



AML / CFT / CFP POLICY

Contents

1. Introduction.....	4
1.1. Applicable Legislation.....	4
1.2. Financial Action Task Force.....	5
1.3. European Union.....	5
2. Definitions of Money Laundering, Terrorism Financing and Proliferation Financing.....	7
2.1. Definition of Money Laundering	7
2.2. Stages of Money laundering.....	7
2.2.1. Placement	7
2.2.2. Layering.....	8
2.2.3. Integration.....	8
2.3. Money Laundering Methods	9
2.4. Definition of Financing of Terrorism.....	10
2.4.1. Non-Profit Organisations.....	11
2.5. Definition of Financing of Proliferation of Weapons.....	11
2.6. Targeted Financial Sanctions	11
3. Risk-Based Approach	13

3.1.	Procedures for preventing money laundering, terrorist financing and proliferation financing	13
3.2.	What is the risk-based approach?	13
3.3.	Identification, recording and evaluation of risks	14
3.4.	Customer risk assessment (CRA)	15
3.4.1.	Low risk customers.....	15
3.4.2.	Normal risk customers	15
3.4.3.	High risk customers	15
3.5.	Design and implementation of measures and procedures to manage and mitigate the risks.....	16
3.6.	Monitoring and Improving the Measures and Procedures	16
4.	Application of Customer Due Diligence (CDD)	18
4.1.	When to undertake CDD	18
4.2.	Ways of application of customer due diligence and identification procedures	18
4.3.	Customer Identification Procedures.....	19
4.4.	Normal risk customers.....	19
4.5.	Enhanced Due Diligence Procedures.....	20
4.5.1.	Accounts in the names of companies whose shares are in bearer form	21
4.5.2.	Trusts accounts.....	21
4.5.3.	Client accounts in the name of a third person.....	22
4.5.4.	Politically exposed persons (PEPs) accounts.....	22
4.5.5.	Customers from countries which inadequately apply Financial Action Task Force's recommendations..	23
4.6.	Failure or refusal to submit information for the verification of customers' identity	24
4.7.	Customer data recording.....	24
5.	Ongoing Monitoring of Accounts and Transactions	26
5.1.	Ongoing customer profile monitoring.....	26
5.2.	Ongoing transaction monitoring	27
6.	Reporting of Unusual Transactions.....	28
6.1.	Recognition of unusual transactions	28
6.2.	Reporting procedures.....	29
6.3.	Submission of information to FIU.....	29
6.4.	Cooperation with FIU after reporting unusual transactions/activities.....	30
6.5.	Failure to report.....	30
6.6.	Prohibition of disclosure.....	30
7.	Record Keeping.....	32
7.1.	Record keeping of documents/data	32

7.2.	Time period of keeping documents/data	32
7.3.	Format of records	32
7.4.	Certification and language of documents	32
8.	AML Compliance Program	33
8.1.	Board of Directors Responsibilities.....	33
8.2.	Compliance Officer	33
8.3.	Employees' Obligations and Training.....	34
8.3.1.	Employee Due Diligence	34
8.3.2.	Employee Obligations	35
8.3.3.	Employee Education and Training Program	35
8.4.	Independent Audit	35
APPENDIX 1: Development and Establishment of Customer Acceptance Policy (CAP) on a Risk-Based Approach		37
APPENDIX 2: Internal Unusual Report for Money Laundering and Terrorist Financing.....		43
APPENDIX 3: Internal Evaluation Report for Money Laundering and Terrorist Financing		45
APPENDIX 4: Compliance Officer's Report to the Unit for Combating Money Laundering (FIU)		46

Version History

VERSION	CHANGES	BY	DATE
1.0			XX April 2024
2.0			XX November 2024

1. Introduction

The Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (“AML/CTF/CPF”) Policy is created for JMS Investment Group N.V. (hereinafter the “Company”), a company licensed in Curaçao, along with its subsidiaries (collectively referred to as the “Group”). The Group is committed to implementing all AML procedures outlined in this manual. The primary activities of the Group include investment holding and online betting operations. The subsidiaries involved in betting are duly regulated. This Policy details the AML system specific to the Group, with a focus on the companies providing betting services.

There is a hierarchy of regulation where money laundering is concerned. This includes international legislation, such as the United Nations resolutions, EU Money Laundering Directives and international policy initiatives, such as the recommendations published by the Financial Action Task Force (FATF). These are distilled into national frameworks, which can be a combination of regulatory requirements, such as gambling license conditions and broader laws, which may apply to a range of commercial activities.

These guidelines are intended to highlight the importance of operators following these national requirements, having regard to the wider international context. Some operators may need to comply with the national requirements of a number of countries, in which case it is usually sensible to the operator to work to the highest applicable standard across the group. The guidance is also intended to suggest practical ways to conduct AML, CFT & CFP.

As a responsible gaming enterprise operating in Curaçao, we acknowledge the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

1.1. Applicable Legislation

The local authorities in charge of the supervision of AML/CFT/CFP matters for the gaming sector are the Curaçao Gaming Control Board (GCB) and the Curaçao Financial Intelligence Unit (FIU). The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- 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);
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282)
- National Decree supervisor unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283)

- 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 Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- 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 Decree prohibition of import, export, and transit of Venezuelan Gold (N.G. 2019, no. 82).
- National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no.74) as amended by (N.G. 2014, no. 90).
- GCB's Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update May 2024.

The Company's operations are guided by collaboration with international regulatory bodies, strengthening our compliance with global standards.

1.2. Financial Action Task Force

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF is therefore a "policy-making body" created in 1989 that works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. The FATF has published 40+9 Recommendations in order to meet this objective. The FATF monitors members' progress in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally. In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism.

1.3. European Union

- Directive 91/308/EEC of 10 June 1991 on the Prevention of the use of the financial system for the purpose of Money Laundering (the 1st Directive).
- Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 on the prevention of the use of the financial system for the purpose of money laundering (the 2nd Directive).

- Directive 2005/60/EC of the European Parliament and of the Council 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the 3rd EU Directive, also known as the “3MLD”).
- Directive 2015/849 / of the European Parliament and of the Council 25 June 2015 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the 4th EU Directive, also known as the “4MLD”).
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the 5th EU Directive, also known as the “5MLD”).

2. Definitions of Money Laundering, Terrorism Financing and Proliferation Financing

2.1. Definition of Money Laundering

Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it allows them to maintain control over those proceeds and, ultimately, to provide legitimate cover for their source of income. Failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions, thus making crime a more attractive proposition.

Certain vulnerabilities exist within the money laundering process that can expose launderers to detection. Key points of risk include the entry of cash into the financial system, cross-border cash flows, and transfers within or from the financial system. These areas present opportunities for financial institutions to identify irregular activity and potential criminal behavior.

2.2. Stages of Money laundering

The money laundering process does not adhere to a single, uniform method. Instead, it generally unfolds in three key stages. These stages can occur independently, simultaneously, or overlap depending on the techniques employed by the criminals involved:

- a) Placement
- b) Layering
- c) Integration.

2.2.1. Placement

Placement is the initial stage, where cash obtained from illegal activities is introduced into the financial system. Criminals are most exposed when they physically possess cash that links them to their illegal acts. To mitigate this risk, they seek to deposit this cash into banks or other financial institutions. Given that money laundering is heavily reliant on cash, this stage often involves substantial amounts generated from illegal operations, such as drug trafficking. The goal here is to distance the cash from its original source and convert it into different asset forms, like traveler's checks or postal orders.

Some placement methods are:

Disguised deposits: Launderers often divide large amounts of cash into multiple small transactions amounts, for example of less than €10,000 by, for instance:

- Making several deposits into a single or multiple accounts on successive days
- Making deposits into a number of accounts (often opened by using false identities) at different branches of the same bank.
- Using different banks and then consolidating the accounts
- Depositing cash into accounts of third parties such as lawyers, real estate agents, brokers and security firms.

- Depositing cash with the assistance of corrupt bank staff who themselves manipulate the deposits to make them appear as if they are below the reporting threshold.

Use of monetary instruments: Launderers purchase monetary instruments, such as money orders, postal orders and travelers' cheques. In this way they convert cash into financial instruments for relatively small amounts, which are easily transportable, and then deposit them elsewhere.

Inter-mingling: Money launderers often attempt to conceal the origin of criminally derived cash by mixing it with legitimately generated cash. They do so by using the services of lawful business enterprises. A cheaper but riskier alternative is to establish what is known as a "front company". This is a company that is incorporated on paper, but that does not own any physical assets and does not trade. The launderer opens an account in the name of the front company and deposits criminally derived cash into it, representing the money as the profits of the front company.

Assets purchases: Launderers may also use the cash proceeds of their criminal activities to buy assets like real estate, gold and precious metals, art, motor cars and antiques. These items may then be sold and converted back into cash.

2.2.2. Layering

Layering follows placement and involves separating the illicit funds from their origins through a series of complex financial transactions. Once the money is in the financial system, launderers can engage in numerous transactions designed to obscure the audit trail and provide anonymity. This stage often aims to confuse investigations by placing significant distance between the original source of the funds and their current form. Common techniques include transferring money through offshore accounts or executing numerous small transactions that make tracing difficult.

A number of different types of transactions may be used at this stage of the laundering process, known as layering, aiming to disguise the proceeds of crime. The main methods of layering are:

Electronic (wire) transfers: Dirty money, once placed in the system, is often transferred by electronic fund transfer (wire transfers) between accounts or between banks, whether domestic or offshore. Launderers might accumulate a number of small deposits in an account(s) and use a domestic electronic fund transfer to consolidate these accounts, followed by an international electronic fund transfer to move the monies offshore. This type of electronic money transfer can be carried out quickly and over vast distances, involving a number of offshore jurisdictions. Funds moved in this fashion, often in purported payment for goods sold or services rendered (that do not in reality exist), on a number of occasions, ultimately become practically untraceable.

Monetary instruments: Once placed in the banking system, dirty money can be used to buy cashier cheques, drafts, travelers' cheques, letters of credit etc. These instruments may then be transported and transferred, either domestically or, more usually, offshore. Funds are first placed in the financial system onshore and are then moved offshore where the layering takes place. Once offshore the funds are often transferred between accounts held by front companies incorporated in offshore centers, where confidentiality provisions allow corporate service providers to act as nominees and/or for bearer shares to be issued in order to maintain anonymity in the outside world.

2.2.3. Integration

Finally, integration is the stage where laundered money is reintroduced into the legitimate economy, appearing to originate from a legal source. This process often involves making the funds look as though they were earned

legitimately. By this point, distinguishing between legal and illegal wealth becomes exceedingly difficult. Methods used at this stage can include establishing anonymous companies to facilitate loans, sending false invoices, or utilizing insurance policies to convert illicit funds into seemingly legitimate returns.

Some commonly used methods to integrate laundered funds into the financial system are:

Loan arrangements: The establishment of anonymous companies in countries where the right to secrecy is guaranteed. They are then able to grant themselves loans out of the laundered money in the course of a future legal transaction. Furthermore, to increase their profits, they will also claim tax relief on the loan repayments and charge themselves interest on the loan.

Sham transactions: The sending of false export-import invoices overvaluing goods allows the launderer to move money from one company and country to another with the invoices serving to verify the origin of the monies placed with financial institutions.

Inheritance: Funds held in one jurisdiction on behalf of the launderer may be transferred to another jurisdiction and be purported to represent a gift or inheritance

Redemption of life policy or similar investment: This method involves the launderer in placing funds with an insurance company and sometime later encashing the property (or borrowing against it) so that a cheque from the insurance company has the appearance of emanating from a legitimate source.

2.3. Money Laundering Methods

The Money Laundering methods are numerous. The most common are the following:

- **Structuring ("smurfing"):** Smurfing is possibly the most commonly used money laundering method. It involves many individuals who deposit cash into bank accounts or buy backdrafts in amounts under €10,000 to avoid the reporting threshold.
- **Money Services and Currency Exchanges:** Money services and currency exchanges provide a service that enables individuals to exchange foreign currency that can then be transported out of the country. Money can also be wired to accounts in other countries. Other services offered by these businesses include the sale of money orders, cashiers' cheques, and travelers cheques.
- **Asset Purchases with Bulk Cash:** Money launderers may purchase high value items such as cars, boats or luxury items such as jewellery and electronics. Money launderers will use these items but will distance themselves by having them registered or purchased in an associate's name.
- **Electronic Funds Transfer:** Also referred to as a telegraphic transfer or wire transfer, this money laundering method consists of sending funds electronically from one city or country to another to avoid the need to physically transport the currency.
- **Postal Money Orders:** The purchase of money orders for cash allows money launderers to send these financial instruments out of the country for deposit into a foreign or offshore account.
- **Credit Cards:** Overpaying credit cards and keeping a high credit balance gives money launderers access to these funds to purchase high value items or to convert the credit balance into cheques.
- **Casinos:** Cash may be taken to a casino to purchase chips which can then be redeemed for a casino cheque.

- **Refining:** This money laundering method involves the exchange of small denomination bills for larger ones and can be carried out by an individual who converts the bills at a number of different banks in order not to raise suspicion. This serves to decrease the bulk of large quantities of cash.
- **Legitimate Business / Co-mingling of Funds:** Criminal groups or individuals may take over or invest in businesses that customarily handle a high cash transaction volume in order to mix the illicit proceeds with those of the legitimate business. Criminals may also purchase businesses that commonly receive cash payments, including restaurants, bars, night clubs, hotels, currency exchange shops, and vending machine companies. They will then insert criminal funds as false revenue mixed with income that would not otherwise be sufficient to sustain a legitimate business.
- **Value Tampering:** Money launderers may look for property owners who agree to sell their property, on paper, at a price below its actual value and then accept the difference of the purchase price "under the table". In this way, the launderer can, for example, purchase a \$2 million dollar property for \$1 million, while secretly passing the balance to the seller. After holding the property for a period of time, the launderer then sells it for its true value of \$2 million.
- **Loan Back:** Using this method, a criminal provides an associate with a sum of illegitimate money and the associate creates the paperwork for a loan or mortgage back to the criminal for the same amount, including all of the necessary documentation. This creates an illusion that the criminal's funds are legitimate. The scheme's legitimacy is further reinforced through regularly scheduled loan payments made by the criminal and providing another means to transfer money.

2.4. Definition of Financing of Terrorism

Terrorism Financing (TF) pertains to the allocation of funds or financial assistance aimed at supporting terrorist activities, individuals, or organizations. It is defined by the objective of instilling fear in populations or compelling governments and international entities to take specific actions or refrain from doing so. In contrast to money laundering, which invariably involves proceeds from unlawful activities, terrorist financing may not always originate from illegal sources. Rather, it frequently utilizes legitimate funds sourced from charitable contributions, business earnings, or sponsorship from foreign governments.

While both terrorism financing and money laundering may utilize analogous techniques—such as cash smuggling, structuring, wire transfers, and the employment of debit and credit cards, the primary focus of TF is to conceal the intended application or final recipient of the funds, rather than their origin. Moreover, financing for terrorist operations does not necessarily necessitate substantial sums of money, as it can accumulate incrementally through relatively minor transactions.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include:

- cash smuggling by couriers or bulk cash shipments;
- structured deposits to or withdrawals from bank accounts;
- wire transfers by using “straw men”;
- false identities;
- front and shell companies.

The gaming industry, particularly online platforms, is notably susceptible to exploitation by terrorist organizations seeking to launder money or transfer funds in a covert manner, owing to its intrinsic anonymity and substantial transaction volumes. Ultimately, the overarching objective of terrorism financing is to enable the planning, preparation, and execution of acts that jeopardize both national and international security.

2.4.1. Non-Profit Organisations

Non-profit and charitable organisations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organisations can be made in the following ways:

- Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.
- A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
- The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.
- The non-profit organisation provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organisations indicating that they may be used for an unlawful purpose are the following:

- Inconsistencies between the apparent sources and amount of funds raised or moved.
- A mismatch between the type and size of financial transactions and the stated purpose and activity of the nonprofit organisation.
- There was a sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.
- Large and unexplained cash transactions by non-profit organisations.
- The absence of contributions from donors located within the country of origin of the non-profit organisation.

2.5. Definition of 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.

2.6. Targeted Financial Sanctions

We are committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with these sanctions. This includes, but is not limited to, the following:

- The Company shall comply with relevant sanctions decrees and regulations and monitor for any and all amendments thereof and implement these without undue delay.
- The Company shall perform perpetual sanctions screening on customers and perform trigger-based sanctions screening of customers at least in the following scenarios:
 - At the moment of registration;
 - At the moment of withdrawal request;
 - At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered, the Company shall immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and shall immediately file a report with the FIU. Once the true match is confirmed by the supervisory authority, the Company shall terminate services and keep the frozen assets until further instruction from the supervisory authority.

3. Risk-Based Approach

3.1. Procedures for preventing money laundering, terrorist financing and proliferation financing

The Law requires all persons carrying on gambling (or other business) activities, to establish and maintain specific policies and procedures to guard against their business and the financial system in general being used for the purposes of ML, TF and PF. In essence these procedures are designed to achieve two purposes: firstly, to facilitate the recognition and reporting of unusual transactions and, secondly, to ensure through the strict implementation of the "know-your-customer" (KYC) principle, and the maintenance of adequate record keeping procedures, should a customer come under investigation, that the Company is able to provide its part of the audit trail.

The Company applies adequate and appropriate systems and procedures in relation to the following:

- a) Customer identification and customer due diligence
- b) Record-keeping
- c) Internal reporting and reporting to FIU
- d) Internal control, risk assessment and risk management in order to prevent money laundering and terrorist financing
- e) Detailed examination of each transaction which by its nature may be considered to be particularly vulnerable to be associated with money laundering offences or terrorist financing and in particular complex or unusually large transactions and all other unusual patterns of transactions which have no apparent economic or visible lawful purpose.
- f) Informing their employees in relation to:
 - i. The above systems and procedures
 - ii. the present Law
 - iii. the Directives issued by the competent Supervisory Authority
 - iv. the European Union's Directives on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing
- g) ongoing training of their employees in the recognition and handling of transactions and activities which may be related to money laundering or terrorist financing

3.2. What is the risk-based approach?

The Company applies appropriate measures and procedures, on a risk-based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher. A risk-based approach:

- a) recognises that the money laundering or terrorist financing threat varies across customers, countries, services and financial instruments;
- b) allows the Board of Directors to differentiate between customers of the Company in a way that matches the risk of their particular business;

- c) allows the Board of Directors to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;
- d) helps to produce a more cost-effective system; and
- e) promotes the prioritisation of effort and actions of the Company in response to the likelihood of money laundering or terrorist financing occurring through the use of services provided by it.

A risk-based approach involves specific measures and procedures in assessing the most cost effective and proportionate way to manage the money laundering and terrorist financing risks faced by the Company. Such measures and procedures are:

- f) identifying and assessing the money laundering and terrorist financing risks emanating from particular customers, financial instruments, services, and geographical areas of operation of the Company and its customers;
- g) documenting in the risk management and procedures manual the policies, measures, procedures and controls to ensure their uniform application across the Company by persons specifically appointed for that purpose by the Board of Directors;
- h) managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- i) continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

3.3. Identification, recording and evaluation of risks

The basis for the application of the risk-based approach is the business risk assessment (BRA). The Compliance Officer has the responsibility to identify, record and evaluate all potential risks in the BRA. The successful establishment of measures and procedures on a risk-based approach requires clear communication of the measures and procedures that have been decided across the Company, along with robust mechanisms to ensure that these are implemented effectively, weaknesses are promptly identified, and improvements are made wherever necessary.

The Company conducts comprehensive BRAs and evaluates potential risk factors related to customers, products, services, geographic locations, and delivery channels. The particular circumstances of the Company determine the suitable procedures and measures that need to be applied to counter and manage risk.

The identification, recording and evaluation of risk that the Company faces presuppose the finding of answers to the following questions:

- a) What risk is posed by the Company customers? For example:
 - companies with bearer shares;
 - companies incorporated in offshore centres;
 - politically exposed persons;
 - customers engaged in transactions which involve significant amounts of cash;

- customers from high-risk countries or from countries known for high level of corruption or organized crime or drug trafficking vi. complexity of ownership structure of legal persons.

b) What risk is posed by a customer's behaviour? For example:

- customer transactions where there is no apparent legal financial/commercial rationale;
- situations where the origin of wealth and/or source of funds cannot be easily verified;
- unwillingness of customers to provide information on the beneficial owners of a legal person.

The application of appropriate measures and the nature and extent of the procedures of a risk-based approach depends on different parameters. Indicative parameters are the following:

- the scale and complexity of the services;
- geographical spread of the services and customers;
- the nature (e.g. non face to face customer) and economic profile of customers as well as of services offered;
- the distribution channels and practices of providing services;
- the volume and size of transactions;
- the degree of risk associated with each area of services;
- the country of origin and destination of customers' funds;
- deviations from the anticipated level of transactions;
- the nature of business transactions.

BRAs are conducted regularly to ensure that the Company's risk profile stays current and accurate, with a comprehensive assessment performed annually. Additional assessments may be prompted by significant events, such as the launch of new products, changes in regulations, or substantial shifts in the business landscape.

3.4. Customer risk assessment (CRA)

The Customer Risk Assessment will assess the particular risks the casino will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile. On the basis of the CRA, the proper level of CDD can then be applied.

The Compliance Officer prepares and maintains a list for the categories (normal or high risk) of customers, which contain, among others, the customers' names, account numbers, and date of commencement of business relationship. These lists are promptly updated with all new or existing customers that the Company has determined, in the light of additional information received.

3.4.1. Low risk customers

The Company's policy is not to classify any Client as Low Risk Client.

3.4.2. Normal risk customers

All customers which do not fall in the high-risk categories are considered as Normal Risk Clients

3.4.3. High risk customers

The category of High-Risk Clients includes the following customers:

- Accounts in the names of companies whose shares are in bearer form;
- Trusts accounts;
- Client accounts in the name of a third person;
- Politically exposed persons' accounts;
- Customers from countries which inadequately apply Financial Action Task Force's recommendations;
- correspondent banking relationships with credit institutions-customers from third countries;
- Companies incorporated in offshore centers;
- any other customer determined by the Company itself to be classified as such.

3.5. Design and implementation of measures and procedures to manage and mitigate the risks

The Compliance Officer is responsible for designing and implementing the appropriate measures for the correct risk management and risk mitigation, especially of high-risk clients, which include but are not limited to:

- the verification of the customers identity;
- the collection of information for the construction of their economic profile;
- monitoring their transactions and activities;
- increase awareness of higher risk situations within business lines;
- increase levels of "Know Your Customer" rules or "Enhanced Due Diligence" at account opening;
- increase monitoring of transactions;
- increase levels of ongoing controls and reviews of relationships;
- seek additional verification information beyond the minimum requirements to substantiate client's identity (request an additional reference letter, make additional web search or apply for the verification to the relevant authorities);
- obtain additional information about intended nature of relationship and estimate of the amount/type of business;
- obtain additional documented information regarding clients' source of funds and wealth;
- independently verified information;
- implement senior management approval of all relationships identified as high risk;
- implement senior management review process to exit from existing high-risk relationships if risk level exceeds the entity's risk tolerance;
- analyse money laundering and terrorist financing risk vulnerabilities for new acquisition processes and product or service development processes;
- Update third party information on a more frequent basis.

3.6. Monitoring and Improving the Measures and Procedures

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Customers' activities change as well as the services and provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

The measures, procedures and controls are kept under regular review by the Compliance Officer so that risks resulting from changes in the characteristics of existing customers, new customers, services and financial instruments are managed and countered effectively.

The Compliance Officer monitors and evaluates, on an ongoing basis, the effectiveness of the measures and procedures, and in general the implementation of the risk management and procedures manual, that have been introduced.

The Compliance Officer applies appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force.

In the event that they identify any shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, the Compliance Officer gives appropriate guidance for corrective measures and, where deemed necessary, informs the Board of Directors.

4. Application of Customer Due Diligence (CDD)

Persons engaged in gambling activities, including the Company, apply customer identification procedures and customer due diligence measures when establishing a business relationship.

Senior management within remote gaming must be fully engaged in the decision-making process. They must take ownership of the risk-based approach because, along with the Compliance Officer, they may be held accountable if the approach is inadequate. This means engaging and participating in the decision-making process, which generates the risk-based policies adopted by the remote gaming operator.

To mitigate the risk of non-compliance with relevant laws and regulations, it is essential to conduct thorough and well-considered risk assessments, as well as to implement proportionate AML/CFT/CFP policies. These policies should be meticulously documented and include clear guidelines on reporting procedures, training requirements, and record-keeping practices.

Failure to implement sufficient systems and controls could lead to the operator being criminally liable or subject to regulatory sanctions, such as fines or license revocation. Remote gaming operators and those who work for them can reduce their personal risks by the implementation and adherence to such a program. The Company ensures there is a proper consideration of the risks, together with a consideration of the way in which they can be mitigated, with discussions and decisions being properly recorded and established procedures being followed in practice.

4.1. When to undertake CDD

Persons engaged in gambling, including the Company must undertake CDD measures:

- When players engage in financial transactions equal to or above Naf. 4,000;
- carrying out occasional transactions above the monetary equivalent of Naf. 4,000;
- there is a suspicion of money laundering or terrorist financing;
- the casino has doubts about the veracity or adequacy of previously obtained customer identification data;
- at any other time the Company's enhanced due diligence (EDD) program requires the casino to collect and verify further know your customer (KYC) information about a customer.

4.2. Ways of application of customer due diligence and identification procedures

Customer identification procedures and customer due diligence measures shall include the following:

- a) Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information .
- b) Identifying the beneficial owner and taking risk-based and adequate measures to verify the identity on the basis of documents, data or information obtained from a reliable and independent source so that the person carrying on in financial or other business knows who the beneficial owner is. Regarding legal persons, trusts and similar legal arrangements, taking risk based and adequate measures to understand the ownership and control structure of the customer.
- c) Obtaining information on the purpose and intended nature of the business relationship.

- d) Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the person engaged in financial or other business in relation to the customer, the business and risk profile, including where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

Persons engaged in gambling, including the Company, apply each of the above CDD measures but may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. The Company must be able to demonstrate that the extent of the measures is appropriate in view of the risks of the use of their services for the purposes of money laundering and terrorist financing.

4.3. Customer Identification Procedures

Casinos are prohibited from keeping anonymous accounts or accounts in obviously fictitious names. The Company must identify the player and ask for the player's name and other relevant information to determine the purpose and nature of the business relationship. The purpose of these procedures is the collection of primary information about the customer, analysis of the collected information and decision for proceeding or not with an agreement for offering the customer a particular service. Without sufficient knowledge, the casino may not establish or maintain a business relationship or carry out occasional transactions. The corporate department is responsible for the collection of all documents/information and the Compliance Officer is responsible to analyze the collected information. The customers of the company are subdivided in two categories:

- Normal risk; and
- High risk.

4.4. Normal risk customers

The following information should be obtained from prospective customers:

- a) True name and/or names used as these are stated on the official identity card or passport;
- b) Date and place of birth;
- c) Permanent residential address;
- d) Nationality;
- e) Identity number;
- f) Unique and verified email address;
- g) Telephone (home and mobile) and fax numbers;
- h) Confirmation of legality and source of the Customer's funds (if possible).

To complete the required customer identification and verification process, the Company asks its customers to upload a copy of valid identification documents. This request is sent to the customer's registered email address. If the documents are in a different language, the Company will take necessary steps to ensure that the documents adequately

prove the customer's identity, such as obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation.

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. Documents issued by the government that lack a photograph can be used to confirm the customer's current address, provided the address is included on the document.

Note: It is not acceptable to use the same verification data or information for verifying the customer's identity and verifying its home address. Thus, separate supporting documents to verify the customer's identity and their home address verification is required.

4.5. Enhanced Due Diligence Procedures

The Company considers the following customers as high risk and thus applies enhanced customer identification and due diligence procedures:

- Accounts in the names of companies whose shares are in bearer form;
- Trusts accounts;
- Companies incorporated in offshore centers;
- Client accounts in the name of a third person;
- Politically exposed persons' (PEP) accounts;
- Electronic gambling /gaming through the internet;
- Customers from countries which inadequately apply Financial Action Task Force's recommendations;
- any other customers that pose a high level of risk for money laundering or terrorist financing and are classified by the Company as high risk on the basis of its customers' acceptance policy.

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 EDD measures include but are not limited to:

- 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.

4.5.1. Accounts in the names of companies whose shares are in bearer form

The policy of the Company is not to accept customers whose companies have bearer shares. However, if in exceptional cases the Company chooses to open such an account, it will be strictly in compliance with the below regulations.

The Company may accept as customers companies whose own shares or those of their parent companies (if any) have been issued in bearer form by applying, in addition to the procedures described above for legal persons ***all the following supplementary due diligence measures:***

- The Company takes physical custody of the bearer share certificates while the business relationship is maintained or obtains a confirmation from a bank operating in the Republic or a country of the European Economic Area that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform the Company accordingly.
- The account is closely monitored throughout its operation. At least once a year, a review of the accounts' transactions and turnover is carried out and a note is prepared summarising the results of the review which must be kept in the customer's file.
- If the opening of the account has been recommended by a third person at least once every year, the third person who has introduced the customer provides a written confirmation that the capital base and the shareholding structure of the company or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones. If the account has been opened directly by the company, then the written confirmation is provided by the company's directors.
- When there is a change to the beneficial owners, the Company examines whether or not to permit the continuance of the account's operation.

Note: For all the above cases, the decision for establishing a business relationship or the execution of an occasional transaction is taken by an executive director and the decision is then forwarded to the Compliance Officer.

The account of the said customer is closely monitored and subject to regular review annually with a view of deciding whether to permit the continuance of its operation. Accordingly, a report is prepared and submitted for consideration and approval to the Board of Directors and filed in the customer's personal file.

4.5.2. Trusts accounts

When the Company establishes a business relationship or carries out an occasional transaction with trusts, it must ascertain:

- The legal substance of the trust;
- The name and the date of establishment of the trust;
- The nature of activities of the trust;
- Purpose of establishment of the trust;
- The source and origin of funds requesting the relevant extracts from the trust deed;
- Any other relevant information from the trustees;

- **And verify** the identity of the trustor, trustee and beneficial owners, according to the customer identification procedures prescribed above.

4.5.3. Client accounts in the name of a third person

The policy of the Company is to avoid opening omnibus accounts. However, if in exceptional cases the Company chooses to open such an account, it will be strictly in compliance with the below regulations.

The Company may open “client accounts” (e.g. omnibus accounts) in the name of:

- Financial institutions from European Economic Area countries or
- Financial institutions from a third country which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it applies procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the European Union Directive.

In the above cases the Company ascertains the identity of the abovementioned financial institutions according to the customer identification procedures prescribed above.

Note: For all the above cases, the decision for establishing a business relationship or the execution of an occasional transaction is taken by an executive director and the decision is then forwarded to the Compliance Officer.

The account of the said customer is closely monitored and subject to regular review annually with a view of deciding whether or not to permit the continuance of its operation. Accordingly, a report is prepared and submitted for consideration and approval to the Board of Directors and filed in the customer’s personal file.

4.5.4. Politically exposed persons (PEPs) accounts

The policy of the Company is to avoid setting up business relationship with politically exposed persons. If, however, the Company chooses in exceptional cases to do so, it will be in strict compliance with the below regulations.

In respect of transactions or business relationships with politically exposed persons residing in a country within the European Economic Area or a third country, the following additional due diligence measures will be applied:

- The Company will have appropriate risk-based procedures to determine whether the customer is a politically exposed person. These procedures may include, depending on the degree of risk:
 - The acquisition and installation of a reliable commercial electronic database for politically exposed persons.
 - Seeking and obtaining information from the customer himself or from publicly available information.
 - In the case of legal entities and arrangements, the Company will also verify whether the beneficial owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute politically exposed persons.
- Have executive director approval for establishing business relationships with such customers. The decision is then forwarded to the Compliance Officer.

- Take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction. The investigation must then determine whether the player's spending pattern matches his legal source of funds. The casino requests a statement from the player about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources. When public sources cannot, or can insufficiently verify the received information, the casino can request the customer to provide documents; and
- Conduct enhanced ongoing monitoring of the business relationship

The Compliance Officer shall make sure that the national law of the country or origin of the customer allows him/her, being a politically exposed person, to establish business relationship of this area of services. The Compliance Officer shall inform in writing the Board of the Company of the result of this investigation.

Should a player who had not been identified as a PEP at on-boarding stage result to have become one, the casino is required to implement the measures described above within 30 days or terminate the relationship.

More attention will be paid when the above persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards.

The account of the said customer is closely monitored and subject to regular review annually with a view of deciding whether or not to permit the continuance of its operation. Accordingly, a report is prepared and submitted for consideration and approval to the Board of Directors and filed in the customer's personal file.

4.5.5. Customers from countries which inadequately apply Financial Action Task Force's recommendations

The policy of the Company is to avoid setting up business relationship with customers from countries which inadequately apply Financial Action Task Force's recommendations. If, however, the Company chooses in exceptional cases to accept a customer originating from, residing in such a country (or a customer, in whose organizational structure there is a legal or natural person originating from or based in such a country), it must be in strict compliance with the below regulations.

The Company applies the following:

- Exercises additional monitoring procedures and pays special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the above recommendations.
- Transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a unusual transaction report is filed to FIU.

With the aim of implementing the above, the Compliance Officer consults:

- The country assessment reports prepared by the FATF (<http://www.fatf-gafi.org>);

- The country assessment reports prepared by other pertinent global and regional bodies, such as but not limited to:
 - MONEYVAL Committee of the Council of Europe (www.coe.int/moneyval);
 - EU Common Foreign & Security Policy (CFSP) (http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm);
 - UN Security Council Sanctions Committees (www.un.org/sc/committees/);
 - International Money Laundering Information Network (IMOLIN) (www.imolin.org);
 - International Monetary Fund (www.imf.org).

Based on the above reports, the Compliance Officer assesses the risk from transactions and business relationships with persons from various countries and decides of the countries that inadequately apply the FATF's recommendations. According to the aforesaid decision of the Compliance Officer, the Company applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating from countries with significant shortcomings in their legal and administrative systems for the prevention of money laundering and terrorist financing.

Note: For all the above cases, the decision for establishing a business relationship or the execution of an occasional transaction is taken by an executive director and the decision is then forwarded to the Compliance Officer.

The account of the said customer is closely monitored and subject to regular review annually with a view of deciding whether or not to permit the continuance of its operation. Accordingly, a report is prepared and submitted for consideration and approval to the Board of Directors and filed in the customer's personal file.

4.6. Failure or refusal to submit information for the verification of customers' identity

If a document submitted by a potential customer does not meet the verification standards, the compliance officer or designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance.

Once a non-compliant document is identified, the customer must be informed without delay. If the customer cannot provide compliant documents within 30 days from the moment the Naf. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and report the transaction to the FIU.

All actions taken in response to non-compliant documents must be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

4.7. Customer data recording

The data for all customers is recorded in a separate form designed for this purpose which is retained in the customer's file along with all other documents as well as all internal records of meetings with the respective customer. The above form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the customer or alters existing information that makes up the economic profile of the customer.

5. Ongoing Monitoring of Accounts and Transactions

5.1. Ongoing customer profile monitoring

The responsibility for the ongoing customer profile monitoring lies with the corporate department, in collaboration with the Compliance Officer. The primary goal of the Company is to maintain a comprehensive understanding of its customers' normal account activities and their economic profiles. To achieve this, the Company implements a robust monitoring system with the following objectives:

- Identification of high-risk customers.
- Detection of transactions that deviate from the regular activity patterns of an account.
- Recognition of complex and unusual transactions that are inconsistent with a customer's economic profile.
- Investigation of transactions lacking an obvious economic purpose or legitimate reason.
- Verification of the source and origin of funds credited to customer accounts.

During the periodic review of a customer, the Company verifies and confirms that the CDD information about the client, nature and purpose of the business relationship, and SOF is still accurate and up to date, evaluate if there are external signals (bad press/adverse news, incidents) that could give rise to a change in the business risk profile of the customer and ensure to perform screening against sanctions lists and PEP lists. The periodic review also includes an overall review of the transaction behavior of the client to determine if unusual activities have taken place, for instance in case of transactions which normally would not be expected. To ensure compliance, all findings will prompt necessary actions, including internal reporting of unusual activities to the Compliance Officer and, if required, to the Financial Intelligence Unit.

The Compliance Officer plays a crucial role in ensuring that customer identification records are consistently updated with all relevant data throughout the business relationship. Regular checks on the validity and adequacy of customer identification information are particularly emphasized for high-risk customers. The frequency of these checks is as follows:

- Annually for High-Risk customers.
- Every two years for Normal-Risk customers.

The outcomes of these reviews will be stored in the respective customer file. If, at any point during the business relationship, the Company identifies that reliable or adequate data is missing regarding a customer's identity or economic profile, the Compliance Officer will take immediate action to apply customer identification and due diligence procedures to collect the necessary information.

Additionally, the Compliance Officer will assess the adequacy of customer data whenever significant events occur, such as:

- a) Unusual or significant transactions that deviate from the normal transaction patterns and economic profile.
- b) Material changes in the customer's legal status, including changes in directors, shareholders, registered office, trustees, corporate name, or major business activities.
- c) Alterations in the operational rules of the customer's account, including changes in authorized personnel or requests for new accounts.

5.2. Ongoing transaction monitoring

The Company shall perform both real time monitoring of transactions, as well as post-event monitoring, to ensure that such transactions and activity are consistent with the Company's knowledge of the client and their expected activity. More attention is paid to high amounts, high-risk clients and high-risk jurisdictions.

Transactions will be evaluated by the executive director in collaboration with the Compliance Officer against criteria such as anticipated account turnover, the typical operational turnover of the customer, and the data maintained in the customer's economic profile. Significant deviations will be thoroughly investigated, and findings will be documented in the respective customer files.

The Company already has in place an automated electronic management information system (MIS) and it has introduced new functions in this MIS which are capable of supplying the Board of Directors and the Compliance Officer, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of customer profile. The Company will take further steps to introduce the functions to effectively monitor the customers' accounts and transactions based on the assessed risk for money laundering or terrorist financing purposes. The decision for implanting this system will depend on the nature, scale and complexity of its business and the nature and range of the investment services and activities undertaken during that business.

The above MIS is used to extract data and information that is missing regarding the customer identification and the construction of a customer's economic profile, while taking into account:

- the economic profile of the customer;
- the country of his origin;
- the source of the funds;
- the type of transaction; or
- other risk factors.

6. Reporting of Unusual Transactions

6.1. Recognition of unusual transactions

The definitions of an unusual transaction, as well as the types of unusual transactions which may be used for money laundering and terrorist financing, are almost unlimited. An unusual transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Company has created for the customer. The Company ensures that it maintains adequate information and knows enough about its customers' activities in order to recognize on time that a transaction or a series of transactions is unusual.

The list containing examples of what might constitute unusual transactions/activities related to money laundering and terrorist financing (see list below) is not exhaustive nor includes all types of transactions that may be used, nevertheless it can assist the Company and its employees in recognizing the main methods used for money laundering and terrorist financing. The detection by the Company of any of the transactions contained in this list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity:

- Transactions with no discernible purpose or unnecessarily complex.
- Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the customer.
- The transactions or the size of the transactions requested by the customer do not comply with his usual practice and business activity.
- Large volume of transactions and/or money deposited or credited into, an account when the nature of the customer's business activities would not appear to justify such activity.
- The business relationship involves only one transaction, or it has a short duration.
- The settlement of any transaction but mainly large transactions, in cash.
- Transfer of funds to and from countries or geographical areas which do not apply, or they apply inadequately FATF's recommendations on money laundering and terrorist financing.
- A customer is reluctant to provide complete information when establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with other Organizations, names of its officers and directors, or information on its business location. The customer usually provides minimum or misleading information that is difficult or expensive for the Company to verify.
- A customer provides unusual or suspicious identification documents that cannot be readily verified.
- A customer that makes frequent or large transactions and has no record of past or present employment experience or any other working experience.
- Customer and the person introducing the customer come from countries where production of drugs or drug trafficking may be prevalent
- Unexplained inconsistencies arising during the process of identifying and verifying the customer (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc.).
- Transactions or company structures established or working with an unneeded commercial way. e.g. companies with bearer shares or bearer financial instruments or use of a postal box.
- Changes in the lifestyle of employees of the Group e.g. luxurious way of life or avoiding being out of the office due to holidays.

- Changes the performance and the behaviour of the employees of the Group.

In cases where there is an attempt of executing transactions, which the Company knows or suspects to be related to ML, TF and/or PF, the Compliance Officer must report the transaction to the FIU.

6.2. Reporting procedures

All unusual activities and transactions, including attempted transactions, are initially reported internally. The officers responsible for transaction monitoring must immediately report any unusual activities to the Compliance Officer upon identification, providing a brief description of the specific mitigating measures taken.

All employees who engage with customers or have access to customer information receive anti-money laundering training. This training prepares them to identify actions by customers that may reasonably raise suspicions of money laundering or terrorism financing. Staff members are expected to recognize and understand any gaming or transaction behaviours that might indicate customer involvement in money laundering or terrorism financing. If they know, suspect, or have reasonable grounds to believe they are dealing with the proceeds of crime, they must submit an internal report to the Compliance Officer (CO) in accordance with the Reporting Procedure. This ensures that the employee's legal obligation to report is fulfilled.

The Compliance Officer receives information from the Company's employees in a written report form (see [Appendix 2](#)). The Compliance Officer will conduct a preliminary review of the reported activity within **24 hours** to assess whether it requires further investigation. The evaluation of the information received is done in writing (see [Appendix 3](#)).

If a more in-depth investigation is necessary, the Compliance Officer will complete this within **five (5) business days**. During this time, the Compliance Officer may request additional information from relevant departments.

After completing the evaluation, if the Compliance Officer chooses not to report to the Financial Intelligence Unit (FIU), a detailed explanation for this decision must be documented in the "*Internal Evaluation Report*." This documentation should include the actions taken, questions posed, and the responses received. By doing so, the Company demonstrates the methodology used to assess potential threats and the rationale behind the selection of appropriate systems and procedures, including due diligence requirements.

If the Compliance Officer concludes that the activity is unusual, an report must be submitted to the FIU Curaçao without undue delay (see [Appendix 4](#)).

All the reports of the Compliance Officer are sent or submitted to FIU by post, facsimile or by hand.

6.3. Submission of information to FIU

The Company ensures that in the case of a unusual transaction investigation by FIU, will be able to provide without delay the following information:

- a) the identity of the account holders
- b) the identity of the beneficial owners of the account
- c) the identity of the persons authorised to manage the account

- d) data of the volume of funds or level of transactions flowing through the account on the basis of the information that the Company has on the day of request
- e) connected accounts
- f) in relation to specific transactions:
 - i. the origin of the funds
 - ii. the type and amount of the currency involved in the transaction
 - iii. the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers, iv. the identity of the person that gave the order for the transaction
 - iv. the destination of the funds
 - v. the form of instructions and authorisation that have been given
 - vi. the type and identifying number of any account involved in the transaction

6.4. Cooperation with FIU after reporting unusual transactions/activities

After the submission of the Compliance Officer's report to FIU, the accounts involved and any other connected accounts, are closely monitored by the Compliance Officer.

The Company adheres to any instructions given by FIU and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active. FIU may instruct the Company to refrain from executing or delay the execution of a customer's transaction without such action constituting a violation of any contractual or other obligation of the Organisation and its employees.

The Compliance Officer acts as the first point of contact with FIU, upon commencement and during an investigation as a result of filing a report to FIU.

6.5. Failure to report

It is an offence for any person, including employees of the Company who, in the course of his trade, profession, business or employment, acquires knowledge or reasonable suspicion that another person is engaged in money laundering or terrorist financing not to report his knowledge or suspicion to Unit for Combating Money Laundering, known shortly as FIU (Financial Intelligence unit), as soon as it is reasonably practical after the information came to his attention. Failure to report in these circumstances is punishable on conviction.

6.6. Prohibition of disclosure

All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of the NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

The Company has implemented a system of measures to ensure that employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the Financial Intelligence Unit Curaçao are safeguarded from threats or hostile actions by other employees, members of the management body, or customers. Additionally, they are protected from adverse or discriminatory employment actions.

After the submission of an unusual report the Company may subsequently wish to terminate its relationship with the customer concerned for risk avoidance reasons. In such an event, the Company exercises caution not to alert the customer concerned that an unusual report has been submitted to FIU (tipping off). Close liaison with FIU is, therefore, maintained to avoid any frustration to the investigations conducted.

7. Record Keeping

7.1. Record keeping of documents/data

The Company keeps a record of the following documents/data:

- copies of the evidential material of the customer identity;
- relevant evidential material and details of all business relations and transactions, including documents for recording transactions in the accounting books;
- relevant documents of correspondence with the customers and other persons with whom they keep a business relation;
- evaluation of the systems and procedures applied by a third person on whom the Organisation relies for customer identification and due diligence purposes.

The Company ensures that all the above documents are made available rapidly and without delay to the competent supervisory authorities for the purpose of discharging their duties.

7.2. Time period of keeping documents/data

The above documents/data are kept for a period of at least five (5) years, which is calculated after the execution of the transactions or the termination of the business relationship.

The documents/data relevant to ongoing investigations are kept until FIU confirms that the investigation has been completed and the case has been closed.

After the retention period, records shall be disposed of securely to prevent unauthorized access or disclosure. Electronic records must be permanently deleted using secure deletion software that ensures data cannot be recovered. Physical records must be shredded using cross-cut shredders or incinerated to ensure complete destruction.

7.3. Format of records

Records shall be stored in a manner that ensures their integrity, confidentiality, and accessibility. Electronic records shall be stored in secure, encrypted databases with access controls to prevent unauthorized access. Physical records shall be stored in locked, fireproof cabinets within secure areas of the office. Access is restricted to authorized personnel only. Regular backups of electronic records shall be conducted and stored in a separate, secure location to prevent data loss.

7.4. Certification and language of documents

The documents/data obtained should be in their original form or in a certified true copy form. In the case that the documents/data are certified as true copies by a different person than the Company itself or by the third person the documents/data must be apostilled or notarised.

A true translation is attached in the case that the above documents/data are in a language other than English.

8. AML Compliance Program

8.1. Board of Directors Responsibilities

The Board of Directors is entrusted with the following responsibilities:

- Establishing, documenting, and approving the overarching policy principles of the Company concerning the prevention of money laundering and terrorist financing, and ensuring communication of these principles to the Compliance Officer.
- Appointing a Compliance Officer, as well as any necessary assistant Compliance Officers.
- Defining the duties and responsibilities of the Compliance Officer and any assistant Compliance Officers.
- Approving the customer acceptance policy.
- Endorsing the risk management and procedures manual.
- Ensuring the dissemination of the risk management and procedures manual to all employees.
- Guaranteeing compliance with all statutory requirements.
- Implementing appropriate, effective, and adequate systems and controls.
- Overseeing day-to-day compliance with money laundering and terrorist financing obligations within their respective areas of responsibility.
- Ensuring timely communication to the Compliance Officer regarding any unusual or suspicious transactions and other significant matters.
- Providing the Compliance Officer with comprehensive and timely access to all customer identity, transaction documentation, and other pertinent files to enable effective fulfilment of their duties.
- Allocating necessary resources for the Compliance Officer to perform their role effectively.
- Ensuring the Compliance Officer has autonomy in the evaluation process for suspicious transaction reporting (STR) and unrestricted access to information required for this process.
- Making all employees aware of the designated Compliance Officer and their assistants.
- Establishing a clear and swift reporting protocol for suspicious transactions directed to the Compliance Officer.
- Evaluating and approving the Compliance Officer's Annual Report.
- Taking appropriate actions to rectify any weaknesses or deficiencies identified in the Compliance Officer's Annual Report.

8.2. Compliance Officer

The Board of Directors appoints a Compliance Officer who is part of the Company's management, thereby ensuring the requisite authority to perform their duties. Depending on the volume and geographic distribution of services, assistant Compliance Officers may also be appointed to assist in processing internal suspicion reports. The Company shall promptly communicate the names and positions of the appointed Compliance Officer and assistants to the regulatory authority.

The Compliance Officer's responsibilities encompass the following:

- **Design of Measures, Procedures, and Controls:** Develops internal practices, measures, and controls to prevent money laundering and terrorist financing, clearly delineating the responsibilities of each relevant department. Implements measures to mitigate risks associated with new technologies and financial systems that could facilitate money laundering and terrorist financing.

- **Development of Customer Acceptance Policy and Risk Management Manual:** Formulates and establishes the customer acceptance policy, submitting it to the Board for approval. Prepares a comprehensive risk management and procedures manual concerning money laundering and terrorist financing.
- **Monitoring:** Monitors and evaluates the implementation of policies, practices, measures, and controls, providing guidance on corrective actions as necessary.
- **Internal Reporting Procedures:** Receives and evaluates internal suspicion reports from employees concerning potential money laundering or terrorist financing activities. Acts as the primary liaison with the Financial Intelligence Unit (FIU) during investigations.
- **Preparation of Customer Risk Lists:** Ensures the maintenance of a risk-based customer list, categorizing customers according to assessed risk levels.
- **Risk Detection and Procedure Updates:** Conducts annual evaluations of risks posed by customers and financial instruments, updating procedures accordingly.
- **Training:** Provides guidance and training to employees on money laundering and terrorist financing matters, developing an annual training program tailored to the needs of various departments.
- **Reporting:** Prepares the Compliance Officer's annual report, responding to inquiries from regulatory authorities and maintaining comprehensive records of reports.
- **Compliance Officer's Annual Report:** The Compliance Officer's Annual Report serves as a critical tool for assessing the Company's compliance levels, outlining measures taken, deficiencies identified, and recommendations for improvement.

8.3. Employees' Obligations and Training

8.3.1. Employee Due Diligence

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing the Company's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors.

The employee due diligence process is informed by the Company's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate money laundering or terrorism financing must undergo screening. This requirement applies to:

- Prospective employees prior to their hiring for such roles.
- Current employees before they are transferred or promoted to such positions.

To screen both current and potential employees, the Company should:

- Identify the individuals.
- Verify their identity.
- Confirm their employment history, such as through references.
- Determine their suitability for the position and assess whether they pose any risk to the Company.

The Company will consider the knowledge and qualifications required for the responsibilities and authorities associated with each role. Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. The Company must evaluate whether the employee:

- Has a criminal record, which may be verified through a police check.
- Is or has been subject to regulatory, court, or legal actions.
- Has leveraged bankruptcy laws for personal gain.
- Has resided in high-risk countries or regions.

Regular updates and re-evaluations are essential for maintaining an effective compliance program against money laundering, terrorism financing, and proliferation financing. This process includes conducting periodic reviews of all employees, with a particular emphasis on those in high-risk roles, to ensure their risk profiles are accurate and current. Additionally, reviews triggered by significant changes in an employee's job responsibilities, promotions, or external alerts that may influence their risk status are also initiated.

8.3.2. Employee Obligations

Employees may be held personally liable for failing to report any suspicions regarding money laundering or terrorist financing. Employees are required to cooperate fully and report any unusual transactions without delay through the Internal Unusual Transaction Report.

8.3.3. Employee Education and Training Program

The training curriculum prepared by the Compliance Officer will address the latest developments in the prevention of money laundering and terrorist financing, tailored to the specific needs of different departments and employee roles. Ongoing training will be conducted regularly to ensure continuous awareness and compliance with relevant policies and procedures.

8.4. Independent Audit

An independent audit function will be established for the annual evaluation of the AML program, ensuring audit personnel are qualified and findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML/CTF/CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.

- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate the Company's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

APPENDIX 1: Development and Establishment of Customer Acceptance Policy (CAP) on a Risk-Based Approach

The Company customer's acceptance policy is prepared by the Compliance Officer after detailed assessment of the risks faced by the Company. In this regard the Company applies appropriate measures and procedures, on a risk-based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher.

1.1 Risk criteria

The Compliance Officer identifies records and evaluates three main risk criteria when assessing the extent of money laundering and terrorist financing risks. Based on the extent and the combination of the given risk criteria, the overall risk of a customer will be quantified as High, Normal or Low.

The Compliance Officer considers the following risk criteria:

- Country or geographic risk
- Customer risk
- Products/services risk
- Delivery channel risk

Further analysis of the above risk criteria (individually or in combination) in assessing the overall risk of potential money laundering and terrorist financing is shown below.

The Compliance Officer should document and periodically review its risk assessment approach.

1.2 Risk indicators

The Compliance Officer analyses the above risk criteria into different risk indicators as shown in the following table (table 1.2.1):

Table 1.2.1: Risk Indicators

Risk Criteria	Risk Indicator
Customer Risk	Customer characteristics/behaviour/History
	Customer Business
	Customer ownership structure
	Duration of Business relationship
	Business activity/Expected transaction turnover

Product and Service Risk	Transaction Types
	Product/service Types
Country/Geographic Risk	Country/Geographic Risk

1.3 Risk Variables

For each risk indicator the Compliance Officer identifies various “risk variables”, as shown in the following table (table 1.3.1):

Table 1.3.1: Risk Variables

Risk Criteria	Risk Indicator	Risk variables
Customer Risk	Customer characteristics/behaviour/History	No financial/commercial rationale for the customer performing the specific transaction
		The origin of wealth and/or source of funds cannot be easily verified
		Requests to associate undue levels of secrecy (unwillingness to provide information on the beneficial owners)
		Accounts for "gatekeepers" (accountants, lawyers, or other professionals) for their clients
		Reliance for KYC and AML matters on the gatekeeper
		Number of related accounts
		SAR Filed Previously
		CTR Filed Previously
	Customer Business	Weapon manufacturers
		Art and antique dealers
		Dealers in high value or precious goods
		Real estate agents
		Unregulated charities
		Unregulated "non for profit" organisations
		Remittance houses
		Exchange houses

		Casinos
		Betting
		Gabling related
		Money transfer agents
		Bank note traders
		Cash intensive business
	Customer ownership structure	Complex business ownership structures
		Transparency structure
		Bearer shares
		Incorporated in offshore centres
	Duration of Business relationship	D < 1 year
		1 year < D < 3 Years
		D > 3 years
	Business activity/Expected transaction turnover	Turn < 100,000
		100,000 < Turn < 500,000
		Turn > 500,000
Product and Service Risk	Transaction Types	Cash transactions
		Size of transaction
	Product/service Types	Do the products/services allow/facilitate payments to third parties
		Can the product/service features be used for money laundering or terrorist financing, or to fund other crime
		Do the products/services intended to render the customer deliberately anonymous to the Company
Country/Geographic Risk	Country/Geographic Risk	FATF recommendations
		Transparency International (CPI)
		MONEYVAL

		EU Common Foreign & Security Policy (CFSP)
		UN Security Council Sanctions Committees
		International Monetary Fund (IMF)
		Office of Foreign Assets Controls (OFAC)
		Transactions to/from high-risk jurisdictions
		Low Risk jurisdiction

1.4 Risk classification model

- For each customer/account, the Compliance Officer analyses the different risk criteria we mentioned before (customer, product/service, geographic risk and delivery channel risk) and assigns scores and weights to the various risk variables and risk indicators.
- The Compliance Officer combines the risk ranking (High or Neutral) from each risk criteria at the customer level to determine the overall risk level.
- The Compliance Officer completes the table below (table 1.4.1).
- The Compliance Officer has the authority, at his/her absolute discretion not to follow the standard procedure described in this section if he/she believes that by following the procedure, for specific customer, the assigned classification will not be correct.

Table 1.4.1: Customers risk classification

Risk Levels	Unique Combinations	Customer Risk	Product/ Transaction Risk	Geographic Risk
Risk Level 1	1	H	H	H
	2	H	H	N
	3	H	N	H
	4	N	H	H
Risk Level 2	5	H	N	N
	6	N	H	N
	7	N	N	H
Risk Level 3	8	N	N	N

H = High Risk

N = Neutral Risk

With this model we have 3 Risk Levels. Risk Level 1 represents accounts with the highest risk.

- **Risk Level 1 (High risk customer):** Accounts with two or three (2 or 3) High Risk designations.
- **Risk Level 2 (Normal risk customer):** Accounts with one (1) High Risk designation.
- **Risk Level 3 (Normal risk customer):** Accounts with no High-Risk designations.

1.5 Customer's categories

Based on the criteria described above customers will be categorised in the following three categories:

- Normal risk (Risk level 2 and Risk level 3)
- High risk (Risk level 1)

1.6 Categories of customers who are not acceptable for establishing a business relationship or an execution of an occasional transaction

All customers are carefully examined by the Compliance Officer as described above and the decision is taken on a case-by-case basis. To approve an application, the Compliance Officer must verify the following:

- the correctness, authenticity and completeness of the information provided by the applicant;
- the creditworthiness of the applicant, through a database search whenever this deems necessary;
- the probability that the applicant is involved in illegal or criminal activities; and
- the completeness of the required agreement/identification documents.

The Compliance Officer shall reject all applications that:

- do not include all the necessary information; or
- involve persons of doubtful creditworthiness or persons that may be involved in illegal or criminal activities.

1.7 Approval of customers' acceptance policy

The Compliance Officer submits the customers' acceptance policy to the Board of Directors for consideration and approval.

1.8 Analysis of customer primary information and writing of the report

The Compliance Officer performs analysis of the collected data, and the risk assessment described above for the purpose of:

- Examination, whether or not the Customer of the company/its environment or partners are involved in any illegal actions in the territory of resident country or any other countries, relations with terrorist organizations or criminal structures.
- Determination of origin of the Customer's funds and their amount. This information is necessary to answer to the question of legality and "cleanness" of the Customer's funds and of the predictable turnover for his accounts and size of transactions.
- Determination of the expected transfer of funds in the Customer's accounts.

- Determination of nature of the Customer's activities. This information is necessary to answer to the question of the Customer's standard operations characteristic for his business.

Analysis of primary information and writing of the report is executed by the Compliance Officer on the basis of data obtained. Special attention on the analysis process is paid to availability of the following indications of the Customer involvement in Legalization:

- Does the Customer provide any information on himself reluctantly?
- Information does not comply with the reality
- Information is not full or contradictory

The result of the analysis is drawn up in the form of a report containing characteristics of the Customer and recommendation on further interaction with him with obligatory indication in the case of a corporation of the following:

- Determination of the real (beneficiary) holder of the Customer's business
- Persons realizing operational control and decision making
- Sources of origin of the Customer's funds and purposes of their usage
- Understanding of the Customer's business and financial transactions accompanying it
- Legal limitations of the Customer activity

Or in the case of a private customer of the following:

- Determination of the real owner of the funds (his existence and position)
- Determination of primary of rise of means and directions of their usage
- Legal limitations of the Customer activity

Upon the results of the analysis, the Compliance Officer writes the report including basic characteristics of the Customer and recommendations on further interaction with him as described in section 1.6 above.

If following the conducted examination and analysis no alarming moments were detected testifying for involvement of the Customer in Legalization, then the necessary contracts should be concluded with the Customer.

Otherwise, in the presence of any justified conclusions about involvement of the Customer in Legalization the Compliance Officer should be obliged to send the report in the established form to respective controlling bodies without notification of the Customer, and the reasoned refusal should be sent to the latter.

The decision on account opening and beginning its servicing is made by the executive director. It is forbidden to accept any order from the Customer before completion of the procedure of verification, analysis and writing the report. It is forbidden to open anonymous accounts or accounts in Favor of any dummy holders or private customers.

APPENDIX 2: Internal Unusual Report for Money Laundering and Terrorist Financing

INTERNAL UNUSUAL REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING	
<u>INFORMER'S DETAILS</u>	
Name: Tel: Department:	
..... Fax:	
Position:	
<u>CUSTOMER DETAILS</u>	
Name:	
Address:	
..... Date of Birth:	
Tel: Occupation: Fax:	
..... Details of Employer:	
.....	
Passport No.:	Nationality:
ID Card No.:	Other ID Details:
<u>INFORMATION / SUSPICION</u>	
Brief description of activities/transaction:	
.....	
Reason(s) for suspicion:	
.....	
..... Informer's Signature Date	
.....	
<u>FOR COMPLIANCE OFFICER' USE</u>	
Date Received: Time Received: Ref: Reported to FIU:	
Yes/No Date Reported: Ref:	

APPENDIX 3: Internal Evaluation Report for Money Laundering and Terrorist Financing

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING	
Reference:	Customer's Details:
Informer:	Department:
<u>INQUIRIES UNDERTAKEN (Brief Description)</u>	
.....	
.....	
..... <u>ATTACHED DOCUMENTS</u>	
.....	
.....	
.....	
.....	
<u>COMPLIANCE OFFICER'S DECISION</u>	
.....	
.....	
.....	
FILE NUMBER:	
<u>COMPLIANCE OFFICER'S SIGNATURE</u>	<u>DATE</u>
.....	

APPENDIX 4: Compliance Officer's Report to the Unit for Combating Money Laundering (FIU)

COMPLIANCE OFFICER'S REPORT TO THE UNIT FOR COMBATING MONEY LAUNDERING (FIU)		
I. <u>GENERAL INFORMATION</u>		
Organisation's Name:		
Address where customer's account is kept:		
Date when a business relationship established or occasional transaction was carried out:		
Type of account(s) and number(s):		
II. <u>DETAILS OF NATURAL PERSON(S) AND/OR LEGAL ENTITY(IES) INVOLVED IN THE UNUSUAL TRANSACTION(S)</u>		
(A) <u>NATURAL PERSONS</u>		
	<u>Beneficial owner(s) of the signatory(ies) of account(s)</u>	<u>Authorised the account(s)</u>
Name(s):		
Residential address(es):		
Business address(es):		

Occupation and Employer: _____

Date and place of birth: _____

Nationality and passport _____ number:

(B) LEGAL ENTITIES

Legal entity's name, country and date of _____ incorporation:

Business address: _____

Main activities: _____

	<u>Name</u>	<u>Nationality and passport number</u>	<u>Date of birth</u>	<u>Residential address</u>	<u>Occupation and employer's details</u>
Registered Shareholder(s)	1. _____	_____	_____	_____	_____
	2. _____	_____	_____	_____	_____
	3. _____	_____	_____	_____	_____
Beneficial Owner(s) (if different from above)	1. _____	_____	_____	_____	_____
	2. _____	_____	_____	_____	_____
	3. _____	_____	_____	_____	_____
Directors	1. _____	_____	_____	_____	_____
	2. _____	_____	_____	_____	_____
	3. _____	_____	_____	_____	_____
Authorized signatory(ies) account(s)	1. _____	_____	_____	_____	_____
	2. _____	_____	_____	_____	_____
	3. _____	_____	_____	_____	_____

III. DETAILS OF UNUSUAL ACTIVITIES

Details of unusual activities should be given

1. _____

2. _____

3. _____

4. Knowledge/suspicion of money laundering or terrorist financing (please explain, as fully as possible the knowledge or suspicion connected with money laundering or terrorist financing)

5. Other information – Other services provided to the customer(s)

Compliance Officer's Signature

Date

.....

.....

NB. The above report should be accompanied by photocopies of the following:

1. For natural persons: The relevant pages of customer's passport or ID card evidencing identity
2. For legal entities: certificates of incorporation, directors and shareholders.

3. All documents relating to the unusual transaction (s).