



Manual and Regulations for combating Money Laundering, the Financing of Terrorism and Proliferation of weapon and mass destruction

WCG B.V.
Korporaalweg 10, Willemstad, Curacao
Version 3 - 2025

CONTENT

1. INTRODUCTION	2
1.2. Purpose of this Manual	2
1.3. Our Operations	3
2. LEGAL REQUIREMENTS	3-4
2.1. What is Money Laundering	4
2.2. What is Financing of Terrorism	4-5
2.3. What is Financing or Proliferation of Weapons	5
3. KEY ROLES AND RESPONSIBILITIES	5
3.1. Money Laundering Reporting Officer	5-6
3.2. Company's Management	6
3.3. Employees of the Company	6
4. RISK ASSESSMENT	6
4.1. Risk Approach	6-7
4.2. Business Risk Assessment	7-8
4.3. Customer Risk Assessment	8
5. GENERAL PRINCIPLES OF THE CAP	8-9
6. DUE DILLIGENCE GENERAL PRINCIPLES	9-10
- Nature and Frequency of Transactions	10
- Source of Funds being transacted	10
- Anonymous Accounts	10
7. DUE DILLIGENCE IN PRACTISE	11
-Identification of Customers	11-12
-Customer's Verification	12-14
-Enhanced Due Dilligence	14-15
-Source of Funds and Wealth	15
-Dealing with sanctioned persons	15-16
-Table 1 – KYC Matrix	16
-Table 2 – Player Risk Matrix	16-17
8. ONGOING MONITORING	17
-Inability to complete CDD	17-18
-Ongoing Monitoring of Transactions	18-19
-Ongoing Monitoring of Identity	19
9. RECORD KEEPING PROCEDURES	19
-Record of Transactions	19-20
-Retention of Records	20-21
10. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES TO THE UNIT	21
-Tipping Off Offence	21-22
-Confidentiality of report	23
-Discharge of Liability	23-24
-Protection of Persons Reporting	24
-Disclosure in Good Faith	24
11. ANTI MONEY LAUNDERING COMPLIANCE PROGRAM	24
- Money Laundering Reporting Officer and Monday Laundering Compliance Officer	24-25
11.1. Staff education, training, and development	25 -26
12. TARGETED FINANCIAL SANCTIONS	26-27
13. PROCEEDINGS	27
Appendix 1	28

1. INTRODUCTION

1.1. The Company

WCG B.V. having company registration number 152285, registered at Korporaalweg 10, Willemstad, Curacao and licensed by the Curaçao Gaming Authority to offer games of chance under license number OGL/2024/826/0339.

The operation of WCG B.V.. is conducted by its subsidiary entity Kalimela Limited a company incorporated in Cyprus with Registration Number HE 411381, registered at Dimofontos Street, Lamda Tower, 6th Floor, 1075, Nicosia, Cyprus is the acting Merchant of Record. Kalimela Limited is acting as the Merchant of Record (MoR), for transaction purposes on behalf of WCG B.V.

Based on the above, the present Manual, applies to both WCG B.V. and Kalimela Limited hereinafter both referred as '**The Company**'.

1.2. Purpose of this Manual

The aim of this manual is to set out the policies, procedures, systems and controls necessary to meet the obligations of the Company that operates from Curacao and is held to compliance with National Ordinance on identification when rendering services (NOIS) and National Ordinance on the reporting of unusual transactions (NORUT).

With the publication of the National Decree supervisor identification when rendering services gaming sector and the National Decree supervisor unusual transactions gaming, the Curaçao Gaming Control Board (GCB) is tasked with the AML/CFT/CFP supervision of the gaming sector operating in and from Curaçao.

The procedures that are appropriate for the purpose of forestalling and prevention of money laundering include:

- Identification
- Record keeping
- Staff education, training and development
- Internal procedures including the reporting of suspicious transactions, both internal and external

It is the Company's policy that NOIS and NORUT obligations to prevent money laundering are to be met in full and the company is committed to meeting and where possible exceeding such obligations.

The Company will not continue established relationships with participants whose conduct gives rise to suspicion of involvement with illegal activities. The company will seek to terminate any participant relationship where the participant's conduct gives reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion to the Curacao Financial Intelligence Unit (FIU) and thereafter shall be undertaken in conjunction with the relevant Government of Curacao authorities and in accordance with Curacao custom and practice to avoid any risk of the Company committing a tipping-off offence.

1.3. Our Operations

The nature of the gambling products made available by the Company and the “arm’s length” nature of the relationship we have with customers brings with them an increased risk from ML (placement, layering and integration might all be possible through an online gaming service) and TF activities, and it is therefore beholden on us as an organization to be diligent when scrutinizing customer transactions on our online gaming products and entering into contractual arrangements with third parties.

Our assessment is based on the following:

- Products – casino products offer a risk of ML/TF due to their high return to player. Certain games, like slots and roulette offer a higher risk than others. Stolen or misappropriated credit and debit cards (i.e. proceeds of crime) can be used to deposit into a customer account. Other ML/TF can occur through the use of multiple deposit/withdrawal mechanisms.
- Customers – we expect a small proportion to be high value players and because of the amounts involved there is an associated risk of money laundering.

Additionally, the business also faces the same risks from its third-party suppliers; particularly where the supply in question is of software or hardware pertaining to the gaming equipment.

A risk assessment is undertaken both annually and when these conditions change, including instances when new third-parties are contracted by the company.

If the minimum requirements set out in this document cannot be applied in certain circumstances or country, because application would be against local law or cannot be enforced due to other than legal reasons, we will not:

- Enter into a business relationship;
- Continue a business relationship or
- Carry out any transactions;

with someone located in that country. If business relations already exist in that country, we will ensure that the business relationship is terminated regardless of other contractual or legal obligations.

2. LEGAL REQUIREMENTS

The Company’s policies and procedures are based upon the regulations referred below and associated guidance issued by the Curaçao Gaming Control Board.

The laws and Regulations are form the main legal basis for the Curacao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);

- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of Article 2 of the sanctions National Ordinance, containing implementation of the United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation article 2 of the Sanctions National Decree containing implementation of the of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of Article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30)
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34)
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)

2.1. What is Money Laundering?

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- **Placement.** During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- **Layering.** This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- **Integration.** The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

2.2. What is Financing of Terrorism?

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations.

A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods like those criminal

organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

2.3. What is 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.

3. KEY ROLES AND RESPONSIBILITIES

3.1. Money Laundering Reporting Office

General

The MLRO shall be skilled, knowledgeable and experienced in the services or other business activities, in which the Company may be involved or as otherwise applicable. The MLRO shall also have the resources, expertise as well as access to all relevant information necessary to perform his duties adequately and efficiently.

The level of remuneration of the MLRO shall not compromise his/her objectivity.

In performing his/her role, the MLRO takes into account the nature, scale and complexity of its business, and the nature and range of services and activities undertaken in the course of that business.

Duties of the MLRO

During the execution of his/her duties and the control of the compliance of the Company with the Law and the Directive, the MLRO shall obtain and utilize data, information and reports issued by international organisations.

The duties of the MLRO shall include, inter alia, the following:

- Developing necessary policies, procedures, training and education of staff.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations and experience/advice from enforcement agencies.
- Representing the Company to all external agencies and any other third- party making enquiries in relation to money laundering prevention or compliance.
- Ensuring that all parts of the Company are complying with the stated policy and therefore monitoring operations and development of the policy to this end.
- Undertaking the internal review of all suspicions and determining whether such suspicions have substance and require disclosure to the FIU.
- All contact between the Company and the Authorities in respect of routine reports to law enforcement in respect of any specific investigations.
- Establishing the suspicious reporting process and ensuring that this process is understood by all staff.
- Maintenance of the register of internal and external disclosures and register of money laundering and financing of terrorism enquiries.
- Establishing, recording, maintaining and operating appropriate procedures and controls for monitoring and testing compliance with the AML/CFT/CFP legislation.

- Adopt policies which manage the risks identified by the Company's business risk assessment, monitor the performance of these policies and address any deficiencies identified.
- Submission of a report, on at least an annual basis, to the Company's senior management that describes:
 - Any new developments within the industry in relation to AML/CFT/CFP including updates to any legislation or regulatory guidance.
 - Any updates to the Company's internal AML/CFT/CFP procedures and policies.
 - Any activities relating to compliance with the NOIS and NORUT.

If while carrying out their duties, the MLRO raises concerns in relation to procedures and practises followed by the Company, will draft an internal report for the Management & Directors providing evidence of her concerns.

3.2. Company's Management

The Company's management is responsible for:

- The day-to-day compliance with AML/CFT/CFP obligations within the areas of the Company for which they are responsible.
- Ensuring that the MLRO is provided with prompt advice of unusual/suspicious transactions and other matters of significance.
- Providing the MLRO and AML/CFT/CFP Compliance Officer with the appropriate resources to fulfil their functions effectively.
- Ensuring that the MLRO has complete autonomy in the suspicious activity report evaluation process and unfettered access to information necessary to carry out that process.
- The Directors and MLRO will ensure that he/she is provided with or has access to the necessary resources to keep up to date with new money laundering requirements and developments.

3.3. Employees of the Company

All employees are responsible for:

- Remaining vigilant to the possibility of money laundering.
- Reporting to the MLRO all knowledge or suspicions of money laundering.
- Complying fully with all money laundering procedures in respect of client identification, client monitoring, record keeping, vigilance and reporting.

4. RISK ASSESSMENT

4.1. Risk Approach

As a subject person, the company follows a risk-based approach in operating its business. We strive to take the appropriate steps, proportionate to the nature and size of our business, to identify and assess the risks of ML/TF that arise out of its activities or business, considering risk factors listed below. For the avoidance of doubt, the analysis also takes into account the risk-rating process of all customers

The Company adapts its measures, controls, policies and procedures and day-to-day scenarios and operations further to the risk assessment conducted. Indeed, the application of checks are designed in a proportionate manner to the assessed risks. Reporting metrics and KYC

databases are efficient and effective automated controls on ML/TF as are trained staff, constantly monitoring player activity.

The Company considers the ML/TF risk on the basis of the following risk factors **See Table 2 – Player’s Key Matrix** in pages 15-16:

- Customer risk/nature/type
- Location
- Transactions – payment methods
- Transactions amount

Customer Risk

We consider that the assessment of the risk posed by a natural person is generally based on the person’s economic activity and/or source of wealth. A customer having a single source of regular income will pose a lesser risk of ML/TF than a customer who has multiple sources of income or irregular income streams.

Product/Service/Transaction Risk

The Company considers customers who use multiple credit cards, e-wallets and prepaid cards to be high risk, both of ML/TF and problem gambling.

Geographical Risk

From a geographical risk perspective, the location or the nationality of the customer, or a country which the customer is associated with for other reasons, is a fundamental consideration. The nationality, residence and place of birth of a customer have to be taken into consideration as these might be indicative of a heightened geographical risk. Certain countries have higher ML/TF risk than others, as well as gambling restrictions.

The company’s risk assessment is applied through the implementation of our customer acceptance policy. The MLRO, Deputy MLRO, and other authorized personnel regularly interrogate the player database for high-risk players then monitor their activity, in conjunction with reporting metrics and KYC measures.

A customer located in a jurisdiction which is not Financial Action Task Force (“FATF”) compliant (named on FATF’s List Black or Grey), will not be accepted by the Company.

4.2. Business Risk Assessment (‘BRA’)

The application of the risk management process in dealing with ML/TF recognizes the existence of risks, undertake a risk assessment, and implement systems and strategies to manage and mitigate the identified risks.

The risk assessment is to be properly documented, approved by the Board of Directors, and be made available to the competent authorities upon demand. The assessment is regularly reviewed and kept up to date.

We revise the BRA whenever there are changes to the environment within which we operate and/or within our business structures/activities, including the introduction of new products or technology, new methods of payment by customers, changes in the customer demographic or any other material changes.

Regardless of such changes, the assessment is reviewed and assessed at least once a year in order to evaluate whether any changes are required. The BRA is a dynamic one and may need to be reviewed earlier if it undergoes any significant changes prior to the scheduled review.

In any review, the MLRO assesses whether there are appropriate policies, procedures and controls in place to prevent ML/TF. Should this prove not to be the case then it will be the duty of senior management to ensure that this is rectified immediately, and new policies, procedures and controls put in place as quickly as possible. The reviews are made with reference to the applicable legal and regulatory requirements.

The documentation from the risk review is circulated to the Senior Management and any action points implemented. These documents are stored in the AML Risk Review file.

4.3. Customer Risk Assessment

Different customers expose the Company to different risks and therefore a customer-specific risk assessment is carried out on each customer to identify potential risks. The assessment allows us to create a risk profile for customers and categorise the ML/TF risk presented by each of them as described in this document. The initial customer-specific risk assessment is revised throughout.

5. GENERAL PRINCIPLES OF THE CAP

The General Principles of the CAP are the following:

- a) the Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client
- b) where the Client is a prospective Client, a registration will be created only after the acceptance of all pre contractual agreements those being:
 - Terms & Conditions
 - Responsible Gaming
 - Self-Exclusion
 - Complaints or Dispute Resolution
 - Essentials of Anti-Money Laundering (AML) Procedures
 - Fairness & RNG Testing Methods
 - Privacy Policy
 - Account, Pay-outs and Bonuses
 - Accounts opened in anonymous or fictitious names(s) are prohibited.
 - Clients who have been convicted for a Predicate Offence (and is yet to serve the sentence), depending on the nature of Predicate Offence, will not be accepted and it at the Company's discretion to close the account even after having served his/her sentence.
 - no account shall be opened if Client is included in Sanction Lists.
 - no account shall be opened if Client is residing in a country where the Company does not provide its services or online gambling is strictly prohibited.
- c) The Company does not accept clients who are legal entities, funds, trusts or fall under any other corporate structure. Only physical persons are accepted and/or allowed to create an account.

In addition to the above, the procedure for the verification of a Client's identity is reinforced if the said Client is introduced by a reliable staff member of the Company, or by another existing reliable Client who is personally known to a member of the Board. Details of such introductions are kept in the Client's file.

Geo-Blocking

As mentioned above in points (f) and (j) players residing in:

- a) countries which are listed in FATF's list 'Jurisdictions under Increased Monitoring' and "High-Risk Jurisdictions subject to a Call for Action"
 - b) EU Commission's list with high-risk third countries
 - c) Countries which are listed in the Terms and Conditions of the Company or;
 - d) In a Country other than those listed in the registration Page of the Company;
- Are not allowed to register or create an account.

In order to minimize such risk, the Company has implemented a geo-blocking system which identifies the location of the applicant based on the IP/VPN.

6. DUE DILLIGENCE GENERAL PRINCIPLES

The main Due Diligence principles:

- All persons conducting business with the Company are properly identified, that their identity is verified where appropriate and sufficient information is gathered and recorded to permit the Company to 'know its client' and predict the expected pattern of business.
 - Potential new business partners that do not appear to be legitimate are declined and where there is suspicion relating to criminal conduct on the part of a declined participant such suspicion is reported to the Money Laundering Reporting Officer (MLRO).
 - Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations.
 - Full co-operation is provided to the law enforcement authorities to the extent required by statute/regulation.
- All suspicions are reported promptly to the MLRO.
That the Company's vigilance systems are implemented and regularly monitored.

The Company shall duly apply Client identification procedures and Client due diligence measures in the following cases:

- Players engage in financial transactions equal to or above EUR 2000,--
- Carrying out occasional transactions above the monetary equivalent of EUR 2000,--
- There is a suspicion of money laundering or terrorist financing; or
- They have doubts the veracity or adequacy of previously obtained customer identification data

A customer would normally register and open an account with the company, but CDD measures would not require application until the said threshold is reached. We are still required to have systems in place allowing us to apply a level of ongoing monitoring, also to ensure that:

- We are able to determine the moment in time when the €2,000 threshold is met;
- The player does not avoid the application of CDD measures by circumventing the €2000 threshold per account, e.g. through the opening of multiple accounts by the

same person, whether under his own name or using the identities of third parties, be they real or fake.

- We are able to identify an account created by a person who has inputted manifestly false details; and
- We are able to detect instances which give rise to a suspicion of ML/TF.

In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the company obtains any necessary information from the customer concerned. However, until such time as the company obtains the necessary information and documentation from the customer to meet its CDD obligations, the customer is not to be allowed to effect any withdrawals from the account independently of the amount involved. Moreover, if following the lapse of 30 days from when the Company has requested from the client to provide the necessary DD information, the customer has not made the requested information and documentation available, the company is to terminate the relationship or suspend the account until compliance of the customer.

Nature and frequency of transactions

Where an individual is making regular deposits and betting transactions there is considered only minimal potential risk of money laundering or terrorist financing, unless they reach the thresholds. Irregular patterns of activity or regular deposits and withdrawals with limited betting transactions may highlight enhanced risk both from an AML/CFT/CFP and social responsibility perspective. Participants managing their payments and withdrawals to remain non-qualifying may also represent enhanced potential risk.

The procedures detailed in the following pages address both the requirement to identify participants and to gather evidence verifying their identity but also to monitor on-going activity to determine a change in the risk profile of the participant.

Several changes to a customer's transactions may prompt an investigation, requiring the customer's identity to be verified and potentially for the customer's source of wealth to be established. Source of wealth checks will establish both the legitimacy of the customer's funds and as to whether they can afford their current levels of spending. Such checks will be conducted on a case-by-case basis.

Multiple accounts are not permitted on the platform. This risk is mitigated by the system automatically preventing registration with matching information. However, there is always the possibility that an individual has used false registration details or details that are not theirs to create several accounts. Multiple accounts can be used to carry out multiple smaller transactions to avoid triggering any due diligence thresholds. Ongoing monitoring practices will be utilized to analyze transactional patterns, similar registration details, matching IP and device data to detect multiple account abuse. In such circumstances these individuals will be automatically banned from the platform unless a reasonable excuse can be provided from the customer.

Source of funds being transacted

The source of the funds will be verified to be coming from a legitimate source with legitimate connections to the customer. Any contradictions to this will result in the customer's account being suspended either indefinitely or until a reasonable explanation be provided.

All withdrawals should be sent to a verified bank account owned by the registered customer.

The Company will accept deposits via electronic payment methods requiring Strong Customer Authentication (3D Secure).

Multiple changes to the source of funds when multiple transactions are being made should also be queried by the Company as this is a potential indicator of money laundering.

Anonymous Accounts

Customers are not allowed to register with fictitious names or anonymous accounts. If during the verification process the Company identifies that the information provided at the registration does not match the identification documents of the client, has right to close the account.

Duplicate accounts will not be allowed, and relevant checks are made during the registration stage (same email, device).

7. DUE DILIGENCE IN PRACTISE

Identification of Customers

For casinos, verification of identity must be conducted when engaging in financial transactions equal to or in excess of EUR 2000.—(equivalent to Ang 3000,--). This implies that all CDD measures must have been conducted at the time the threshold is reached. However, casinos are required to apply a minimum level of CDD measures prior to reaching the threshold. Thus, simultaneously with the opening of an account, casinos are to identify the customer by collecting the minimum personal details such as:

- a) Registered name and surname;
- b) permanent residential address;
- c) date of birth;
- d) gender;
- e) e-mail address.;
- f) Phone Number;

Participants registering on the site are required to input a password of their choosing. No player under the age of 18 can register with the company. If their age is below 18, they are unable to register.

Records will be maintained by the Company's administration of all current, attempted and past registrations.

Upon completion of all required fields and confirmation of agreement to the terms and conditions, an email will be sent to the registered user at the email address provided. Registration will not take place if all fields are not completed. To activate the player will be required to re-log on to the respective domain using the link provided, upon successful input of their password their account will be activated.

No monies can be deposited with the company and no bonuses allocated to the account until the account has been activated.

Customers' Verification

Payments made to participants that exceed EUR 2000 (or currency equivalent) trigger the requirement for evidence to be gathered confirming the registered participant's identity.

CDD measures to be taken are as follows:

- a) Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information
- b) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
- c) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, its source of funds

1. Verification of identity:

The verification of identity may be completed via the verification screening conducted upon first deposit depending on the information gathered. Should the screening report support enough information whereby the customer's name, address and date of birth can be relied on as being accurate then that will be sufficient for this purpose and no further information will be required from the customer. However, consideration must also be applied should there be any other suspicion, for example if you suspect that the customer is underage and is using the details of an adult to register on the platform. In such circumstances further due diligence items should be requested from the customer.

As part of the screening report, PEP, sanction and adverse media checks will also be made.

Documents used for verification purposes are provided electronically through a secure upload function accessible only from customer's registered email and to which customer received a unique url from the 3rd party due diligence screening platform. These documents must be clear, in colour, legible and of good quality.

Risk team are to ensure as much as possible that the documents obtained are authentic or reproduce authentic ones, even though the authenticity of some documents may be easier to assess than that of others. These checks may be carried out either by the company itself or through the 3rd party due diligence screening platform.

Verification requires not only the production of documents but ensuring that the individual providing the document is the one referred to therein. There are circumstances in which the company is able to determine as much on the basis of information in its possession (for example, geo-location information, IP address data, funding method data, etc.) which allow it to corroborate the information contained in the documents provided by the customer.

Biometric checks, also take place via the 3rd party due diligence screening platform to confirm that the individual providing the document is the one described therein.

If the Risk team is unable to satisfy either aspect of verification, they are expected to undertake additional measures. Therefore, apart from obtaining identification documents, it needs to be determined whether additional, or EDD, measures need to be taken.

When requesting due diligence from a player, at a minimum the following information must be collected:

- Full name
- Identification document
- Permanent residential address
- Date of birth
- Place of birth
- Identity number

In order to verify the Client's identity/name the Company shall request a copy of the original document which is issued by an independent and reliable source that carries the Client's photo:

- Passport
- National Identity cards
- Driving License
- Residency Cards

To be acceptable identity documents must be:

- Match the name registered by the Client for the opening of the account;
- The expiration date is not less than 2 weeks;
- A good clear high-quality color scanned copy, plainly legible,
- All 4 corners of the document are visible;
- Bear a photo of the holder, and
- The Document has the issuance authority's Logo;
- Both Sides of the Document are provided (back and front).
- The Document contains the signature of the Client.

2. **Verification of address:** Depends on the risk Level of the client- see Table 1 KYC Matrix. Hard copies for the proof of address will be requested for Medium and High Risk customers.

The Client's permanent address shall be verified upon the discretion of the Company, with the production of utility bill:

- a) local authority tax bill. A recent rate, council tax or utility bill (recent in respect of utility bills is for the last quarter i.e. no more than 6 months old).
- b) A recent account statement (i.e. no more than 6 months old) from a recognized bank, building society or credit card company or the most recent mortgage statement from a recognized lender.
- a. land line bill
- b. insurance letter
- c. certificate or/letter issued by a governmental authority
- d. University letter
- e. Rental Agreement only if executed in the last 6 months and are dully certified by a certifying officer or governmental authority. If the Tenant/ Landlord is a Legal Entity then the agreement shall include their Logo.
- f. An unexpired photographic driving license or national identity card containing current residential address if the document has not been used to verify identity.
- g. Correspondence from an official independent source such as a central or local government department or agency Known lawyer's confirmation of property purchase or legal document recognizing the title to the property.

Requirements for Proof of Address:

- i. Be not older than 6 months old
- ii. Match the address registered by the Client for the opening of the account;
- iii. Colored Copy;
- iv. All 4 corners of the document are visible;
- v. The Document has the issuance authority's Logo;

Company does not accept as Proof of Address:

- i) Mobile telephone bills are not acceptable as evidence of address under any circumstances.
- ii) Receipt from shops
- iii) Pay slips
- iv) Documents provided to verify an address should not refer to P.O. Boxes or care of addresses.
- v) they appear to be under the age of 18 or of a different age than that provided upon registration
- vi) they appear to be linked to criminal activity or terrorist organizations

Enhanced Due Diligence

In certain cases, highlighted by the risk assessment, the Company may consider that a participant poses a higher risk. In these circumstances, enhanced due diligence will be requested and collected by the Company (see **Table 1 KYC Matrix** page 15). Participants who pose an additional risk will be recorded as high risk within the administrative system and a report of their transactions and any other relevant information made available to the MLRO.

Enhanced due diligence will consist of the requirements as established for standard customer due diligence, in addition to the following:

- Requirement of additional identification data (middle names, former names, aliases, occupation, employer, personal identification number, previous addresses)
- Consideration as to whether this data needs to be further verified (additional identity documents, telephone or video call with the customer, 'selfie' with the identity document, certified documents)
- Establish the source of funds
- Establish the source of wealth – Source of Wealth Questionnaire
- Flag the participant for enhanced on-going monitoring
- Open-source checks

A customer that is deemed high risk and has complied with all EDD requirements will be referred to a senior manager or the MLRO for approval before the customer is permitted to continue with any further activity on the platform.

A participant who poses a higher risk may be:

- a PEP
- Resident in a country which the company has reason to believe does not apply or insufficiently applies the FATF recommendations.
- Meets the EDD requirement on the risk matrix due to their level of transactions

- Meets the EDD requirement on the risk matrix due to the number of changes to their payment method.
- Any persons who are the subject of any warnings or notices.

Source of Funds and Wealth

Source of funds is quite simply the method by which the customer has deposited funds onto the platform. This should be easily identified upon the customer depositing, as the system should detect the method being used e.g. debit card or payment wallet.

Should the system not recognize the payment method, is a method unauthorized to be used on the platform, or the payment details do not match with that of the registration, all activity on the account will be suspended and the matter reported to the MLRO.

Source of wealth is how a person has generated the money they are spending on the platform and their financial standing in general. When conducting enhanced due diligence, reasonable measures must be made to establish source of wealth.

As an example, the SoW check is carried out as follows taking into consideration the different risk levels:

- Low risk: background check by the Risk team through open source intelligence social media to assess the customer's play in line with publicly available information relating to, amongst others, occupation and potential wealth.
- Medium risk: Source of Wealth Questionnaire of the customer's economic activity and/or source of wealth, including estimated annual income, and substantiate with background checks by Risk team.
- High risk: Source of Wealth Questionnaire together with any supporting documentation as evidence of declaration submitted.

When reviewing the source of wealth information, the Company staff will need to consider how reliable or independent the source of the information is, how plausible the information is, and how this compares to the customer's activity.

Dealing with sanctioned persons

In case when the Employee during Client on-boarding, COD or EDD procedure, or during Client ongoing monitoring becomes in the possession of the information that the Client is a sanctioned individual or has any links to sanctioned individuals and/or entities, he MUST:

- Immediately freeze all the funds / economic resources of the Client available to the Company;
- Not enter into any financial transactions or provide financial assistance or services to the Client;
- Apply Enhanced Due Diligence measures;
- Immediately inform and file the internal report to the MLRO;
- Suspend the account of the Client until further instructions from the MLRO.

It is prohibited to inform the Client or any third party (except a senior manager or MLRO) in advance, that a freezing measure is to be applied.

The MLRO has to review the internal report as soon as practicable and, in case there are reasonable grounds to suspect that the Client is the sanctioned individual from the lists provided by OFAC, EU, UN or national Sanctions regimes, the MLRO will cease to conduct any further business and a report will be submitted to the FIU.

TABLE 1 - KYC Matrix

The following matrix details the customer due diligence requirements:

Due diligence check	Low	Medium	High
Government Issued ID	✓	✓	✓
Proof of Bank details Ownerships (IBAN Certificate)	✓	✓	✓
Selfie ID / Liveness check	✓	✓	✓
PEP, Sanction and adverse media Screening	✓	✓	✓
Good Standing Questionnaire	✓	✓	✓
Proof of address documents		✓	✓
Source of funds (Bank cards Copies)		✓	✓
Responsible Gaming Questionnaire		✓	✓
Open source checks			✓
Source of Wealth Questionnaire		✓	✓
Source of Wealth documents			✓
Additional identity and address documents		✓	✓

TABLE 2 - Player Risk Matrix

Risk rating	Nature	Location	Source of funds/ Wealth	Transaction size
Prohibited	Legal Entities	Closed jurisdictions	Cash	A customer that has breached any of the below thresholds but does not comply with the Company's CDD/ EDD requirements
	Sanctioned individual or entity	Named on FATF's Blacklist.	A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements	
	A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements	A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/ EDD requirements	Funds appear to be generated or linked to the proceeds of crime	
	Anyone deemed to be linked with the financing of terrorism			
	PEP			
High	Any individual or entities subject to warnings	Countries with AML/CFT/CFP strategic difficulties	Multiple payment methods	Deposit or withdrawal of EUR 50,000 in any period
	Professional gambler		Use of voucher or pre-paid card	

	Customers that are sporting professionals betting on sports High net worth individuals		Where the method of withdrawal differs to that of original deposit	
Medium	Public profile raises some form of concern e.g. adverse media, social media activity	Named on FATF's List B. Countries which in the opinion of the MLRO represents heightened risk	Use of voucher or pre-paid card Where the method of withdrawal differs to that of original deposit Multiple payment methods	Deposit or withdrawal of over EUR 10,000 (or currency equivalent) or aggregate more than EUR 5,000 (or currency equivalent) in any 30-day period
Low	Individual	Fully compliant with FATF No AML/CFT/CFP concerns	Bank transfer Debit or credit card Approved payment service provider	Under any of the qualifying payment thresholds

Following the risk assessment, customers will be identified as either low, medium, high.. The relevant level of customer due diligence will then be applied to each participant's account and reviewed on an on-going basis as part of the monitoring procedure.

The Company will undertake a review of the relevance of its risk assessment as part of the AML/CFT/CFP Compliance Officer's annual report to senior management or as and when significant changes in business operations dictate.

8. ONGOING MONITORING

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

Inability to Complete CDD

In the event that a customer is not willing to provide the necessary information/documentation notwithstanding numerous requests, the company is required to adhere to the following:

- i) To terminate the relationship with the customer. We are not to allow any activity of any kind on the player's account or provide any other service to the customer. We may decide to either close the account or to keep it blocked and suspended in its entirety.
- ii) To consider whether there are any grounds giving rise to suspicion of ML/TF. The reluctance of the customer to provide CDD documentation on its own should not be automatically equated to a suspicion of ML/TF. If there are grounds to suspect ML/TF, then the company has to submit an SAR to the FIU.

- iii) Where there are no grounds to suspect ML/TF or the transaction has not been suspended by the FIU or by operation of the law, nor is there an attachment or freezing order, then we would have no reason justifying the retention of any such funds.

If the customer's funds are to be remitted back, the company should:

- i) Consider whether there is any other legal impediment to the remittance of the funds; and
- ii) Remit the funds to the same source through the same channels used to receive the funds.

If the company is unable to remit the funds to the same source through the same channels, it will inevitably have to request fresh instructions from the customer. In such exceptional circumstances (and as a measure of last resort), the company should remit the funds to a single account held with a credit or financial institution in a reputable jurisdiction in the customer's name. If these instructions give rise to an AML/CFT suspicion, it should submit an SAR and suspend the remittance pending the FIU's feedback expressing their opposition or otherwise to the said transaction.

Whenever we are remitting funds we are also, to the extent possible, to indicate in the script/instructions accompanying the funds that these are being remitted due to our inability to complete CDD.

Importantly, funds should never be remitted to:

- i) Multiple accounts; and/or
- ii) An account held with an institution located in a non-reputable jurisdiction

Ongoing Monitoring of Transactions

All transactions by all customers are recorded and can be reported on a daily, weekly, monthly, or annual basis.

It is recognized that a significant change to the normal operation of an account could be a sign of suspicious activity. A change may be:

- Unusually large deposits based on past deposit history
- Unusual patterns in betting activity
- Large deposits followed by large withdrawals combined with minimal betting transactions
- Multiple changes to deposit and withdrawal methods

If during daily monitoring it is noted that a player's profile has altered in a way that would alter their risk level an immediate review would be undertaken to ensure that all due diligence criteria for the new risk level is met. Should any further documents or information be required the participant will be contacted with a request to provide such within a timely manner.

In this respect, the Risk Department shall be responsible for maintaining as well as developing the on-going monitoring process of the Company.

The Risk Department monitors and ensures, on a frequent basis, that the actual amount of funds deposited by Clients is consistent with the amount of funds indicated during the Client's DD, as well as with the economic profile of the Client.

Additionally, the Risk Department must be alerted to detect and report internally any activity on the Client's account or behaviour, which is inconsistent with the previously disclosed/obtained information. Employees must inform accordingly the MLRO.

Where the activity is deemed to be unusual, an investigation into the customer may begin which may include asking the customer for their rationale for carrying out the activity or further information or evidence of the source of funds or source of wealth.

Ongoing Monitoring of Identity

Changes made to a customer's identity and personal information will be reported on to the Risk Department. ~~The~~ The evidence of identity previously provided by the participant will be reviewed and steps taken to renew and update that information considering the reported changes to the participants identity.

In such circumstances, the verification procedures shall be followed in addition as to the customer providing reasoning for the change in details.

Should a customer's risk level increase (e.g. from low risk to medium risk) and due diligence documents are already held on the customer, consideration must be made whether further documents must be submitted. The previously supplied documents must be reviewed to ensure that they are not expired, in such circumstances up to date documents must be requested.

CDD/EDD held will be reviewed on an annual basis regardless of any changes to the customer's circumstances.

In the event that satisfactory confirmation of the information as to the identity of the participant or satisfactory verification of evidence of identity is not provided, then the account will be suspended, no further betting activity allowed, and consideration be given to the lodging of a suspicious transaction report.

9. RECORD-KEEPING PROCEDURES

Record of Transactions

The Company will maintain appropriate records of all participants and their associated transactions. The MLRO has unfettered access to all records (other than those which are stored in an encrypted or hashed form) and reporting through the back-office computer system. All records and audit trails can be accessed by them and reported in hard copy format without delay and within 7 days of any request being made.

All internal due diligence documents will be held on the back-office system, with the MLRO having full access.

Retention of Records

All the above-named records will be maintained in a secure and accessible form. Secure backups are made daily of the following customer data:

- Records
 - all registration details
 - identification verification details
 - standard and enhanced due diligence items
 - suspended accounts and reason for suspension
 - closed accounts
 - financial transactions – deposits, bets made, withdrawals, prize payments
 - self-exclusion periods (temporary and permanent)
 - self-imposed limits
 - excluded players
 - complaints and responses
 - audit trails
 - bank reconciliations
 - Customer Service electronic correspondence records

Records associated with a customer (including all identification records and the financial transactions made by them) are maintained for a period of 5 years after the date of closure of the customer's account or the date of the last transaction.

Records associated with the register of internal and external disclosures and the register of money laundering and financing of terrorism enquiries will be maintained for a period of 5 years following the finalization of the relationship with the related parties or for the period as advised by the FIU.

The right of access of the data subject to the data concerning him / her may be waived in part or in full according to the provisions of the Personal Data Processing (Protection of Individuals) Law as amended every time:

- a) For the purposes of properly performing the duties of the Company , or
- b) In order not to impede the conduct of official or legal investigations, analyzes or proceedings for the purposes of the Law and to ensure that the prevention, investigation and detection of money laundering and terrorist financing.

The processing of personal data under this law for the purpose of preventing money laundering and terrorist financing is considered to be an issue of public interest in accordance with Directive 95/46 / EC.

The Company incorporates strict rules and specific procedures into the day-to-day operations in order to guarantee its clients and employees the maximum achievable level of security in

handling personal data. All personal data held by the Company is protected under the applicable Data Protection Legislation and the Data Protection Officer is responsible for overseeing the procedures and policies implemented by the Company for the processing of the personal data.

Additionally the Company ensures that the following data subjects' rights, as these are stated under the applicable Data Protection Legislation, are respected:

- a) Request access to personal information which enables the data subject to receive a copy of his personal information that the Company holds about him and to check that the Company lawfully processing it.
- b) Request correction of his personal information which enables the data subject to have any incomplete or inaccurate information corrected.
- c) Request erasure of his personal information which enables the data subject to delete or remove personal information where there is no good reason for the Company continuing to process it.
- d) Object to processing of his personal information where the Company is relying on a legitimate interest (or those of a third party) and there is something about his particular situation which makes him want to object to processing on this ground. The data subject has also the right to object where the Company is processing his personal information for direct marketing purposes.
- e) Request the restriction of processing of his personal information which enables him to ask the Company to suspend the processing of personal information about him.
- f) Request the transfer of his personal information to another party.

10. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS / ACTIVITIES TO THE UNIT

An unusual transaction is a transaction inconsistent with the player's profile. Therefore the 1st key to recognize that a transaction or series of transactions is unusual is to know enough about the player. Suspicions must be reported to the MLRO as soon as reasonably practical.

To make a report form as outlined in **Appendix A** can be used.

Receipt of the report will be acknowledged by the MLRO. It is necessary for the person making the report to include their name. Once an initial report has been submitted the person should continue to submit reports where further suspicious activity takes place, or if there are developments in respect of the matter originally reported.

The following transactions or intended transactions are deemed unusual:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice.
- Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55)

- Transactions in the amount of NAF 5,000 (equivalent EUR 3000, --) or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means.

This includes but not limited to:

- A cashless transaction in the amount of NAF 5,000 or more. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client;
- Accepting or releasing a deposit in the amount of NAF. 5,000 or more at the request of the client;
- Sale to a customer of chips in the amount of NAF. 5,000 or more. "chips" include but is not limited to tokens and credits.
- A cash out in the amount of NAF. 5,000 or more.

Note; A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAF. 5,000 or more and is considered per gaming day. Also credit card transactions and e-wallet transactions are to be reported to the FIU.

The MLRO have full access to information and records of the company that the Directors consider necessary to evaluate internal reports received. They will document the evaluation process and the reasons for conclusions reached.

If after completing the evaluation process the MLRO considers that there is knowledge of, suspicion or reasonable grounds to suspect money laundering or terrorist financing the MLRO is responsible for:

- Submitting the necessary information to the FIU.
- Recording the disclosure in the register of disclosures.
- Dealing with subsequent production or account monitoring orders if there are any.

Tipping Off/Confidentiality

Any person must treat any information where that person knows or suspects that an unusual transaction report has been made or that an investigation is under way or proposed or strictly confidential.

No staff member may disclose to any person s/he has formed a suspicious that a person may be involved in suspicion that a person may be involved in suspicious matters or transactions or that a report has been lodged about that person with the FIU or any other authority.

Clear lines of reporting where matter or transactions are referred to the MLRO need to be maintained. All matters or transactions are to remain confidential between the reporting staff member and the MLRO.

It is an offense to disclose that an unusual transaction report or related information on a specific transaction has been reported to the FIU or that an investigation into money laundering, terrorist financing or the proceeds of crime is impending/pending, and to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

Confidentiality of report

The Company, a structural unit of the obliged legal entity, a member of a management body and an

employee is prohibited to inform a person, its beneficial owner, representative or third party about a report submitted on them to the Financial Intelligence Unit, a plan to submit such a report or the occurrence of reporting as well as about a compliance notice issued by the Financial Intelligence Unit or about the commencement of criminal proceedings. After the compliance notice issued by the Financial Intelligence Unit has been complied with, the obliged entity may inform a person that the Financial Intelligence Unit has restricted the use of the person's account or that another restriction has been imposed.

Discharge of liability

The Company, its employee, representative and the person who acted on its behalf is not liable for damage caused to a person or customer participating in a transaction made in economic or professional activities, in performing an official operation or in the provision of an official service:

- upon performance of duties and obligations arising from the AML Act in good faith, from failing to make the
- transaction or from failing to make the transaction within the prescribed time limit;
- in connection with the performance of the duty to report a suspicious transaction, in good faith;
- The performance of the duty to report a suspicious transaction and submission of information by the
- The Company is not deemed breach of the confidentiality requirement arising from law or contract and the statutory or contractual liability for the disclosure of the information is not applied to the person who performed the duty to report. An agreement derogating from this provision is void.

After the submission of a suspicious report the Company may subsequently wish to terminate its relationship with the Client concerned for risk avoidance reasons. In such an event, the Company exercises particular caution, not to alert the Client concerned or other third persons that a suspicious report will be or has been submitted to the Unit, concerning ML or TF. Moreover, it is not allowed for any person to make any disclosure which may cause obstruction or negatively interfere with interrogations and investigations carried out while it knows or suspects that such interrogations and investigations are under way. Close liaison with the Unit is, therefore, maintained in an effort to avoid any frustration to the investigations conducted.

Furthermore, after the submission of a suspicious report the Clients' accounts concerned as well as any other connected accounts are placed under the close monitoring of the MLRO.

Protection of Persons Reporting

Bona fide disclosure of information by the Company or by an employee or director of the Company does not constitute a breach of any contractual or statutory, regulatory or administrative prohibition of disclosure of information, nor implies any liability for the Company or its directors or employees, even if the circumstances did not allow them to know precisely what the main illegal activity was and regardless of whether it was actually committed Illegal activity.

Persons who submit an internal report or report to the Unit for suspicious transactions shall be protected against any threat or hostile action and in particular by adverse acts or discrimination in the workplace.

Disclosure in Good Faith

Disclosure of information in good faith by the Company or by an employee or director of the Company, shall not constitute a breach of any contractual or legal, regulatory or administrative restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the Company or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether the illegal activity actually occurred.

11. ANTI MONEY LAUNDERING COMPLIANCE PROGRAM

An anti-money laundering program is an essential component of a casino's compliance regime. The primary goal of every good program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

The basic elements a casino must address is an anti-money laundering compliance program are:

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

Money Laundering Reporting Officer and Money Laundering Compliance Officer

The Company shall always have an appointed MLRO and MLCO. The appointed of both roles will be sufficiently senior within the company and will have the right of direct access to the Directors of the Company and is independent from the games operations.

The MLRO and MLCO will have unfettered access to all reports, transaction histories, complaints and audit trails.

11.1. Staff education, training, and development

Importance for AML/CFT/CFP risks

The way the company is organized can increase or mitigate the exposure of the company to money laundering and terrorist financing risks. Procedures and controls operated by the company, many of which are required by law, can be applied to manage AML/CFT/CFP risk.

The Importance of Staff in ML prevention

Success in preventing money laundering and terrorist financing cannot be achieved by having appropriate policies alone. Even the best policies are useless if staff ignore or circumvent them, whether through ignorance, carelessness or deliberately. Staff are a business's strongest defense or their weakest link.

Staff Knowledge, Training and Awareness

Recruiting staff of integrity is not sufficient in of itself. Staff must have sufficient awareness and training to detect money laundering and terrorist financing and to understand what is expected of them.

It is key to effective AML/CFT/CFP arrangements that:

- Staff have sufficient knowledge or awareness to detect money laundering.
- Staff have sufficient training to know how to deal with cases once they know of or suspect money laundering.
- Staff are aware of their personal legal obligations.

All members of management and staff will receive initial training and on-going training at least on an annual basis or as and when required.

Refreshment trainings will be arranged and to demonstrate compliance with the staff training requirements records will be maintained that include:

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

Integrity

The integrity of the directors and employees of the Company are the foundation of its AML/CFT/CFP measures. If staff lack integrity there is a danger that they may become involved in or become willing accomplices to laundering activity.

Direct involvement in laundering operations is the possible extreme. More likely is that staff without the right attitude are unlikely to:

- Maintain awareness and detect money laundering.
- Report money laundering if they become aware of it.
- Take seriously their own training or that of their subordinates.
- Encourage reporting and foster a culture that supports money laundering prevention.

Technological Developments

The Company recognizes the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism. As a consequence:

- The Directors retain a close eye on technological developments that are taking place particularly in relation to phishing activity, identity fraud, money laundering etc.
- In addition, the company has engaged with technology partners who are at the forefront of software and IT security and are engaged to maintain the on-going integrity of the website, servers and backup.
- The Company is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solutions.

12. TARGETED FINANCIAL SANCTIONS

Sanctions are restrictions used by international communities as part of an attempt to stop financial crime and terrorism. They are designed as attempts to change the behavior of a targeted country, regime or individuals where diplomatic efforts have failed. Sanctions can take form of economic, trade, financial services, or international movement (travel bans) prohibitions. Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities.

UN Sanctions

The United Nations Security Council publishes the names of individuals and organizations subject to UN financial sanctions in relation to involvement with ISIL (Da'esh), I-Qaeda, and the Taliban. All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities. The UN has in place other sanction lists pertaining to other jurisdictions, entities, and individuals, including wider terrorist activity under UNSR 1373.

The UN consolidated sanctions list is available at the following link:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

EU Sanctions

The European Union applies sanctions or restrictive measures in pursuit of the specific Common Foreign and Security Policy (CFSP) objectives set out in the Treaty of the European Union. Restrictive measures imposed may incorporate UN Security Council sanctions or EU autonomous sanctions. The latter cannot be imposed against individuals or entities where there is no foreign policy dimension.

Link to the EU sanctions regimes: <https://www.sanctionsmap.eu/#/main>

The above-mentioned website also includes information about the UN sanctions regimes.

OFAC Sanctions

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on the US foreign policy and national security goals against targeted foreign countries and regimes; terrorists; international narcotics traffickers; and those engaged in activities related to the proliferation of weapons of mass destruction; and other threats to national security, foreign policy or the economy of the US. It is important to note that while US sanctions do not directly apply to non-US companies outside the US, the use of the US dollar currency automatically engages OFAC regulations. US prosecutors take the view that if a financial transaction has cleared in the US (as do all US dollar payments, in New York), the US has jurisdiction over the offence. OFAC publishes a list of 'specially designated nationals' or SDNs (known as the SDN List) whose assets are blocked and firms, including US persons, are generally prohibited from doing business with them. The OFAC Sanctions List Search is available at the following link:

<https://sanctionsssearch.ofac.treas.gov/>

13. PROCEEDINGS

Offences

Any person who contravenes the NOIS / NORUT rules in regard to the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT/CFP) will be reported to The Financial Intelligence Unit of Curaçao.

In determining whether a person has complied with any of the requirements of any part of NOIS / NORUT a court may take account of any relevant supervisory or regulatory guidance which applies to that person and which is given by the Gaming Control Board.

Version Control

Document Name	AML/CFT/CFP Manual
Version	3.0
Author	MLRO
Updated By	MLRO
Authorized By	Board of Directors
Distribution Date	22/05/2025

Appendix A | Suspicious Activity Report

Report prepared by:	
Business partners	
Name	
Account ID	
Address	
Email address	
Telephone number	
Is identification and address verification held?	
Is enhanced due diligence held?	

Reason for suspicion	
To include: Identification verification Criminal conduct known or suspected	
Date of report	

Receipt of report acknowledged	
Signed MLRO	
Date	

Approval / Rejections				
Director	Signed		Date	
MLRO	Signed		Date	
Development Review				
Responsible Person Review of Development	Date			
	<i>Review to comment on whether the development has been implemented in accordance with the outlined previously on this Form and whether a further risk assessment should be conducted</i>			
Approved	Director 1 Signed		Date	
	Director 2 Signed		Date	

Approved and Signed by:

Signed by:



E9C1A4A3F74E4ED...

Signed by:



8737E2B30CF043F...

By Lorenza Godett and Analissa Heiland
Directors of Xecutive Corporate Management B.V.
May 22,2025