

Raging Rhino N.V.

AML/CTF Policy

Version 3.0

Document Status

Version Number	V.3.0
Status	Active
Authorization and approved by	MLRO
Next review not after	01.02.2026
Owner	Raging Rhino N.V.
Number of pages	19
Change History	August 2019 – v1.0 August 2021 – v.2.0 19 th December 2022 – v2.1 23 rd January 2023 – v2.2 15 th June 2023 - v2.3 19 th January 2024 – v2.4 3 ^h February 2025 – v3.0

Version Control

Effective date	Version	Comments
August 2019	1.0	Full policy creation
August 2021	2.0	Full change in all the document content and structure
December 2022	2.1	Additions to the CDD procedure
January 2023	2.2	Additions to Geographical risks and addition of Third Party Due Diligence subchapter
June 2023	2.3	Removal of Appendix D to be replaced with a separate list referenced in the policy.
January 2024	2.4	Adding information on International Sanctions, on on-going monitoring and on obligations of the employees
February 2025	3.0	Full policy revision. New regulatory requirements (published in January 2025) have been added into the policy -and implemented by the company-. In concrete: - Section 5.5: Lines of defence - Section 6.2: personal information gathered during the identification and verification thresholds - Section 6.4: acceptable documents - Section 6.6: New risk scoring in place and removal of Appendix C

Scope

This document provides controls which Raging Rhino N.V. ("RR" or, the "Company") has in place to mitigate the risks posed in relation to money laundering or the financing of terrorism under the Curaçao regulations.

Responsibility and Authority

Ultimate responsibility for the implementation of this policy rests with the Directors of the Company, who have appointed the Compliance Officer ("the Officer") to be responsible for the production and maintenance of the AML/CTF Policy.

Control and Distribution

This is as a controlled document and can only be updated by the Compliance Officer or by an authorized information management representative. It must include a revision status and traceability of the change process.

Contents

1. Introduction.....	5
2. Key Concepts.....	5
3. Applicability, Regulatory framework and Authority.....	6
4. Policy Review.....	6
5. AML/CTF Risks.....	7
5.1 Customer risks.....	7
5.2 Geographical risks.....	8
5.3 Product risks.....	8
5.4 Transactional risks.....	8
5.5 Operational risks.....	9
5.6 Third-party and Intermediaries risks.....	9
6. Customer Acceptance Policy (CAP).....	9
6.1 International Sanctions.....	10
6.2 Customer Due Diligence (CDD).....	10
6.3 Third Party Due Diligence.....	11
6.4 Acceptable documents.....	11
6.5 Enhanced Due Diligence (EDD).....	11
6.6 Ongoing monitoring.....	13
7. Reporting of suspicious activity.....	13
7.1 Obligations of the employees – Internal Reporting.....	14
7.2 Tipping off and failure to disclose.....	14
7.3 Obligations of the Officer.....	14
8. Governance.....	15
8.1 Training.....	15
8.2 Employee screening.....	15
8.3 Management.....	15
9. Record keeping.....	16
10. Appendices.....	18
10.1 Appendix A - Specific legislative framework.....	18
10.1.1 Curaçao.....	18
10.2 Appendix B - Internal Suspicious Activity Report (ISAR).....	19

1. Introduction

RR and its company group are committed to the industry goal of keeping crime, and the proceeds of crime out of gambling. Maintaining a safe environment for our customers and our staff is a core pillar of our business.

This document sets out the strategy of the Company to comply with all the applicable anti money laundering and counter terrorism financing (“AML/CTF”) regulation, requirements, and best practices, in general within the AML standards and specifically meeting Curaçao statutory and regulatory obligations.

The Policy functions in combination with the AML/CTF Business risk assessment (“BRA”) and any procedures set out in relation to this, to ensure appropriate measures are in place to mitigate the risks the business faces in relation to money laundering and terrorism financing (“ML/TF”).

Positive management action will be exercised in order to minimize the risk of the RR services and gaming activities being abused for the purposes of laundering funds associated with criminal activity, as defined by the relevant legislation. RR shall not continue established relationships with participants whose conduct gives rise to suspicion of involvement with illegal activities. The Company shall 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 Financial Unit of Curaçao (FIU).

The Policy has been approved to ensure a company culture of clear intent, realistic evaluation and actionable processes, in order to carry out the mentioned company goal of fighting ML/TF. Mainly, the current Policy is maintained to ensure:

- All persons conducting business with RR 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 participants 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 key functionality holder.
- Established participants activities are regularly monitored to ensure that they fit the customer’s profile, especially in respect of large or abnormal transactions;
- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations;
- All suspicions are reported promptly to the Officer;
- Full cooperation is provided to the law enforcement authorities to the extent; required by statute/regulation; and
- That vigilance systems are implemented and regularly monitored.

2. Key Concepts

Money laundering is the processing of criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source. Although money laundering is a diverse and often complex process, it generally involves three stages: placement (inserting the proceeds of crime into the financial system), layering (separating the proceeds of crime from the source and true ownership), and/or integration (introducing the funds with an appearance of being legitimate into the economy).

Terrorist financing involves the solicitation, collection, or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources.

3. Applicability, Regulatory framework and Authority

The AML/CTF Policy applies to the Company, and it will be communicated to all the employees of the licensed entity, as well as the subsidiaries, parent and sister companies within the group to which RR outsources some of its operations to ensure they are aware of their responsibilities under the current AML/CTF regulation and the policies set out by the company, for each version update the Policy will be communicated to the staff as soon as possible.

Ultimate responsibility for the implementation of this policy rests with the Directors and Board Members of the Company. The Board commits to provide the Officer appropriate resources to fulfil the function effectively, full access to necessary resources to keep up to date with ML/TF requirements and developments as well as complete autonomy in his role. On the other hand, the Officer commits to be responsible for the following, to ensure that the Company complies with all the AML/CTF obligations:

- ☐ 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 and terrorist financing prevention
- ☐ 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
- ☐ Receiving internal disclosures
- ☐ Deciding whether these should be reported to the FIU
- ☐ If appropriate, making such external reports
- ☐ Ensuring that appropriate consent is applied as necessary
- ☐ Demonstrating support for compliance with all the policies and procedures with sound corporate ethics

4. Policy Review

The Officer is the unique and ultimate responsible for designing, monitoring, and updating all the AML/CTF controls, including this Policy. He also holds the responsibility of approving it, besides the Board of Directors. However, and in addition to this, the Policy will be reviewed and approved by the board on an annual basis at minimum, or in case significant changes are done at a level which warrants a Directors / Board approval. The Officer will review the AML/CTF Policy whenever circumstances change to warrant a review and update of the document as set out by the following criteria:

- ☐ upon the discovery or recognition by an audit or risk assessment that the Policy requires amendment.

- upon the change of any relevant law or regulation which applies to the Policy;
- upon the finding by any regulator that an amendment to the Policy is required;
- upon the acceptance of customers from a jurisdiction / territory where company did not previously accept customers;
- upon acquiring a new product / vertical;
- whenever significant changes occur in the business, that will have a direct or indirect impact on the area this document concerns.

Any amendment of the Policy shall, as soon as is reasonably practicable, be distributed or informed to all persons within the scope of the Policy for information of the amendment. The Policy approver is responsible for making sure that the Policy is reviewed and updated on a regular basis.

5. AML/CTF Risks

RR ensures to carry out and maintains an up-to-date control on the AML/CTF risks of the business, assessing these risks in the business and in the industry in order to implement an effective and proportionate policies and procedures.

This risk control cover, at minimum:

- Customer Risks: the general characteristics of the customer.
- Geographical Risks: the characteristics of the country of residence of the customer, alongside other geographical risks.
- Product Risks: the characteristics of the products and services provided by business.
- Transactional Risks: characteristics of the risks linked to specific transactional activities.
- Operational Risks: risks linked staff and the practical implementation of the AML/CTF processes
- Third-party and Intermediaries Risks: the characteristics of intermediaries and interface risks.

These risks are continuously analyzed for potential threats and vulnerabilities of the business from perceived risks in the business and the likelihood that they can be exploited for criminal intent. Following this, the likelihood of such risks arising will be analyzed, and the impact this will have on the business should this risk factor materialize.

5.1 Customer risks

RR recognized that risks related to the customer are the highest where it is possible to gamble anonymously, and the company does not allow for this. The remote set up of a gambling operation also carries risk due to the lack of physical meetings with the customer. Every player is required to register and identify themselves with RR, providing name, date of birth, address, and contact details. Further details of the KYC process are set out in section 6. A registered account is only allowed to be operated by the registered individual, and we do not allow for third party use of an account or Business

Participants. A customer is only allowed to hold one account with the Company, and an email can only be used once to register. The system is regularly scanned for links between accounts in the registered details. RR is not willing to engage or maintain any business relationship with Politically Exposed Persons (“PEPs”), or sanctioned individuals and they are not allowed as customers. All customers are screened on registration and at intervals using reputable third-party software, and if a match should be found the account will be blocked with immediate effect, to ensure the company does not transact with any sanctioned individuals. Sanctions checks are also conducted using third party software and form part of the risk assessment of the applicant. Any match detected during these scans, where there is a high likelihood of being a true match, will be evaluated by the Officer in order to consider whether there is reasonable ground to submit a Suspicious Activity / Transaction report to the relevant FIU.

5.2 Geographical risks

Customers from countries that pose high ML/TF risks which lie outside of the business risk appetite will be blocked from registration and login. The Officer reviews the list of accepted countries on a regular basis, in line with official, certified, and credible sources of information regarding level of ML/TF risks, corruption, political unrest and other risk elements relevant to mitigating geographical risks. When applying simplified measures for customer knowledge and requesting identity documentation in order to verify the customer, we will also look to obtain the nationality and country of birth of the individual in order to support the customer risk assessment. The Company does not allow any customer, whether resident or visitor, to utilize any of the Company’s products or services other than those customers who are resident in countries allowed by the concrete license. To be allowed access and use of our sites players must have an unpolluted IP address originating from their respective country. The verifying of player locations and VPN detection is not only occurring on visit but also on login and on accessing a game to ensure that only eligible traffic are allowed to use our services. The IP Geolocation service is provided by Maxmind Inc. and is implemented in the web application firewall together with the VPN and Open Proxy Detection provided by Cloudflare Inc. To restrict access from US or other black-listed countries (see separate blacklist of EU and FATF high-risk jurisdictions), as well as for malicious traffic, we have partnered with Cloudflare Inc. to implement a web application firewall as the first point of contact accessing the sites. Multiple levels of security measurements including bot detection, IP reputation scoring and headless browsing are monitored in real-time.

5.3 Product risks

The main games offered by RR are RTP based automated online slot machines (“slots”) and live casino. RR contracts with reputable, licensed, or certified game providers, to ensure the correctness of the game mechanics. All transactions are monitored to detect players that exhibit patterns which differ from the general standard.

5.4 Transactional risks

RR does not allow for cash payments and does not provide credit to our customers. RR does not allow for P2P transfers between accounts. Based on known indicators of potential ML, RR has various tools in place to detect activity that corresponds to potentially suspicious behavior and analyze the accounts and the transactions therein. Some of the greatest ML/TF risks are connected to the deposits made into and going from the customer account. The Company therefore employs a closed loop policy, where a payment can only be made to the same method used to deposit. Where a payment method does not allow for a closed loop, we may allow for a withdrawal to another method provided the scenario poses low risk, where we have sufficiently verified both the customer and the ownership of the payment methods used. An attempt to withdraw the same amount, which was deposited, can be a sign of layering. No customer can deposit and withdraw without wagering the deposit amount one time.

5.5 Operational risks

RR employs a combination of automated solutions, and operational procedures in order to create a robust safety net to mitigate the risks connected to ML/TF. The implementation of certain processes and procedures in place to combat ML/TF and keep crime out of the business, relies on human effort, and the knowledge and assertiveness of our staff. As per section 8.1 of this Policy, all operational staff are trained in AML/CTF, and the internal procedures put in place in order to identify, prevent and mitigate ML/TF risks in the business, including KYC measures. Within operations, RR has implemented a model consisting of “three lines of defense”, where each function is specialized in an area of customer knowledge measures, with a clear escalation line to Officer.

Line of defense	Definition
1 st LoD	Responsible for identifying potential AML indicators and to escalate to the MLRO. This LoD is composed of the AML risk score and automatic AML alerts (set up for detecting ML/TF patterns). Composed by Customer Support, Fraud and Payment agents, it is responsible for reviewing in-depth all the alerts and /or red flags and to escalate them to the MLRO for a technical review and for a potential SAR/STR submission.
2 nd LoD	Composed by the MLRO, is responsible for ensuring all policies and procedures are being followed and properly implemented by each of the Lines of Defence and, in case it applies, to report to the applicable FIU.
3 rd LoD	Composed by the independent AML audit and the FIAU. It provides assurance that the firm is adequately addressing the ML/TF risks and compliant with the regulatory requirements. Independent AML Audit helps identify gaps and improvement areas and take corrective actions.

5.6 Third-party and Intermediaries risks

RR sets out to only contract with credible business partners and employs a risk-based approach in order to evaluate the risk each new business relationship may carry. When onboarding a new client, a risk assessment will be conducted to measure the risk in the relationship and an appropriate level of due diligence will then be carried out based on this risk assessment. The Companies execute a due diligence form and request supporting documents from the potential business partner.

6. Customer Acceptance Policy (CAP)

The RR customer acceptance policy is based on what is required under law and in line with the Company risk appetite and the risk assessment of the business. Certain types of individuals will not be accepted as customers, by either being prevented from registering or blocked from using our site:

- ☐ Under 18s;
- ☐ Individuals on EU or UN sanctions lists.
- ☐ Individuals’ resident, or located, in high-risk countries, based on known trusted sources to measure AML/CTF risk.

- Individuals where we have reason to suspect involvement in ML/TF or other types of criminal activity.
- Self-excluded customers, excluded from our site or any national self-exclusion register available within the license conditions.
- Individuals who have submitted documentation or information which we have reasonable grounds to suspect is fake or fraudulent.
- Persons who attempt to fund their gambling with deposits from business accounts.
- Customers were at an increased risk level in the customer profile for any reason; warranted the company terminating the customer relationship. The risk level will be decided by a combination of automated monitoring matrices and manual account reviews.

Active customers are monitored, in terms of behaviors and transactions, and should the risk level in the account increase we may apply enhanced measures for due diligence or terminate the customer relationship. The expected nature of the customer relationship is that of entertainment. Based on this expectation information is collected, and the profile of a player assessed, in order to identify deviations from the expected customer profile.

6.1 International Sanctions

As a remote casino operation, RR is not willing to maintain any business relational with sanctioned individuals. Therefore, and as a general and mandatory principle, any account getting a confirmed positive result by our control system will be closed and the account funds will be seized. As stated in this policy, this result will trigger an escalation to the MLRO and a report to the applicable law enforcement authority. The Company is well aware of its obligations under the international sanctions laws and all the employees are somehow involved in detecting and preventing any activity coming from an international sanction individual or institution.

6.2 Customer Due Diligence (CDD)

Customer due diligence is carried out as required by our regulatory obligations and in order to sufficiently verify our customers, to be satisfied that the customers are who they say they are; to determine whether customers are acting on behalf of others; and in order to guard the Company against being used for fraud, money laundering or other criminal activity.

For identification, RR requests -at registration- the player's full name, permanent residential address, and date of birth. In cases where the player's risk is higher than low, place of birth, nationality and identity number will also be requested. Player's verification takes place upon the player's first withdrawal or when engaging in financial transactions equal to or in excess of NAF. 4,000. All the documents are requested by the Payments team and verified and approved by the Customer Support team.

Measures to electronically verify the credibility of the registered details are put in place via third party providers on registration. The registration step also includes screenings for flags which could indicate fraudulent activity. Variations between implementations specific to a jurisdiction will be detailed in processes, procedures, and jurisdiction specific Appendices. If the customer fails to provide the requested documentation at a stage where this is required, the account will be closed, and a suspicious activity report will be filed if the risk in the customer relationship calls for this; if there is reasonable ground to suspect ML/TF activity. Further procedures developing CDD measures are in place.

In carrying out the CDD measures, customers are allowed to continue using their gaming account while the Company obtains any necessary information from the customer concerned. However, if the Naf. 4,000 threshold is reached because of a deposit of the player, they cannot further deposit funds into the account or withdraw funds from the account. They still are able to play, using the funds already in his account. However, if the Naf. 4,000 threshold is reached because the customer wants to withdraw their money, a complete freezing of the account should occur. Besides that, if the requested information and documentation is not received within 30 days from the moment the Naf. 4,000 threshold is reached, the casino will terminate the relationship with the player and report the transaction to the FIU if a presumption of money laundering or terrorist financing exists.

6.3 Third Party Due Diligence

In order to meet the regulatory and the industry standards, RR has established a process to scan any third party (game providers, PSPs...) the company has signed or engaged a business relation with. All the scans will be performed prior to entering the business relationship and will be conditioned on the final risk scoring.

For Low-Risk companies, no further checks will be needed, and the company will be re-assessed in 5 years. For Medium Risk companies, there will be a continuous monitoring and the company will be re-assessed in 3 years. For High Risk companies, RR will request concrete documentation -intended to mitigate the risk- (UBOs passport, org.chart...) and will evaluate adequacy of the due diligence performed. For High-Risk scenarios, the company will be re-assessed in one year. The screening and assessing process is carried out via ComplianceCatalyst, a solution supplied by Bureau Van Dijk.

6.4 Acceptable documents

The following methods / documents are accepted as a means of verification of identity if the document contains photographic evidence of the player, is valid and not expired:

- ☐ Passport
- ☐ Driving license
- ☐ National Identification card (photographic)

Where the identity does not allow verification of the player's residential address, the casino will obtain other documents (never older than 6 months):

- ☐ Recent Utility bill (gas, electric, satellite TV, landline phone bill)
- ☐ Government letter
- ☐ Local authority council tax bill

RR reviews existing records and regularly refreshes the documentation obtained for the purpose of applying CDD measures.

6.5 Enhanced Due Diligence (EDD)

Measures of enhanced customer due diligence goes beyond that of the CDD. Enhanced measures are warranted especially in cases identified as high risk:

- ☐ When a customer or potential customer is a PEP, or a family member or known close associate of a PEP;

- Where the customer is the citizen of a high-risk third country;
- Where a transaction is complex and unusually large, or there is an unusual pattern of transactions;
- Where the customer is situated in a high-risk third country;
- When the risk profile of the customer is high, and any other case which, by its nature; can present a higher risk of money laundering or terrorist financing;

The EDD measures that RR applies in case there is a higher risk of money laundering or terrorist financing includes:

- Examining the background of the transaction;
- Increasing the degree and nature of the monitoring of the business relationship, in which the transaction is made, to determine whether that transaction or that relationship appear to be suspicious;
- Taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the customer relationship, including greater scrutiny of transactions; seeking additional independent, reliable sources to verify information provided by the customer;
- Taking additional measures to better understand the background, ownership and financial situation of the customer, and other parties to the transaction, i.e.: payslips, savings,

inheritance, bank statements, etc.

Enhanced measures may range between utilizing information available in open sources to obtaining documentation from the customer to establish and verify Source of Wealth (SOW) / Source of Funds (SOF). Suspicious activity will be investigated and reported to the FIU, and a decision reviewed and made by the Officer regarding terminating the customer relationship.

6.6 Ongoing monitoring

RR conducts ongoing monitoring of the business relationship, including:

- scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the knowledge of the customer and the customer's risk profile;
- undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying customer due diligence measures up to date.

Customer due diligence measures must also be adopted at other appropriate times to existing customers on a risk-based approach when becoming aware that the circumstances of an existing customer relevant to the risk profile for that customer have changed, such as:

- a change of identity of the customer;
- transactions which are not reasonably consistent with RR knowledge of the customer.

Risk assessments of all customers are carried out on an ongoing basis, where the level of customer due diligence will vary depending on the risk profile of the customer. RR uses both automated data reporting and manual reviews to carry out risk assessments of all customers on a risk-based approach. The Company has implemented an automated risk scoring solution, which evaluates all player activity based on multiple risk flags which could indicate ML/TF activity and assigns a risk score to the customer account where customers with a higher score are subject to EDD and manual AML reviews. The model is based on a in-house tailored risk scoring that takes into account the transactional and the gambling activity, as well as the ratio between deposits and withdrawals. In concrete, the scoring follows three concrete metrics (average trend of expenditure, average bet per session and ratio between withdrawals and deposits). The outcome of this risk scoring results in three possible customer risks: High Risk, Medium Risk, Low Risk.

RR implements manual controls based on the risk level in the account where dedicated staff will review the account and activity therein to evaluate if there is reasonable ground for suspicion or if the activity can be explained with further investigation and measures. Higher risk customers will also be added to a monitoring list, where dedicated staff will continuously follow up on such customers. If the risk profile of a customer increases beyond the company's risk appetite, and suspicious activity is detected, a report to the FIU will be made by the Officer and the customer relationship terminated. Low and Medium risk players will be continuously monitored in order to be able to find any change in their known patterns that could increase their risk. That monitoring includes a continuous review on transactional and gambling patterns, as well as the concrete characteristics of the player account.

7. Reporting of suspicious activity

As mentioned before, RR will permanently monitor ongoing business relationships and examine individual transactions to detect activities or transactions that are suspicious or inconsistent with what is known about the customer. Any suspicions will be reported immediately to the relevant Financial Intelligence Unit (FIU).

7.1 Obligations of the employees – Internal Reporting

All RR employees, following the given training, will report to the Officer any suspicions found during the functions inherent in their position within each operational department. As stated above, this is set up by RR as the second line of defense (e.g.: manual alerts raised by Customer Support agents...).

Any suspicions found must be reported to the Officer as soon as reasonably practical using the attached form, as per Appendix B. This form will always be available on request from the Officer and will be in an accessible folder for all the employees. The form is the unique and mandatory channel to internally report suspicions and cannot be substituted by any other means as it properly documents the report itself and ensures that all relevant information is included. All communications must remain confidential -regardless of its nature- and it's the employee responsibility to maintain and guarantee that confidentiality.

The receipt of the report will be always acknowledged by the Officer. It is not necessary for the person making the report to include their name on it. However, if an acknowledgement is required the person making the report will need to identify themselves to the Officer in some other way, such as by providing a covering memo. 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. All the reports should be sent to mlro@lucky7.ventures.

Regarding the protection of the employees, RR may not discharge, demote, suspend, threaten, or harass, directly or indirectly, or in any other manner discriminate against an individual based on his or her whistleblowing or reporting. In that regard, the Officer will continuously work to guarantee that protection to all the employees, regardless of the nature of the position held by the individual.

7.2 Tipping off and failure to disclose

Tipping off is a criminal offence. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, any employee of RR suspects that any transaction or behavior is related to money laundering or terrorist financing, the Company prohibits disclosure of this information or of the fact that a report is being escalated to the FIU. A risk exists that customers could be unintentionally tipped off when the company is seeking to perform its obligations in these circumstances. The customer's awareness of a possible report or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

Failing to report knowledge, suspicion or when there are grounds to suspect money laundering to the Officer as soon as reasonably practicable after the information came to your attention, is a criminal offence. Employees have an obligation to be vigilant and raise any such activity directly to the Officer. Through training and by fostering a culture of accountability in ongoing day to day tasks, employees are kept aware of their obligations to raise any suspicious activity to the Officer directly. Employees who do not make an internal report to the Officer when knowledge or reasonable suspicion exists, may face criminal sanctions which may include a prison term of up to five years.

7.3 Obligations of the Officer

The Officer shall consider any internal report (or any suspicion found in his reviews) and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that a customer is engaged in money laundering or terrorist financing. If so, the Officer shall submit a report to the Financial Unit of Curaçao (FIU). In any case, when a report is escalated, RR will aim at ending the business relationship with the concerned customer. However, when reporting, the Company will always follow the FIU instructions and advice before taking any action on the business relationship and will respect the given investigation timing of the authorities.

8. Governance

In order to properly target all the potential ML/TF risks, RR understands the importance of having a strong compliance culture. Therefore, it is the Company objective to make sure the risk knowledge and support is offered to all the staff.

8.1 Training

All staff, including management are made aware of the company obligations under anti-money laundering and counter terrorist financing regulation, and the risks the company faces in relation to this. Training is carried out and adapted to the role and the responsibility of the staff, and a log maintained of the training carried out.

As mentioned, all staff will receive AML/CFT training, to include

- The provisions of the AML/CFT code and the appropriate internal procedures and policies including registration and identification procedures, record keeping etc.
- Their personal obligations under the AML/CFT Code and associated personal liabilities for non-compliance
- The internal reporting procedures detailed in the AML/CFT Manual

AML/CFT refresher training will be delivered at least annually for all staff and the Officer will provide other ad hoc information about news and developments as well as periodic reminders of the need to report certain matters This will be targeted as appropriate.

8.2 Employee screening

RR will only contract and hire individuals of good standing. When hiring new staff, RR makes sure to collect an appropriate level of due diligence to verify the age and identity of a new employee and to allow for background checks. For key positions in the company, responsible for crucial areas within the business, more extensive measures for due diligence are carried out. The following documentation will be collected from all employees;

- Copy of ID;
- Information on employment history and references;
- A police conduct will also be collected to ensure key personnel do not have a criminal record.

8.3 Management

Management commits itself to ensuring that a positive cultural attitude toward AML/CTF prevails in the organization. This will be driven by encouragement of various initiatives, including setting the tone from the top, by supporting and enabling the continuous operational efforts to combat ML/TF, including sufficient resourcing and appropriate training. This includes not only hiring staff but hiring the most appropriate staff.

9. Record keeping

RR maintains appropriate records of all players and their associated transactions. The Directors and specially the Officer have 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 Gaming Innovation Group ("GiG"). 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.

Among all the records for AML / CTF purposes retained for period of 5 years, RR includes:

- copies of any documents and information obtained to satisfy the customer due diligence requirements, and enough supporting records in respect of each transaction which is subject to customer due diligence measures or ongoing monitoring to enable the transaction to be reconstructed.
- internal and external reports on suspicious activity, including decisions and actions taken, or not taken, by the Officer;
- contact between the Officer and law enforcement agency or FIUs, including records connected to requests for a defense (appropriate consent);

Records will be maintained in a secure and accessible form. Secure backups of all data are made daily and held on a secure server.

- Records include:
- Registration details
- Identification verification
- Enhanced Due Diligence
- Suspended accounts and reason for suspension
- Closed accounts
- Suspicious transaction reports
- Financial transactions (deposits, bets, withdrawals, prize payments)
- Self-exclusions
- Self-imposed limits
- Excluded players
- Bets placed
- Complaints and responses
- Audit trails
- Accounting and bookkeeping records including VAT returns, duties payable etc.
- Bank reconciliations
- Customer Service electronic correspondence records

Once the retention period has expired, any personal data shall be deleted unless RR is required to retain records for a longer period.

10. Appendices

10.1 *Appendix A - Specific legislative framework*

Alongside all the FATF and the CFATF-GAGIC legal framework (recommendations, assessments, guidelines...) the Company approach is based upon a concrete jurisdictional legal framework.

10.1.1 Curaçao

- National Ordinance Reporting Unusual Transactions (NORUT)
- National Ordinance Identification when Rendering Services (NOIS)
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction
- Sanctions National Ordinance

10.2 Appendix B - Internal Suspicious Activity Report (ISAR)

Report prepared by	
Full name	
Position	
Date of the report	
Personal details	
User ID	
Customer full name	
Registered address	
Date of birth	
Email address	
Phone number	
CDD / EDD information	
Has the customer provided POI?	
Has the customer provided POA?	
Has the customer provided POP?	
Has the SOF/SOW been collected?	
Reason for suspicion	
<i>Please include the suspected conduct as well as all the details</i>	

LUCKY DAYS

