

Raw Entertainment B.V.

AML Policy

Version 2.1

Table of Contents

1. POLICY HISTORY	4
2. POLICY STATEMENT	5
3. DEFINITIONS	5
4. PURPOSE	11
5. AUDIENCE	11
6. LEGAL FRAMEWORK	11
7. GOVERNANCE FRAMEWORK	12
7.1. Board of Directors	12
7.2. Compliance Officer	12
7.3. Targeted Financial Sanctions	14
7.4. Risk-based approach	14
7.5. Technological developments risk assessment	16
7.6. Data processing system	17
7.7. Staff Training	17
8. BUSINESS RISK ASSESSMENT (BRA)	17
9. CUSTOMER RISK ASSESSMENT	21
9.1. Risk Categories	21
9.2. Risk Score Calculation	22
9.2.1. Automatic Extreme Risk	22
9.2.2. Automatic High Risk	23
9.2.3. Risk Category Scoring Model	23
10. CUSTOMER ACCEPTANCE POLICY	25
10.1. Sanctions Screening	26
11. CUSTOMER DUE DILIGENCE	27
11.1. Standard Customer Due Diligence (SDD)	27
11.2. Customer Due Diligence (CDD)	28
11.3. Enhanced Due Diligence (EDD)	30
11.4. Politically Exposed Persons (PEPs)	31
11.5. Identification and Verification of Beneficial Owner	32
11.6. Ongoing monitoring	33
11.7. Procedure for Account Closure	33
12. DEPOSIT AND WITHDRAWAL MANAGEMENT PROCEDURES	34
12.1. Customer Account Balance	34
12.2. Payment Methods	34
12.3. Customer Deposits	34
12.4. Customer Withdrawals	34
12.5. Withdrawal Payouts	34
13. REPORTING OF UNUSUAL TRANSACTIONS	35

13.1. Unusual Transactions	35
13.2. Red Flag Indicators	36
13.3. Inability to Complete CDD/EDD Measures	36
13.4. Internal Suspicious Activity Report	37
13.5. External report to FIU	37
13.6. Reporting Procedure	38
13.7. Tipping-off	38
14. RECORDKEEPING	39
15. TRAINING	40
16. EMPLOYEES BACKGROUND CHECK	41
17. AUDIT	41
18. EXAMINATION BY THE GAMING CONTROL BOARD	42
19. INTERNAL AND EXTERNAL REVISION AND STAYING UP TO DATE	43
20. APPROVAL & REVIEW	43

1. POLICY HISTORY

Subject	Anti-Money Laundering and Prevention of Terrorism Financing and Proliferation Financing (AMLTF)	
Purpose	The AMLTF Policy establishes the principles followed by Roobet to fight money laundering, terrorism financing and proliferation financing. It also sets the ground principles of Roobet's governance framework that ensures appropriate measures are put in place to meet the AMLFT regulatory obligations.	
Responsible Department	Risk Director – Frederico Perez	
Policy Version	Approval Date	Changes Description
V1.0	22/04/2021	Creation
V1.1	26/06/2021	Major Update
V1.2	06/10/2021	Policy Review
V1.3	02/06/2022	Annual Review
V1.4	05/09/2022	Policy Update
V1.5	24/01/2023	Annual Review
V1.6	09/06/2023	Major Update
V1.7	06/06/2024	Annual Review
V2.1	12/12/2025	Major Update

2. POLICY STATEMENT

Roobet, its Executive Committee, Senior Management, Employees, and other Staff are committed to the highest standards and best industry practices of anti-money laundering and prevention of terrorism and proliferation financing, including anti-fraud, anti-corruption and anti-bribery. Robust and effective risk assessment and due diligence measures and controls are in place to ensure compliance with the applicable regulations, laws and industry standards and ensure a continuous practice of monitoring and training for an inclusive approach.

Roobet expressly prohibits the use of its website and services for any form of illicit activity, including money laundering, terrorist financing or trade sanctions violations, and is committed to ensure compliance with the applicable regulation and industry best AMLTF practices.

Roobet hereby:

- Recognizes that it is under the Curaçao Gaming Control Board Supervision; and
- Warrants that it complies with the January 2025 GCB Regulations and has implemented all the measures, processes and principles set on the same.

3. DEFINITIONS

The below terms shall have the meaning stated below:

Term	Definition
Adverse Media	Means any bad and/or negative information about the customer or business discovered from various sources. This information can also expose someone to being involved in a crime. Any new or existing customer mentioned in adverse media will be a subject for EDD. The Company may close the account or reject the registration depending on EDD results.
AMLFT	Means Anti-Money Laundering and Prevention of Terrorism Financing and Proliferation Financing
Employees / Staff	Means all individuals that have an employment relationship with Roobet or are contractors of Roobet including permanent, fixed term, and temporary employees, any third-party representatives, contractors or subcontractors,

	agency workers, volunteers, interns, and agents engaged with Roobet, regardless of level or seniority.
High Risk Countries	Means jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and proliferation financing. The Company defines the High Risk Countries based on the FATF regulations, which can be found on the following website: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

Money Laundering ML	Means money laundering, which is the process of concealing, disguising, converting, transferring, or removing criminal property. In other words, it is the process of converting the proceeds of crime into assets with legal origin. There are three stages of money laundering: 1. Placement – placement of funds generated from crime into financial system, either directly or indirectly (blending of funds, invoice fraud, smurfing). 2. Layering – the process of separating illicit proceeds from their source by creating complex “layers” of financial transaction designed to disguise the audit trail and provide anonymity (multiple bank transfers, investing in “cash” business). 3. Integration – the provision of apparent legitimacy to criminal derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system and appear to be legitimately earned or acquired funds (property dealing).
------------------------------	---

Terrorist Financing TF	Means terrorist financing, which is the provision or collection of funds with the intention that they should be used (or in the knowledge that they are to be used) to carry out acts that support terrorists or terrorist organizations or to commit acts on terrorism. The key differences between ML and TF are: • For money laundering to occur, the funds involved must be the proceeds of criminal conduct. • For terrorist financing to occur, the source of funds is irrelevant, i.e., the funds can be from a legitimate or illegitimate source. However, they both involve money or other forms of value. They both involve the movement of money or value, for example, from one person to another, one account to another, one institution to another, one country to another, one asset class to another. They are both keen to disguise the source and destination of funds.
PEP	Means any person who has been entrusted with a high-ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level. In particular, PEPs are: • heads of state, heads of government, ministers, members of the European Commission, deputy ministers and assistant ministers, • members of parliament and members of similar legislative organs, • members of the governing bodies of political parties, • members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of

	which are usually not subject to further appeal, • members of the boards of courts of audit, • members of the boards of central banks, • ambassadors, chargés d'affaires and defence attachés, • members of the administrative, management or supervisory bodies of state-owned enterprises, • directors, deputy directors, members of the board or other managers with a comparable function in an international or European intergovernmental organisation. Family member of PEP means a close relative, in particular • the spouse or civil partner, • a child and the child's spouse or civil partner and • both parents.
Policy	Means this AMLTF Policy.
Proliferation Financing PF	Means providing funds or financial services used for the manufacture, acquisition, or use of nuclear, chemical, or biological weapons and their delivery systems and related materials, in violation of national laws or international obligations.
Roobet Company	Means Raw Entertainment B.V., a limited liability company incorporated under the laws of Curaçao, with the company number 157205, having registered office at Korporaalweg 10, Willemstad, Curaçao that is under the supervision of the Curaçao Gaming Control Board (CGB).

Sanctioned List	Means a list published by governments and international authorities to combat persons engaged in illegal activities. Sanction lists include sanctioned people, organisations, or governments. Companies, individuals, organisations, or governments are on these lists as they may pose a high risk. Individuals and entities on this list are subject to financial restrictions prohibiting counterterrorism regimes and money laundering worldwide. Any new or existing customer that is found on the Sanctions database will have their account rejected or closed.
Source of Funds	Means the origin of the particular funds being used to deposit on the Company's website. This is not simply verifying which bank or financial institution the customer may have received the funds from. The information obtained should be substantive, relevant and establish the method/circumstances under which the funds were acquired.
Source of Wealth	The Source of Wealth refers to the origin of the entire body of wealth (i.e. total assets) of the customer. The information that the Company obtains should indicate the volume of wealth the customer would reasonably be expected to have and provide a picture of how it was acquired.
Website	www.roobet.com

4. PURPOSE

The purpose of this policy is to ensure that the Company complies with the obligations and requirements set out by the applicable regulation and rules regarding the prevention, identification and reporting of money laundering, terrorism and proliferation financing. This includes ensuring that there is an AMLTF Governance Framework in place, and implemented by the Company, that sets adequate procedures and controls to mitigate AMLTF risks.

This Policy, in conjunction with the AMLTF Governance Framework, is intended to support Roobet to:

- Carry out risk assessments and identify areas where there may be a heightened vulnerability to ML, TF and PF;
- Prepare, maintain, and approve written policies, procedures and controls detailing how the Company manages the risks of ML, TF and PF;
- Review and update the policies, procedures, and controls to reflect changes to the risk landscape and the continuously evolving internal approach to AMLTF;
- Provide training and guidance to all Employees / Staff on how to effectively implement the policies and controls outlined within this Policy, and how to monitor the risks and outcomes;
- Ensure that adequate resources, funds and systems are in place to support the controls needed to identify, assess and manage ML, TF and PF risks;
- Monitor the effectiveness and adequacy of the Company's policies and controls, and make improvements where required; and
- Ensure that action is taken where appropriate and that transactions are reported to the authorities when applicable and required.

The Policy is in place to ensure a company culture of clear intent, realistic evaluation and actionable processes, in order to achieve the Company goals of combating ML/TF/PF.

5. AUDIENCE

This Policy applies to all Roobet's Employees and Staff that work, collaborate or partner with Roobet. The adherence of Employees and Staff to this Policy is mandatory and non-compliance can lead to disciplinary action.

6. LEGAL FRAMEWORK

The Company's Policy and Procedures were created subject to the relevant applicable legislation, in particular (but not limited to):

- Curaçao - National Ordinance on Games of Chance (LOK) of 17 December 2024;
- Curaçao - National Ordinance Reporting Unusual Transactions (NORUT) of November 7, 2017;

- Curaçao - National Ordinance Identification when Rendering Services (NOIS) of October 2, 2017;
- Curaçao - National Ordinance Penalization of Money Laundering (NOPML);
- EU-Directive 2015/849 of the European Parliament and of the Council of 20 May 2015;
- EU-Directive 2018/843 of the European Parliament and of the Council of 30 May 2018;
- EU-Directive 2018/1673 of the European Parliament and of the Council of 23 October 2018; The FATF Recommendations for International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, adopted on 16 February 2012 and regularly updated thereafter.
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nation's Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the 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).

7. GOVERNANCE FRAMEWORK

The Company has developed internal security measures to prevent ML, TF and PF. The key features of these measures aim to stay aware of high-risk customers and detect suspicious activity, including the predicate offences of ML, TF and PF.

The Company has implemented an AMLTF framework that encompasses appropriate governance and oversight roles, internal controls, and sound practices for the management and supervision of the risks associated with ML, TF and PF.

7.1. Board of Directors

The Board of Directors are responsible for ensuring that they understand the AMLTF statutory obligations placed upon them and the Company. They are accountable for approving this AMLTF Policy as well as monitoring the effectiveness of the Company's AMLTF Program on a regular and ongoing basis. The Board is also responsible for receiving periodic reporting from the Compliance Department and the MLRO on adherence to the requirements established within this Policy and to provide further direction, if required.

7.2. Compliance Officer

The Company has appointed a Compliance Officer as part of the art. 5g of the NOIS. The Compliance Officer, the key individual responsible for the prevention of ML, TF and PF, has overall responsibility for ongoing regulatory compliance and anti-money laundering procedures.

The Compliance Officer's main responsibility is to review any internal suspicious transaction reports of unusual or suspicious transactions, and where necessary to submit a suspicious activity report ("SAR") with the Financial Intelligence Unit ("FIU"). The Compliance Officer is the main contact point for the FIU. In order to ensure that the Compliance Officer is able to fulfill their role effectively, the Company ensures that:

- Compliance Officer acts independently, has been provided the necessary knowledge of the Company's activities and is able to decide independently as to whether internal reports are to be escalated to the FIU.
- Compliance Officer has no conflicting responsibility which may pose a conflict of interest.
- Compliance Officer has sufficient time, resources and information to fulfill their responsibilities.
- Compliance Officer has a right to create work assignments to relevant employees and take decisions regarding ML/TF/PF prevention.

The Compliance Officer and their deputy carry out the following functions (including but not limited to):

- Creation (in writing) and further development of internal risk analysis, including a complete scope of risks connected to ML, TF and PFg.
- Developing and updating internal policies and procedures to prevent ML, TF and PF.
- Creation of uniform reporting channels.
- Be involved in the creation of new products, product changes, new practices and implementation of new technologies to ensure the correct measures are put in place to mitigate AMLTF risk.
- Ensuring compliance with current AMLTF regulations, and other relevant legislation.

- Ongoing monitoring of the Company's business activity to comply with applicable AMLTF regulations.
- Ensuring Standard Due Diligence (SDD), Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD). is undertaken as and when appropriate.
- Conducting suspicious activity risk assessments.
- The submission of SARs in appropriate cases.
- Contributing to the content of staff AMLTF training.
- Maintaining a list of all inquiries received from law enforcement agencies and records relating to internal and external disclosures.
- Submitting a report to the Board of Directors and other senior management on Compliance Officer activities, the risk situation of the Company, and the measures taken and intended to implement the obligations under applicable AMLTF regulations;
- Decide if customer funds shall be frozen before an ML/TF/PF risk.

The Compliance Officer and their deputy are authorized, within the scope of their performance of their work:

- To perform their tasks independently and effectively.
- To submit the necessary legally binding declarations for the undertaking and represent it externally in relevant situations.
- To provide undertaking-specific instructions for all matters relating to the prevention of ML, TF and PF.
- To carry out random checks without restriction.

7.3. Targeted Financial Sanctions

The Company will freeze funds and assets that have origin in sanctioned countries or individuals 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. The funds will be frozen without delay and without prior notice to the customer. The Company will also file a report with the FIU..

The Company checks on a daily basis for amendments of Sanctions Decrees and Regulations and updates its CDD and this policy accordingly to reflect such amendments.

7.4. Risk-based approach

The Company undertakes to prevent and combat ML, TF and PF following a risk-based approach. The risk-based approach happens on 2 (two) different levels, the Business Risk Assessment and the Customer Risk Assessment.

The Business Risk Assessment is carried out by the Company to: (i) assess its own operations; (ii) understand the risks to which it is exposed and (iii) assess if the business is within the adequate risk appetite / profile. The Customer Risk Assessment is carried out by the Company on each customer since each customer can have a different risk profile and consequently impact differently the business risk.

The Risk Based Approach performed by the company covers the following areas:

a) Customer Risk

Customer risk is the risk of ML/TF/PF that arises as a result of the relationship with a customer. The assessment of the risk posed by a customer is generally based on the customer's activity and/or their Source of Funds and/or Wealth. Categories of customers whose activities may indicate a higher risk include: (i) Customers who have multiple sources of income; (ii) Customers with irregular income streams; (iii) PEPs; (iv) High spenders (money maybe derived from illegal activities); (v) Disproportionate spenders (inconsistent with the company information on the customer source of income); (vi) Casual customers like locals/tourists, especially when spending pattern changes; (vii) Customers who are being exploited by third parties (e.g. criminals use third parties to gamble and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid CDD measures); (viii) Customers using multiple casino customer rating accounts to hinder a casino to track their gambling activities; (ix) Unknown customers (redeeming large amounts of chips); (x) Junkets (junket operators monitor customer activity and issue and collect credit).

b) Geographic Risk

Geographical risk is the risk posed to the Company by the geographical location of the customer and/or their Source of Funds and/or Wealth. The nationality, residence, place of birth and jurisdiction in which the customer has made their money are taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AMLTF system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered as high risk. The company takes into account a variety of sources of information produced by the FATF and well-known non-governmental well-known bodies. Some sources to use are:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Reports (INCSR)

- Countries sanctioned by the Office of Foreign Assets Control (OFAC);
- Countries identified by credible sources as providing funding or support for terrorist activities or having terrorist organizations operating within them;
- Countries on the European Commission's list of third countries having strategic deficiencies in their AMLTF regime;
- Countries on the Corruption Perception Index compiled by Transparency International.

c) Product Risk

Some products or services are inherently riskier than others and are therefore more attractive to criminals. The Company considers that the following may indicate high risk of ML/FT/PF, on its products:

- Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and/or theft from employer;
- Anonymous payment methods, such as pre-paid cards and certain virtual assets;
- Use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or after minimal play;
- Peer to peer gaming;
- The use by customers of accounts held or cards issued in the name of third parties;
- The transfer of funds from one gaming account to another;
- Types of financial services (credit/marker, currency exchange, check cashing);
- Multiple casino accounts or wallets (internet operator may own and control multiple web sites);
- Changes to the financial institution accounts used to fund casino account;
- Evidence of identity fraud. Details of financial institution accounts may be stolen and used on web sites. Alternatively, stolen identities may be used to open new financial institutions accounts;
- Using cash to fund a pre-paid card poses similar risks as cash;
- Games involving multiple operators;
- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts.

d) Distribution Channels Risk

The Company also takes into account that it operates an online business and the risks linked to it. While situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes. Accordingly, the Company has adopted technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations.

7.5. Technological developments risk assessment

The ML/FT/PF risks are always changing, especially with the launch of new technologies and products that can shape the industry. Being aware of these risks, the Company has set a Technology Risk Assessment process that requires all new products, businesses practices and technologies incorporated into the business to go through a risk assessment to understand if they promote ML/FT/PF risk in any way.

Accordingly, whenever any department within the Company wants to create new products, adopt new business practices or add new technologies to its process, it must file a formal request to the Risk Director for an internal risk assessment in advance.

The Risk Director will review the request and ensure that the new product | practice | technology:

- Does not promote ML / FT / PF;
- Does not promote anonymity;
- Is aligned with the business risk appetite.

The Risk Director will document the checks done to the new product | practice | technology and provide guidance on measures that should be implemented to mitigate any potential risk from a ML / TF / PF perspective. The Company also performs a Technological Risk Assessment on all of its existing products during the Business Risk Assessment.

7.6. Data processing system

The Company operates its internal data processing system to detect high-risk scenarios for ML, TF and PF in day-to-day operations.

The Data processing system consists of the following mechanisms:

- identification and verification of all customers before the business relationship is established is carried out manually by internal KYC team;
- PEP and sanction list checks are performed by the relevant software;
- transaction monitoring is managed by trained staff; and
- reporting of all suspected ML, TF or PF are escalated to the Compliance Officer, who will determine whether to submit a SAR to the FIU.

The Company will monitor trends and changes connected to ML/TF/PF and will develop additional internal procedures to keep it up to date.

7.7. Staff Training

Upon joining the Company and thereafter annually, all Employees and Staff receive training on AMLTF procedures and associated policies. The training will be supplied by online and face-to-face training providers or by the appropriate Company's internal specialists. Specific Employees and Staff members are trained depending on the individual risk analysis.

8. BUSINESS RISK ASSESSMENT (BRA)

The Company carries out an annual business risk assessment to identify the ML/TF/PF risks to which it is exposed and to ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. Through the BRA, the Company is able to identify the inherent and residuals risks of the business and can decide on the best mitigation actions to take in order to stay within its risk appetite

The Company's BRA covers:

- **Geographical Risks:** the characteristics of the country of residence and other geographical risks;
- **Customer Risks:** the general characteristics of the customer;
- **Product Risks:** the characteristics of the products and services provided by the Company;
- **Transactional Risks:** risks connected to specific transactional behavior;
- **Delivery channels:** the characteristics of intermediaries and interface risks;
- **Operational risks:** including risks connected to Employees / Staff and the practical implementation of AMLTF processes.

The BRA is performed through analysing the above risks across the business and identifying potential ML/TF/PF threats to the business; vulnerabilities in the business; and the likelihood that those risk / events can be exploited for criminal intent. Following this first assessment, the Company assesses the likelihood of such risks arising, and the impact it will have on the business should these risk factors materialize. Based on this information, the Company can measure the risk and decide on the controls that need to be implemented in order to best mitigate those risks.

The risk is assessed attending to the following criteria:

INHERENT RISK MATRIX						
	LIKELIHOOD					Inherent Risk Scoring
	1. Rare	2. Unlikely	3. Possible	4. Likely	5. Almost Certain	

IMP ACT	1. Insignificant	1	2	3	4	5	1. Very Low
	2. Minor	2	4	6	8	10	2. Low
	3. Moderate	3	6	9	12	15	3. Moderate
	4. Major	4	8	12	16	20	4. High
	5. Extreme	5	10	15	20	25	5. Extreme

Inherent risk represents the risk level that exists without controls or mitigations in place. It

can be measured by two factors – likelihood and impact assigned to individual Risk Factors:

a) Likelihood - is how probable it is that an event will occur;

b) Impact - is an estimate of the harm that could be caused by occurrence of an event without controls in place.

Inherent risk = Likelihood x Impact

LIKE LIHO OD	Rare	The risk may only be realized in exceptional circumstances with a less than 5% likelihood of occurrence
	Unlikely	The risk may occur infrequently with 5% to 30% likelihood of occurrence
	Possible	Likely occurred previously and could reasonably occur again; 30% to 60% likelihood of occurrence
	Likely	Extremely likely to occur with 60% to 95% likelihood of occurrence
	Almost Certain	The risk is certainly expected to occur regularly and has greater than 95% likelihood of occurrence

IMP ACT	Insignificant	Minimal/insignificant impact on operations with no real reputation or financial impact.
	Minor	Unlikely to have any significant impact on performance: a) Loss of <1% of revenue; b) Increase in costs of <1%; c) Slight impact on customer satisfaction;

		d) No regulatory non-compliance; e) Low impact on reputation.
	Moderate	Will have considerable impact on operations in the short-term period: a) Loss of revenue of 1-10%; b) Increase in costs of 1-10%; c) Potential regulatory compliance impact; d) Potential reputation impact.
	Major	Impact will have a serious effect on operations: a) Loss of 10-30% of revenue; b) Increase in costs of 10-30%; c) Significant regulatory non-compliance that can lead to fines and financial impact; d) Significant impact on reputation that can generate negative headlines in media.
	Extreme	Impact will have a serious effect on operations in the long-term: a) Loss of more than 30% in revenue; b) Increase in costs of more than 30%; c) Substantial regulatory consequence that can lead to high value fines, criminal offences or licence suspension; d) High impact on reputation and ownership.

CONTROL EFFECTIVENESS		
5	Non-Existent	No controls in place
4	Weak	Significant control gap. Limited policy and procedure in place to implement the controls; controls that are in place are not tested for effectiveness.
3	Adequate	Controls in place are largely addressing the root cause of the risk but are not very effective
2	Reasonably Strong	Controls in place are addressing the root cause of the risk and is effective, scope for more improvement in process
1	Strong	Control has proven to be highly effective in mitigating the risk

Control Effectiveness is assigned by taken into consideration controls that are in place to mitigate the inherent risk. Note: in certain cases the rise may arise, not because of a lack of control, but because

of a failure of existing controls. Hence, the key to mitigating the risk effectively is to ensure that the controls are effective.

RESIDUAL RISK RATING MATRIX							
		INHERENT RISK RATING					RESIDUAL RISK RATING
		1. Very Low	2. Low	3. Moderate	4. High	5. Extreme	
CONTROL EFFECTIVENESS	5. Non-existent	5	10	15	20	25	Extreme
	4. Weak	4	8	12	16	20	High
	3. Adequate	3	6	9	12	15	Moderate
	2. Reasonably Strong	2	4	6	8	10	Low
	1. Strong	1	2	3	4	5	Very Low

Residual risk is the risk that remains after taking into account the controls that are in place.

Residual risk is the greatest when inherent risk is high and the controls put in place are not effective, it decreases if controls are effective.

Residual risk = Inherent risk x control effectiveness

The BRA is a living document, maintained and updated on a regular basis depending on changes in the business, changes in regulation or new risks identified in ongoing daily tasks and reviews - or as identified by any supranational, national or sector specific risk assessments issued by regulatory authorities. The BRA as well as this Policy will be reviewed and approved by the Board of Directors on an annual basis, at minimum. The BRA will also be sent for review, should new risks arise with a risk classification that warrants the awareness of the Board of Directors.

9. CUSTOMER RISK ASSESSMENT

The Company takes a risk-based approach to identify, assess, mitigate and manage potential ML / TF / PF risks of its customers. Accordingly, the Company will risk rate all its customers based on identified risk factors upon registration and will continue to update and review the customers' risk on an ongoing basis. The Company follows the criteria set out in applicable AMLTF regulations to assess the customer risk.

Through the Customer Risk Assessment, the Company will:

- Assess a Customer's ML/TF/PF risk;
- Ascertain the level of management approval required;
- Determine the level of due diligence required that would be appropriate with the Customer's identified level of risk; and
- Determine the frequency for ongoing monitoring and Customer information update.

9.1. Risk Categories

Before the customer starts a relationship with the Company, the Company will perform a Customer Risk Assessment to determine the risk category in which the customer falls into and if the customer risk is within its Customer Acceptance Policy scope and risk appetite.

The Company categorizes its customers risk in 4 different categories depending on the ML/TF/PF risk that they pose to the business:

- Low
- Medium
- High
- Extreme

To understand in which Risk Category the customer falls into, the Company will analyse the customer risk attending to the customer:

- **Individual status** – Assess if the customer is a PEP, under sanctions, Adverse Media, etc. based on his personal information.
- **Geographical location** – Assess if the customer is using proxies or is resident in High Risk Countries or sanctioned territories.
- **Gambling and transactional behaviour** – Understand the customer behaviour on the website and if there are any suspicious ML/TF/PF behaviours connected with it.
- **Payment methods** – Assess the risk of the payment methods being used by the customer and whether they promote anonymity or favour ML/TF/PF.
- **Fraud red flags** – Assesses the severity of the alerts that the customer triggers during its ongoing relationship with the Company.

9.2. Risk Score Calculation

Each Customer will be assigned a risk category of Extreme, High, Medium or Low. The Customer Risk Assessment Scoring Model will assist in determining a customer's risk level through assessment of preconditions and other risk factors relevant to a customer. Based on the Customer profile information that is inputted against each risk factor, the Customer Risk Assessment Scoring Model will produce a risk score and assign a corresponding risk profile for the Customer.

There are factors that trigger an automatic Extreme and High risk rating regardless of whether or not there are any other risk factors at the time of the account registration or on an ongoing basis. These factors include (i) the customer is associated with a country, occupation or industry that are considered High Risk, (ii) the customer is a PEP or a close associate of a PEP; or (iii) the customer reveals a positive sanctions check match. If the Customer does not meet any of the pre-conditions, then the risk will be calculated in accordance with the Customer Risk Assessment Scoring Model set below.

9.2.1. Automatic Extreme Risk

All customers that meet any of the below conditions will automatically be categorized as Extreme Risk and will have their accounts closed:

Conditions	Risk Category	Rationale
Public safety risk	Extreme	Customer who has Adverse Media that confirms its connection to organized crime groups or to has been convicted or linked to ML/TF/PF practices.
Affiliated with organized crime groups	Extreme	Customers who have been confirmed by law enforcement agencies to be part of or affiliated with organized crime groups.
Positive match to sanctions list or terrorist list	Extreme	Customers that through the sanction screening process were identified and being on a sanction / terrorism list.
Sanctioned Country	Extreme	Customers that are confirmed to live in sanctioned countries.

9.2.2. Automatic High Risk

All customers that meet any of the below conditions will automatically be categorized as High Risk and will be submitted to Enhanced Due Diligence:

Conditions	Risk Category	Rationale
PEP	High	Customer who is a PEP or has a close connection to PEP (son, daughter, wife, dad, etc.)
High Risk Country	High	Customer is resident in a high-risk country, or his deposits or withdrawals are from or sent to high risk countries.

Customer associated with high risk occupation	High	Customer has a high risk occupation such as jewellery or oil industry.
Multiple suspicious transaction reports (STRs)	High	2 or more STRs have been filled to the FIU.

9.2.3. Risk Category Scoring Model

All customers that do not meet any of the above mention conditions will have their risk category assessed through the below Customer Risk Assessment Scoring Model:

Indicator	Description	Score
Individual status		
Head of International Organization	Customer is not a PEP, but is the head of relevant institutions that holds high influence in the society.	40
Adverse Media	A customer was mentioned in negative news or information the Company discovered from various sources	40
Geographical Location		
Not at home	A customer whose IP location is different from their registered address	20
Medium-risk country resident	A customer resides in a Medium-risk country as defined by the company.	30
Gambling Behaviour		
Large sums no play	A customer depositing large sums, then places minimal stake bets, then withdrawing all their funds	50
Large sums big losses	A customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence (XCG 10,000 per week)	50
Low odds betting	A customer repeatedly placing short odds (such as red/black on roulette or repetitive betting on favourites) bets	25
Big changes in money	Dramatic changes in terms of volume and size of customer deposits or staking activity	20
Several gaming accounts	A customer is trying to register several gaming accounts	30
Transactional Behaviour		
Smurfing	A customer making multiple deposits or withdrawals of small amounts without no objective reasons	30

Spending above wages	A customer's spending is outside of their affordability	20
No withdrawals	Customer has never requested a withdrawal	-20
Withdrawal without playing	Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling	30
Payment Methods		
Card switching	A customer opening an account and registering several different cards and making transfers between them	20
Low Risk Payment Methods	Customer uses Bank transfers (Klarna, Trustly, Rapid, ApplePay), debit cards issued by banks.	10
Medium Risk Payment Methods	Customer uses EEA licensed e-wallets (Skrill, Neteller, paysafecard)	20
High risk payment methods	Customer uses prepaid cards, Vouchers and Cryptocurrency	30
fraud red flags a customer triggered		
VPN	Customer used a VPN	30

Once the score is calculated, a risk level is assigned based on the below scoring board:

<u>Risk Assessment Score</u>	<u>Risk Category</u>
0-20	Low
21 - 40	Medium
41 - and higher	High

The customer risk assessment will be done on a daily basis and will be updated automatically in accordance with the customer behavior during the business relationship. This means that a customer risk profile can increase and decrease while the business relationship goes on.

10. CUSTOMER ACCEPTANCE POLICY

The Customer Acceptance Policy defines the criteria by which the Company may or not accept potential customers and describes the registration process. The Company has adopted a Customer Acceptance Policy that complies with all applicable regulations, laws, and licence obligations of the Company.

The Board of Directors and senior management have communicated the importance of the Customer Acceptance Policy to all employees to protect their customers, minors, and their business interests,

ensuring adherence on all levels of operation. The following groups are banned from opening accounts on the website:

- Individuals which are under 18 years old (Minors) and those who are not able to participate responsibly in gambling services due to addictions, mental issues and/or self-excluded individuals.
- Legal entities or individuals acting on behalf of a third person. Exclusively natural people may open a non-transferable account on Roobet.
- Any individual having connections to illegal or illicit activities. Roobet has a zero-tolerance approach to all forms of ML, TF, PF and Sanctions evading.
- Any individual who is not lawfully allowed to participate in gambling services, due to regulatory or local requirements.
- Individuals who have been excluded from Roobet due to past violations or refusal to comply with the Company's verification requests.
- Anonymous or clearly fictitious accounts.

The following groups are welcome to open an account on Roobet:

- Any natural person lawfully allowed to participate in gambling services.
- Customers who intend to fully comply with the company's AMLTF Policy, measurements and verification requirements.
- Individuals whose Source of Funds confirms the funds were lawfully acquired.

Following the Customer acceptance policy, an individual risk score will be applied to each customer and risk-mitigating measurements will be taken following the evaluation to ensure the individual is not engaged in illicit activities or behaviours not tolerated by the Company. Roobet only allows use of its service in a non-professional, exclusively personal manner, for recreational and entertainment purposes only.

Customers may only open one account in their name on the Website. Additional checks are run to block multiple accounts by email address, mobile number, device and certain other combinations of customer data. These checks are done in order to prevent customers opening multiple accounts.

10.1. Sanctions Screening

Individuals that are sanctions or listed in any blacklists, in particular, in the lists mentioned below, will not be able to register an account:

- Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s."
- Australian Sanctions (AU)
- Bureau of Industry and Security - Entity List (US)
- Bureau of Industry and Security - Unverified List (US)
- Bureau of Industry and Security (US)

- Canada, Office of the Superintendent of Financial Institutions, OSFI Consolidated
- CIA Leader list
- Consolidated Canadian Autonomous Sanctions List
- Department of State, AECA Debarred List (US)
- Department of State, Non-proliferation Sanctions (US)
- EU Financial Sanctions (EU)
- European Union, Consolidated list of persons, groups and entities subject to EU financial sanctions
- Foreign Financial Institutions Subject to Part 561 (the Part 561 List)
- Foreign Sanctions Evaders List (FSE)
- INTERPOL Wanted List
- Islamic Republic of Iran
- Libya Sanctions
- Non-SDN Iranian Sanctions Act List (NS-ISA)
- OFAC Consolidated Sanctions List
- Office of the Superintendent of Financial Institutions (Canada)
- Palestinian Legislative Council (PLC) List
- Sectoral Sanctions Identifications (SSI) List
- Specially Designated Nationals (OFAC)
- Specially Designated Nationals List (SDN)
- Switzerland Sanction List (SECO)
- U.S. Department of Commerce, Bureau of Industry and
- Security - Denied Persons List
- U.S. Department of the Treasury, Office of Foreign
- Assets Control (OFAC)
- UK Financial Sanctions (UK)
- UK, Consolidated Financial Sanctions list (HMT)
- United Nations Sanctions (UN)
- United Nations Security Council (UN), Consolidated Sanctions list
- US Consolidated Sanctions (US)
- US State Dept. WMD Non-Proliferation List
- Existing customers who have an existing exclusion on the site.
- Individuals with fraud red flags.

11. CUSTOMER DUE DILIGENCE

The Company is required to verify the identity of all of its customers. The Company will collect and verify the identification information collected from each of its customers and retain such information as part of the business relationship. The customer identification will be split into SDD, CDD and EDD

11.1. Standard Customer Due Diligence (SDD)

The SDD applies to all customers that want to register an account on the website and consists of collecting identification information of the customer. Accordingly, all customers that want to register on the website must previously provide the following information:

- a) Full Name;
- b) Date of Birth;
- c) Permanent Address;
- d) E-mail;
- e) Username; and
- f) Phone number (optional).

Without providing the above identification information, the customer will not be able to register an account, deposit, bet, or take any other action on the website. After the customer has completed the registration form to open an account, the Company will perform a set of verification procedures in order to ensure the authenticity of the information provided by the customer. The checks will include:

a) Personal Information Check

The Compliance Team will verify the information uploaded by the customer and confirm if the same is legitimate, belongs to a celebrity or is potentially fake. In case the information appears to be suspicious, Customer Due Diligence will be applied to the customer before he can use his account.

b) Sanction Screening

Sanction screening will be run on Seon's platform. The customer's name, address and date of birth will be automatically sent by Roobet database to Seon's platform, which will run the customer information through the sanctions list. In the event that there is a match, the Compliance Team will be notified and will verify if it is a true match or a false positive and will add a description on Seon's platform of the reason why it is a true match or a false positive and will accept or reject the customer registration accordingly.

In case of a positive match, the Compliance Team will reject the account registration and will report the event to the MLRO.

Sanction screening is performed upon registration and on a daily basis through Seon's platform. The checks will also be performed whenever there are changes to the sanctions list to evaluate if there are any changes to the customer profile. In the cases where a new match is triggered, the Compliance Team will be notified and will verify if it is a true match or a false positive and take the necessary actions.

c) PEP Screening

The Seon platform will run the customer information within the PEP lists. In case there is a match, The Compliance Team will be notified and the customer account will be automatically suspended and an EDD request will be sent to the customer. The checks will be run upon registration and on a daily basis. In the cases where a new match is triggered, the Compliance Team will be notified and will take the necessary actions.

The PEP screening is performed upon registration and on a daily basis through Seon platform. The checks will also be performed whenever there are changes to the PEP list to evaluate if there are any changes to the customer profile. In the cases where a new match is triggered, the Compliance Team will be notified and will verify if it is a true match or a false positive and take the necessary actions.

d) Adverse Media

The Seon platform will run a search on the customer name on the internet to try to find any Adverse Media regarding the same. In case such Adverse Media is found, the Compliance Team will be notified and will analyze such Adverse Media, perform a risk analysis, and make a decision on whether to accept or not the customer.

e) Risk Scoring

The Company will also run a risk assessment on the customer and categorize it as Low, Medium, High or Extreme.

11.2. Customer Due Diligence (CDD)

CDD consists of collecting the customer identification document and attesting the information provided by the customers on registration. CDD is required when:

- a)** The customer is categorized with a Medium Risk;
- b)** The customer has deposited through a single or linked transactions a total amount of XCG 4,000 (or equivalent) within a year;
- c)** The customer has tried to withdraw XCG 4,000 through a single or linked transactions a total amount of XCG 4,000 (or equivalent) within a year;
- d)** The customer has triggered suspicious Adverse Media that is not enough to classify it as High or Extreme Risk;
- e)** Whenever the Compliance Team considers relevant to collect additional customer information.

Upon triggering any of the above scenarios, the customer account will be automatically restricted and the customer will not be able to bet, deposit or withdraw funds from the website, with all available balance frozen until the customer completes CDD. To complete CDD the customer will have to provide the following documents:

a) Identification Document:

To evidence identity, the Company requires a valid (non-expired) government issued document containing photographic evidence of the customer's identity. The following documents may be accepted for the verification purpose:

- Passport;
- Driving License;
- Government Issued Identity Card.

b) Proof of Address:

As proof of address the Company only accepts the below documents, as long as their were issued within the last 6 months:

- Utility bill of water, electricity or gas;
- Bank Statement;
- Correspondence or any other government-issued document from a central or local government authority, department or agency issued in the last 6 months.
- Lease agreement (Does not have to be issued in the last 6 months but must be currently valid.)

The Company will not accept documents that:

- Have expired;
- Are not clear, legible and of good quality;
- Are cropped or blurred.

If the CDD information is not received within 30 (thirty) days from the moment the customer triggered the CDD process, the Company will close the customer account, freeze the funds and report the transaction to the FIU if a presumption of ML, TF or PF exists. If no presumption of ML, TF or PF exists, the Company will transfer the funds to the same bank or wallet it was deposited from.

11.3. Enhanced Due Diligence (EDD)

The Company performs EDD on all customers that in its understanding pose a higher risk to the business or that due to its activity on the website raise internal flags that require further analysis to ensure that no illicit activity is taking place on the Website. For example:

- The customer is categorized as High Risk;

- The customer is a resident of High Risk Country;
- The customer is a PEP or a family member or known close associate of a PEP;
- The customer has triggered alerts that raise concerns with the customer activity on the Website;
- The customer has Adverse Media that raised ML/FT/PF concerns;
- The Company was informed by the authorities that the customer has a high risk of ML, TF or PF;
- If the Company has doubts as to whether the information collected regarding the identity of the customer is correct or not (or no longer) accurate;
- In any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose,
- If the payment of a customer's winnings is made to a different payment account of the customer than to the account from which the customer deposited funds.

The Company can perform EDD whenever it considers relevant and wants to have a better understanding of potential ML / FT / PF profile of the customer. Upon triggering any of the above risk factors, the customer account will be automatically restricted and the customer will not be able to bet, deposit or withdraw funds from the website, and all available balance will be frozen till the customer completes EDD.

The applied EDD measures will vary in accordance with the risks identified and will increase the degree and nature of monitoring of the customer activity, in order to determine whether transactions or activities appear unusual or suspicious. At a minimum, EDD will include one or more of the following measures:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Undertaking re-verification of identity (repeated CDD).
- Requesting information regarding the Source of Funds and Source of Wealth of the customer.

For example:

- salary income or company profit (certified payslip / certified employer letter / audited accounts if self-employed)
- sale or liquidation of financial instruments (certified shares/investments sale contracts or statements/ accountant letter)
- sale of property (certified copy of the contract of sale or letter from a solicitor or estate agent) of inheritance (certified copy of will including the value of heritage)
- sale of the company (certified contracts, media articles, certified letter from accountant or solicitor).
- Obtaining information on the reasons for intended or performed transactions;

- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In cases where the Company believes higher ML/FT/PF risk to be present, it will request the customer to provide updated information from time to time even though there may not be any change in pattern or activity conducted by the customer.

If the EDD information is not received within 20 (twenty) days from the moment the customer triggered the EDD process, the Company will close the customer account, freeze the funds and report the transaction to the FIU if a presumption of ML / TF / PF exists. If no presumption of ML / TF / PF exists, the Company will transfer the funds to the same bank or wallet that they were deposited from.

In cases where there is a higher risk, establishment of the business relationship or continuation of the business relationship (if the higher risk only arose later or was only recognised later) may occur only with the consent of the Compliance Officer.

11.4. Politically Exposed Persons (PEPs)

The Company takes reasonable measures to determine whether a customer is a PEP or a related person (a family member or close associate of PEP) at the time of registration.

Whenever a PEP or related person is detected the customer account will be suspended and the Compliance Team will promptly perform an EDD and request the customer to provide the following information:

- a) Source of Wealth;
- b) Source of Funds;
- c) Office or position of the PEP;
- d) Organization / institution name of the PEP;
- e) Record of the nature of the relationship with the PEP.

The Compliance Team might request additional information whenever they find it relevant. After collecting the above information, the Compliance Team shall file a report to the Compliance Officer requesting the approval of the continuing of the business relationship. The Compliance Officer shall make a decision within 2 (two) days from the notification of the Compliance Team.

If the customer has not provided the requested information within 30 (thirty) days, the Compliance Team shall close the customer account and inform the Compliance Officer.

11.5. Identification and Verification of Beneficial Owner

The Company is also required to identify and verify the identity of the beneficial owner. Accordingly, the company has implemented the following processes:

a) Third Party Accounts

The company does not accept that customers register accounts through third parties or on behalf of a third party. Upon registration all customers must confirm through accepting the Terms of Service that they are registering an account to play and transact on their own and not on behalf of a third party.

In case the Company finds an account that is being used on behalf of a third party, the Company will apply EDD measures on the account and will perform EDD on the third party on behalf of which the account is being used.

b) Syndicates

In the cases where the Company encounters a situation involving an account being used by a syndicate or multiple customers that share the deposits and wins of the accounts, the Company will apply EDD measures to all the beneficial owners of the account. During that time the account will be restricted and the funds frozen until all beneficiaries provide the requested information. Additionally the Compliance Officer shall be informed of such cases and take the necessary actions.

c) Business Accounts

The company does not permit businesses to open accounts on its website. In case, the Company ever accepts a business to open an account on its website, it will perform a EDD on the beneficial owners and will collect the following information:

- Certificate of Incorporation;
- Bylaws;
- Identification information, verification and evidence of all persons holding 25% or more of the shares or voting rights or a person who otherwise exercises ultimate effective control of the customer.

11.6. Ongoing monitoring

The general due diligence duties include the ongoing monitoring of the business relationship. This includes:

- Obtaining fresh identification when existing documents have expired. (This can be done on a risk-sensitive basis.)
- Questioning the data and information the Company has whenever inconsistencies are noticed.
- Generally reviewing and updating information from time to time, on a risk sensitive basis.

- Checking if transactions match with the documents and information available to the Company about the customer and the origin, customer's assets
- Updating the respective documents, data, or information at appropriate intervals.

To keep all customers' information up to date, the Company applies CDD procedures every 6 months from the date of the successful complete verification of each customer on a risk-sensitive basis. Shorter time periods may be applied to high risk customers that have been submitted to an EDD.

11.7. Procedure for Account Closure

There are numerous reasons for why the Company will want to close a customer's account:

- Fraud
- Cheating
- Bonus Abuse
- Allowing a third person to use their account
- Underage gambling
- Problem gambling
- Being abusive to staff
- Commercial concerns
- CDD failure
- Terms and Conditions breach

By law the Company must end the business relationship with the customer unless we have obtained appropriate consent for it to continue and even then it is precautionary to close the account.

Due to applicable AMLTFlaws on tipping off, the Company cannot inform the customer that it has concerns regarding ML/FT/PF, and so account closure must be done sensibly and sensitively. The Compliance Officer considers whether a SAR should be submitted regarding the Company's concerns about the customer's behaviour and consent sought from the FIU to continue the business relationship with the customer, to avoid tipping them off while an investigation is ongoing.

12. DEPOSIT AND WITHDRAWAL MANAGEMENT PROCEDURES

12.1. Customer Account Balance

Each customer has a wallet with funds from which bets are deducted, and winnings added. All funds deposited by the customer or owed by the Company are credited to the customer's corresponding account. The customer can top up the funds in his account by depositing through the cashier on the

site and then use these funds to place bets. Bets are deducted from his account balance, and winnings are added to the account balance.

The customer can withdraw withdrawals of available funds in the customer's balance. The Company does not offer credit to customers. A customer may not transfer funds to another customer.

12.2. Payment Methods

Payments are only accepted from accounts held with licensed financial institutions or through licensed payment providers. No cash deposits/withdrawals will be effected directly between the Company and its customers.

12.3. Customer Deposits

After registering, a customer may deposit funds into their account through the cashier on the site. In order to facilitate these deposits, the company has integrated with a number of gateways. All gateways are PCI DSS compliant, and the company does not hold any credit card data itself. The company submits the transaction to the payment service provider and then waits for approval from the card acquirer/e-wallet. On approval, the deposit status is updated and the funds added to the customer's balance.

12.4. Customer Withdrawals

A customer with an available balance will be able to request a withdrawal of the funds via the cashier on the site. The customer will enter the amount they wish to withdraw and select their preferred payout method. The withdrawal amount is then deducted from the customer's balance.

12.5. Withdrawal Payouts

In remitting funds to the customer, we will, where possible, remit the funds directly into the account from which the funds originated. Provided that where this is not possible, we will remit the funds to the customer in line with the requirements under AMLTF legislation.

13. REPORTING OF UNUSUAL TRANSACTIONS

Employees and Staff of the Company must report to the Compliance Officer if there is suspicion or knowledge of ML, TF or PF or if the funds being used on the Company's website are otherwise the proceeds of criminal activity. The Compliance Officer will consider each report and determine whether it gives grounds for knowledge or suspicion. If it does, then a SAR should be submitted to the Financial Intelligence Unit – Financiële Inlichtingen Eenheid (hereinafter – FIU or FIU Curaçao).

Knowledge means that the person reporting knows the event to be a fact. Suspicion implies that the person reporting the incident may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial or financial sense.

A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report the activity then arises. Likewise, if concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and will need to be reported to the FIU. The Compliance Officer assesses all the circumstances and the customer or others more questions if needed. The choice depends on what is already known about the customer and the transaction and how easy it is to make further enquiries.

13.1. Unusual Transactions

The following transactions or intended transactions are deemed unusual:

- a) Transactions which in connection with ML, TF or PF are reported to the Police or to the Department of Justice;
- b) 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);
- c) Transactions in the amount of XCG. 5,000 (or equivalent) or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:
 - a. A cashless transaction in the amount of XCG. 5,000 (or equivalent) 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;
 - b. Accepting or releasing a deposit in the amount of XCG. 5,000 (or equivalent) or more at the request of the customer;
 - c. Sale to a customer of chips in the amount of XCG 5,000 (or equivalent) or more. "Chips" include but is not limited to tokens and credits.
 - d. A cash out in the amount of XCG. 5,000 or more;

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 XCG. 5,000 (or equivalent) or more and is considered per gaming day.

- d) Presumed money laundering transactions or terrorist financing: transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

13.2. Red Flag Indicators

Red flags are not intended to automatically result in filing a SAR with the FIU, however are merely indicators that should lead the Company to question the customer's behaviour. If there is no reasonable

explanation for the red flags, then an internal report must be made to the Compliance Officer. The following is a list of possible red flags which should be considered:

- Customer does not cooperate in the carrying out of CDD/EDD.
- Customer attempts to register more than one account on the Website.
- Customer makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquires about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the Customer's wealth, income or financial situation.
- Customer seeks to transfer funds to a bank account held in the name of a third party.
- Customer requests a withdrawal to an account he never deposited with.
- Customer opening an account and registering several different cards and making transfers between them,
- Customer deposits large sums, then places minimal bets, then withdrawing all their funds,
- Customer deposits large amounts and repeatedly losing large amounts as if the loss is of no consequence.

13.3. Inability to Complete CDD/EDD Measures

If a customer refuses to provide CDD/EDD documentation, the Company won't immediately equate this on its own to suspicion of ML/FT/PF. The Company will consider all factors and information, including the payment method used, games played, playing trends and patterns, residence jurisdiction, and open-source information. If there are grounds to suspect ML/FT/PF after considering all of these factors, then a SAR must be submitted.

13.4. Internal Suspicious Activity Report

All Employees and Staff have a duty to report suspicious transactions. If an Employee or Staff member has any suspicion about a customer's behaviour or transaction, it must be reported to the Compliance Officer immediately. All Employees and Staff members are expected to report suspicious transactions to the Compliance Officer. For this purpose employees use approved Internal Suspicious Activity Report Form.

The Employee or Staff member should still submit the report, even if their superiors are not in agreement. It will then be up to the Compliance Officer to determine if the information available can be considered as sufficient for a SAR to be made to the FIU.

The following information is included to an Internal SAR:

- The customer's details
- The member of staff's statement about what gave them cause to make the report
- All relevant documentation and information

The Compliance Officer will:

- acknowledge receipt of the report and review and investigate further as required
- make an assessment based upon all the information and decide whether the matter needs to be reported to law enforcement
- if it does, submit a SAR to the FIU
- make a record and inform senior management about the decision taken.

13.5. External report to FIU

Once the Compliance Officer has received an Internal SAR, they will decide if a SAR should be submitted to the FIU. When making this decision, the Compliance Officer should consider that AML legislation is intended to address and attack serious crime which usually either involves amounts that are not minimal or circumstances that show an intent to circumvent and abuse the safeguards in place to deter the use of the financial system for criminal purposes. For example, identity fraud and chargebacks may give rise to ML, but a licensee will only be subject to reporting obligations if they result in funds derived from these activities being deposited with or held by the licensee. However, the Company won't report single instances involving small amounts but should consider whether it can detect a more significant pattern or scheme.

The Compliance Officer considers whether an internal report gives rise to a suspicion of ML/TF/PF by taking into account all relevant information, including assessing whether there are common denominators between e.g., repeated suspicious behaviour, instances of chargebacks or identity fraud. For example, these may consist of common or related persons, common IP addresses etc.

The Compliance Officer, in deciding to submit the SAR or not, should answer the following questions:

- Who is involved?
- How are they involved?
- What is the criminal/terrorist/other property?
- What is the value of the criminal/terrorist/other property (estimated as necessary)?
- Where is the criminal/terrorist/other property?

- When did the circumstances arise?
- When are the circumstances planned to happen?
- How did the circumstances arise?
- Why are you suspicious or do you have knowledge?

13.6. Reporting Procedure

The Company will report without delay any unusual transaction or any intended unusual transactions to the FIU, through the user interfaces on the FIU's website or by mail (if possible), without due delay if there are indications that:

- the Company know, suspect, or has reasonable grounds for knowing or suspecting money laundering and/or terrorist financing,
- an asset related to a business relationship or transaction originates from a criminal offence that could constitute a predicate offence to money laundering,
- a business case, transaction, or asset is related to terrorist financing.

When the Company decides whether it is necessary to submit SAR, it takes the following factors into account, including but not limited to:

- the purpose and nature of the transaction,
- peculiarities in the customer,
- the financial and business background of the customer,
- the origin of the assets contributed or to be contributed.

The Company doesn't execute suspicious transactions, except in cases where it cannot postpone the transaction or if the postponement could hinder the prosecution of an alleged criminal offense. In this case, the Company submits SAR immediately.

13.7. Tipping-off

It is an offence to tell anyone that a SAR has been submitted or is being considered to be submitted and that this is likely to prejudice the investigation by the FIU. This means it is possible to have an internal discussion about the customer, but in no way can the customer or their associates be given any indication that the customer may be under investigation.

This means that no Employee or Staff member::

- can, at the time, tell a customer that a transaction is being delayed because a report is awaiting a defence (consent) from the FIU
- can tell the customer that law enforcement is conducting an investigation.

14. RECORDKEEPING

The Company keeps all the documents and data collected or obtained within the scope of the due diligence, including:

- all data and information used to identify and verify customers (including type and number of the document, issuing authority, etc.)
- all records (receipts) relating to transactions, i.e., winnings paid out or refunds to customer accounts,
- all documents and records used for the preparation of the risk analysis, the risk analysis itself, including the results of the risk assessment, as well as the documentation on the appropriateness of the measures taken based on these results,
- the results of internal investigations, communication with FIU and regulators,
- documents collected within the scope of business partners due diligence,
- documents collected from the Employees and Staff within the scope of the due diligence,
- documents regarding AMLTF training (training materials, examination results, etc.).

The Company also keeps all documents created and processed in connection with a suspicion of ML / TF / PF, including:

- all related internal and external correspondence,
- file and interview notes,
- the results of internal investigations and the measures taken, that can explain why the money laundering officer concluded and initiated the actions taken.

The retention period is five years and starts with the end of the calendar year in which the business relationship ends and in all other cases with the end of the calendar year in which the respective information was ascertained. Applicable legislation may provide for a more extended retention period.

The Company destroys all the documents and data collected after retention period expiration unless other recordkeeping or retention obligations apply, but not later than after 10 years.

15. TRAINING

The Company will provide training to all Employees and Staff directly or indirectly through a service provider upon joining the Company and thereafter annually.

Relevant training materials will be prepared for all teams based on the company policies which have been compiled according to the applicable legislation requirements and guidelines.

Training will be conducted as follows:

- Training material based on the finalised and approved policies the Company has, in the form of documents and presentations.
- Training will be provided to existing management and staff in a class setting or online.
- Training will also be included in the induction of all new staff.
- Training will be followed up with a questionnaire to test everyone's understanding.
- Should the Company find that some issues are not clear we will repeat the training focusing on the issues that were not understood.
- Regular refresher training will be given, which will include any updates and will focus on any shortfalls that arose during the previous period.
- Any update in policy will be communicated in a group email and through ad-hoc training, and added to periodic training updates and material.

Staff training will focus on ensuring awareness of:

- all applicable legislation,
- the provisions of the money laundering and terrorist financing requirements,
- staff personal obligations under the money laundering and terrorist financing requirements,
- applicable internal reporting procedures,
- Company's policies and procedures to prevent money laundering and the financing of terrorism,
- Company's identification and verification procedures, record-keeping, and other procedures to prevent money laundering and the financing of terrorism,
- recognition and handling of suspicious transactions,
- Staff personal liability for failure to report information or suspicions under the money laundering and terrorist financing requirements and the Company's internal procedures; and
- New developments, including information on current techniques, methods, and trends in money laundering and the financing of terrorism.
- The money laundering and terrorist financing risks faced by the Company
- Data protection regulations.

Induction training sessions will be conducted for all employees and will include fraud prevention, detection and ancillary matters, as required by their role. Refresher training will also be provided, both on a regular basis and as needed, so as to keep employees up to date and informed of the Company's policies and procedures and any changes or improvements made.

The Money laundering Officer keeps records of training delivered, showing what training has been provided, when and by whom, and the next training date. In case of any changes to the Company's policies and procedures or applicable legislation, all staff will get the relevant training.

16. EMPLOYEES BACKGROUND CHECK

Prior to engaging Employees and Staff, the Company will carry out relevant integrity checks, in-line with their position, responsibilities and access levels. The Company will not employ any persons who are not deemed to be fit and proper. To assist with its review, the Company may request the following documents (in each case with due regard to data protection):

- a valid original identity document,
- CV,
- any other documents as the Company deems necessary to request.

Once a person is employed / contracted, screening shall be carried out on an ongoing basis as required. All Company's employees must guarantee that they observe the provisions of applicable legislation and the associated due diligence obligations, report facts relevant to ML / TF / PF, and not themselves participate actively or passively in dubious transactions.

Senior management will regularly carry out checks on Employees and Staff whenever the Company feels the need to perform such inspections. In particular, such inspections shall be carried out when suspicion arises concerning the behaviour of specific Employees or Staff members. The Company may carry out these checks through surprise spot checks or other procedures that will enable such personnel to verify whether Employees or Staff members comply with the policies and procedures.

The frequency and extent of screening that shall be carried out shall be proportionate to the risk level posed by the Employee or Staff member. The risk level will be determined case by case depending on the Employee or Staff member's position (e.g., head of dept, senior, mid), the scope of duties and obligations, etc.

The Company will check all Employees and Staff members at least once a year. The Company will use a performance review for this purpose.

17. AUDIT

The AMLTF compliance program will be monitored and evaluated at least annually by an external independent party. The audit will be independent, thus performed by people not involved with the Company's compliance team. Those performing the audit will be sufficiently qualified to ensure that their findings and conclusions are reliable. These tests will include:

- An evaluation of the institution's AMLTF Policy and manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable AMLTF laws and regulations;

- Evaluation of the system's ability to identify unusual activity;
- Interviews with Employees and Staff members who handle transactions and with their supervisors;
- A sampling of unusual transaction on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

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

18. EXAMINATION BY THE GAMING CONTROL BOARD

The Company will provide information or documentation on its money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the GCB in preparation of or during an examination and upon GCB request during the year. The Company will make the following items readily available:

- Written and approved AMLTF Policy;
- Records of its Business Risk assessment;
- The name of each Compliance Officer responsible for the Company's AMLTF Policy and procedures and their designated job description;
- Records of reported unusual transactions;
- Records of unusual transactions which required closer investigations;
- Records of frozen accounts;
- Schedule of the training provided to Employees and Staff members on ML, TF and PF;
- The assessment report on the Company's policies and procedures on ML, TF and PF by the auditors;
- The customer's files including customer risk assessment, CDD, customer acceptance and transaction information.

19. INTERNAL AND EXTERNAL REVISION AND STAYING UP TO DATE

The Company has compiled its policies and procedures according to the requirements of the applicable legislation and guidance of the FATF, GCB and FIU. However, the requirements and guidance, as well as external fraud trends, can and will change. Therefore, the Company has implemented the following measures to ensure the relevance of the Company's internal AMLTF documentation:

- Key personnel have subscribed to mailing lists offered by the FIU, GCB and FATF and joined relevant forums

- The Company periodically takes legal advice from the gambling consultants for AMLTF best practices
- In the case of an update, the Company will take the following steps, as necessary:
 - Update Company's policy documentation and training materials;
 - Inform all relevant Employees and Staff via the internal communication platform regarding the updates, meet with relevant team managers, and ensure they update their teams appropriately;
 - Update email communication templates and chat canned responses;
 - Update website policies, maintaining a version number and 'last update' date;
 - Update the Company's terms and conditions on the Website (T&Cs), maintaining a version number and 'last update' date.

Any consequential update to the T&Cs will trigger a pop-up notification to customers on their next login where they will need to accept and agree to the new version before proceeding.

The Company may engage a third-party service provider with expertise in AMLTF compliance to conduct independent external reviews of our AMLTF Policy and internal procedures. The results of these reviews will be reported to the Board of Directors and senior management and used to enhance our internal AMLTF measures and associated documents as needed. The frequency of external reviews is determined by the Board of Directors. It may be conducted annually or more frequently, depending on the need for an updated assessment of our AMLTF program's effectiveness.

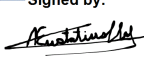
20. APPROVAL & REVIEW

This Policy is approved by the Board of Directors and will be reviewed on an annual basis at minimum, or whenever one of the following cases occur:

- a)** Upon the discovery or recognition by an audit or risk assessment that the Policy requires amendment;
- b)** Upon the change of any relevant law or regulation;
- c)** Upon the finding by any regulator that an amendment to the policy is required;
- d)** Upon acquiring a new product / vertical;
- e)** 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 Employees and Staff members within the scope of the Policy for information of the amendment. Any change to the Policy that gives rise to a new procedure review shall be identified and such changes shall be implemented to the relevant procedure.

For Approval

Signed by:

8737E2B30CF043F...
Analissa Heiland

Signed by:

E9C1A4A3F74E4ED...
Lorenza Godett

Board of Directors

Xecutive Corporate Management B.V.

On behalf of **Raw Entertainment B.V.**

12/12/2025