - termination of the relationship with the customer.

By registering on our website, customers enter into a business relationship with us. At all stages of the relationship, it is necessary to consider whether the customer is engaged in money laundering (including criminal spend) or terrorist financing.

Customer Account Lifecycle:



5.2. Identification & verification

Identifying a customer means obtaining information about their identity:

- full legal name;
- full physical address;
- date of birth;
- personal telephone number;
- email address;
- identity number;

To open an account with the Company, the Player must first complete the registration process. Customers must be over allowed legal age to be permitted to register on the Website - no underage users are allowed to use the Company's services.

Verifying the identity means obtaining evidence that supports the outcome of the identifying process. Company's verification method consists of an electronic method of verification and manual verification.

5.2.1. Player risk assessment

Customer risk assessment starts at the beginning of the relationship. The Company recognizes the extent to which a particular customer triggers the risk factors and assesses the risk of the customer accordingly. More information can be found in the Player Risk Assessment Policy.

5.2.2. Simplified Due Diligence

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

- Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the casino to obtain the player's identity.
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low risk situation, the 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.);
- The extent of personal details verified can also vary. In low risk situations, the casino has to verify the basic identification details, while the verification of any other personal details is upon the casino, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

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

5.2.3. Enhanced Due Diligence

A risk-based approach should be taken, so more thorough checks should be undertaken for higher risk customers. The Enhanced Due Diligence (EDD) measures should be consistent with the risks identified. They should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. Enhanced Due Diligence must be conducted where the risks of money laundering or terrorist financing are higher. This concerns for example:

- Residents of higher risk geographic areas;
- Political Exposed Persons (PEP's);

- Products or transactions that might favor 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.

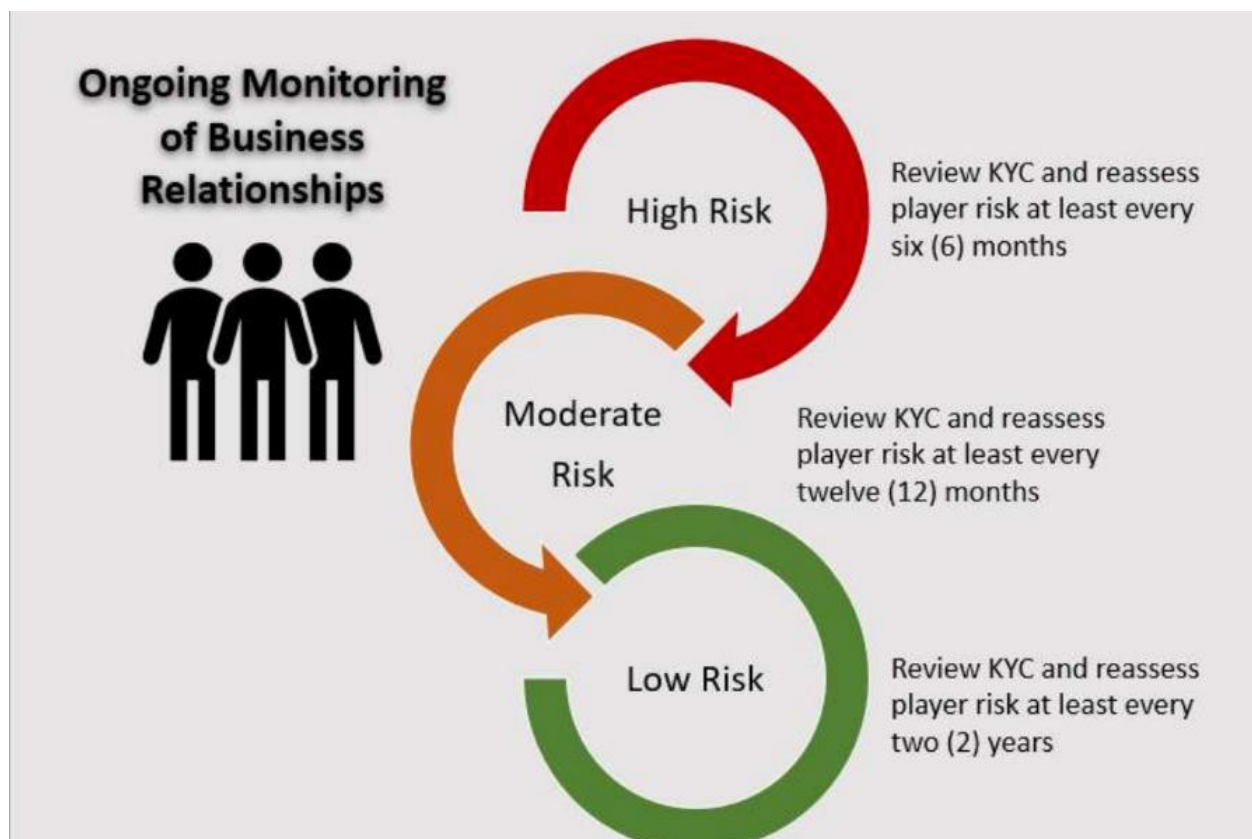
The applied measures must be consistent with the risks identified. They should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced due diligence measures include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player. Examples of 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 must be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

5.3. Ongoing Monitoring

Monitoring of Players is carried out using the risk-based approach. Players are monitored on an ongoing basis and assessed on a risk-sensitive basis, with extreme and high-risk Players being subjected to an enhanced ongoing monitoring conducted with appropriate frequency and depth of scrutiny:



On a day-to-day basis, Players are checked throughout the course of the relationship to ensure that transactions are consistent with the knowledge and risk profile Company holds on to the Player.

In addition, the MLRO and deputy MLRO review the existing records of Players to ensure procedures and policies are carried out correctly. Transaction monitoring rules are being reviewed at least annually.

5.4. Termination of a business relationship

Circumstances when the Company may need to terminate a business relationship with a customer include:

- it is known that the customer attempted to use the relationship to launder criminal proceeds or use it for criminal spend;
- it is not possible to complete CDD or EDD checks in regard to the customer;
- if the risk score is recognized as extreme or high;
- their activity raises to an increased level of suspicion or knowledge of money laundering/terrorist financing;
- there are reasonable grounds to believe that the customer is not the identity they claim to be.

More information about the account termination can be found in the Player Risk Assessment Policy and External Reporting Policy.

6. Risk-Based Approach

6.1. Objectives

The Company has adopted a player risk-based approach towards AML & ATF. More information can be found in the Player Risk Assessment Policy.

Objectives of the Player risk assessment are:

- to assess a Player's ML/TF risk;
- to determine the level of due diligence required that would be appropriate with the Player's identified level of risk;
- to determine the frequency for ongoing monitoring and Player information update;

7. Regulatory Reporting

The company shall fulfil all regulatory reporting requirements - including internal and external reporting. More information can be found in the Internal and External Reporting Policies.

8. Protection of employees and whistleblowing

Zoomba B.V. has established routines to protect persons who fulfil Deck's obligations under the AML/ATF regulations.

Moreover, any individual (including employees, consultants, and Zoomba B.V. officials) who reports suspicions of ML/TF, internally or to the FIU Curacao, is protected under the regulations from threats or hostile action, and from adverse or discriminatory employment actions. Further information can be found in the Whistleblowing Policy.

9. Training

Ongoing AML/ATF training plays a critical role in combating and preventing ML and TF risks. One of the most important controls over the detection and prevention of ML/TF activities is to have employees who are knowledgeable in ML/TF risks and who are well trained in the identification of unusual activities or transactions which appear to be suspicious.

Company employees are required to complete the training module at the time of their onboarding (prior to any Player interaction or fulfilment of any AML related activities) and on an annual basis thereafter (i.e., refresher training).

AML/ATF training must be delivered to the following employees (at a minimum) who are responsible for onboarding and due diligence (including high-risk Player monitoring)

- Monitoring Player transactions
- Addressing Player queries or concerns (such as a customer service team)
- Technology functions related to AML activities

Training trail:



10. Record keeping

It is essential that proper records are kept of the due diligence carried out on the customer, evidence gathered, the decisions that were made and the reasons behind them.

All AML records shall be retained for five years. A record (or a copy) may be kept in a machine-readable or electronic form, so long as a paper copy can be easily produced.