

AML/CTF Policy

Stake

Key Information	
Approving Official(s)	Head of Compliance
Responsible Office	Compliance Team – MLRO – HR
Effective Date	30 May 2025
Next Review Date	30 May 2026

1. Policy Statement

1.1 In order to prevent customers from exploiting Medium Rare N.V. (hereafter “**Stake**” or the “**Company**”) for purposes of money laundering and terrorist financing, Stake is fully committed to complying with the laws and regulations of its licensing bodies in Curaçao. Stake is not a financial institution within the meaning of applicable laws of Curaçao and is accordingly not directly subject to the statutes and regulations applicable to certain financial institutions, money transfer, or virtual asset service providers. However, in accordance with the 2025 Regulations for Anti-Money Laundering and Combating the Financing of Terrorism (“AML/CFT”)¹ applicable for the Curaçao jurisdiction, as provided by the Curaçao Gaming Authority, Stake expressly prohibits and rejects the use of Stake products for any form of illicit activity, including money laundering, terrorist financing or trade sanctions violations, consistent with various national anti-money laundering (“AML”) laws, regulations and norms. Stake continues to monitor norm setting parameters promulgated by institutions such as the Financial Action Task Force (“FATF”) and certain gaming trade groups in addition to the Curaçao Gaming Authority and will take necessary action as it deems appropriate to reflect changes in law.

1.2 Stake’s intention is to follow global best practices in guarding against Stake products being used to facilitate such activities. Those best practices include:

- The MLRO and the Compliance department to oversee the implementation of the policy, procedures and controls;
- The provision of related training to relevant personnel; and
- The independent reviews from the Internal audit department, monitoring and maintenance of the policy, procedures and controls.
- Engage external third-party Independent professionals to conduct periodic reviews and audits of its AML/KYC policy, procedures and controls.
- Adoption of a written policy, and procedures and controls, reasonably designed to guard against money laundering, terrorist financing and trade sanctions violations.

¹ Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction Applicable to Curaçao casinos and providers of other online games, January 2025

https://gamingcontrol.spin-cdn.com/media/aml_cft/20250110_regulations_for_the_combating_of_money_laundering_and_financing_of_terroris_m_version_january_10_2025.pdf

2. Purpose

This document sets out the obligation of the Company to comply with applicable anti-money laundering and counter terrorism financing regulation, requirements, and best practice, in line with the Company's risk appetite and the risk assessment of the business. These policy requirements are designed to assist in the detection, prevention and deterrence of potential money laundering and terrorism financing in order to prevent customers from exploiting the Company for these purposes.

3. Audience

The policy applies to all departments relevant to preventing AML/CTF efforts, including:

- Senior Management / Board of directors;
- Money Laundering and Reporting officer and Compliance Team;
- Customer facing employees (Customer Operations/Services Team Payments Team);
- Finance and financial partners;
- Marketing and business development.

4. Definitions

The following defined terms are widely used in the industry:

Money Laundering (ML): The process of making illegally-gained proceeds appear legal. This process is generally broken down into three steps: placement, layering and integration, typically involving three stages.

1. Placement: The process of placing unlawful proceeds into traditional financial institutions, through deposits or other avenues.

2. Layering: The process of separating proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveler's checks, money orders, wire transfers, letters of credit, stocks, bonds or purchasing assets.

3. Integration: Using apparently legitimate transactions to disguise the illicit proceeds, allowing the laundered funds to be distributed back to the criminal; integrating the now clean money back into normal use.

Terrorist Financing (TF): while distinct in its ultimate goal of funding terrorist acts, shares some similarities in its process. It generally involves the following stages:

1. Raising: The process of raising funds, which can come from both legitimate (e.g., donations, businesses) and illicit (e.g., criminal activities) sources.

2. Moving: The process of moving these funds often involves similar methods to money laundering, aiming to obscure the trail and reach the intended recipients.

3. Using: The process of using the funds to support terrorist activities, which can include recruitment, training, procurement of weapons, and the execution of attacks. Unlike money laundering, where the aim is to make the funds usable by the criminal, terrorist financing focuses on providing resources for terrorist operations.

Suspicious Activity: Activity conducted by a user or non-user using the institution where there are indications that the persons engaging in the transaction may be doing so for fraudulent or illegal purposes.

Sanctions: Sanctions are activities conducted by the international community to prohibit or constrain activities of the target of the sanctions. For example, they are used:

- To encourage a change in behaviour for a target country or regime;
- To prevent and suppress the financing of terrorists or terrorist acts.
- To apply pressure on a target country to comply with set objectives;
- As an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed.

5. Policy Implementation

The MLRO and the Compliance department are responsible for coordinating the implementation of the AML Policy and the AML program. The Chief Compliance Officer's duties also include developing AML initiatives, working with other stakeholders to revise the AML policy, assessing new regulatory requirements and investigating potentially suspicious or unusual activity. Stake also provides AML training to all of its employees on a regular basis.

5.1 Business Risk Assessment

The Company operates in a highly regulated industry where risk plays a major role in every aspect of the business. Having an effective and appropriate Risk Management Framework where ML/TF risks and the controls that mitigate them are documented and regularly monitored is crucial. The Business Risk Assessment provides guidance to the business on what our ML/TF risks are, how we mitigate them and what improvements can be made to further reduce those risks.

A company that is managing its risk effectively is where everyone is aware of the key risks within their departments, reports their incidents and improves controls to further reduce the risk of ML/TF related incidents occurring.

Whilst risk is a part of every person's role at the Company, the Compliance department's and MLRO role is to:

- identify and create the risk framework;
- document the ML/TF risks across the company;
- maintain the risk register;
- apply a risk based approach and document and rate the controls ;
- Assist the teams and departments with managing ongoing remediation items, decision making and strategy to ensure any gaps in our controls are improved and provide a baseline for ongoing monitoring.

The teams and departments across the Company are responsible for mitigating their risks, recording ML/TF incidents and improving their controls where gaps are identified. The Compliance team will review the Business Risk Assessment document on a regular basis to ensure the risks remain current and reflect the evolving nature of the business, products, and regulatory expectations. The Internal Audit department will provide independent assurance by evaluating the effectiveness of the AML framework, including the risk assessment process, and verifying that appropriate controls are in place and operating as intended.

5.2 Customer Risk Assessment

The Customer Risk Assessment (CRA) evaluates the risk that a specific customer may use our platform for ML/TF, or other financial crimes, and to apply appropriate risk-based measures in response.

The Company employs a “Risk Model” which performs a risk assessment on every customer based on several factors including their betting behaviour, physical location (e.g. Country), depositing and withdrawal behaviour etc. The model operates during the onboarding process and throughout the customer’s lifecycle.

If a Customer meets certain criteria, the model may determine that they are a High, Medium, or Low risk customer, depending on the nature and severity of the risk factors triggered. Classified as “High” risk Customers will trigger the requirement for an Enhanced Due Diligence review to be conducted.

Generally, these reviews require the Company to verify the customer’s source of funds and/or source of wealth to satisfy the Company that these funds are not the proceeds of crime or other illicit activities.

Examples of documents which may be required are:

- Payslips or proof of salary/wages;
- Business documentation to prove business ownership, directorships;
- Bank statements, financial reports to show ongoing legitimate source of funds or wealth;
- Income statements from properties or other investments.

If a customer fails to provide the above requested documentation, their account may be restricted or suspended.

A customer who is determined to be a “Low Risk” based on the model, may require some ongoing review, e.g. some further verification or due diligence checks may be required as per the needs of the Company.

If a customer is confirmed to be either a:

- a) Politically Exposed Person or;
- b) a Sanctioned individual

Then the account will be suspended pending an Enhanced Due Diligence review. Confirmed Sanctioned individuals shall have their account closed. Confirmed PEP will have to go through an internal review to assess whether the individual can be accepted.

5.3 Customer Acceptance Policy

Stake will not accept a and will block the users that:

- a) Do not provide the identification information requested by Stake;
- b) Provide fake identification documents;
- c) Try to use different means to deceive about their location;
- d) Are from restricted or prohibited jurisdictions; or
- e) Are subjected to United States, European Union, or other global sanctions or watch lists;
- f) Are gambling addicted or have mental health issues;
- g) Its source of funds originates from exchanges in restricted jurisdictions;
- h) Stake reserves the right to block and suspend player(s) for any other reasons at its own discretion.

5.4 Customer Due Diligence (CDD)

5.4.1 Stake has adopted a risk based CDD approach to enable it to understand the nature and purpose of the user relationship to its platform in order to develop a customer risk profile. To establish a customer's risk profile, Stake obtains relevant documentation during the account opening process. The nature and extent of this information obtained are aligned with the specific type of account and the services offered by Stake. Stake maintains different CDD for different accounts and services.

5.4.2 For instance, the CDD requires users to go through Stake's customer identification program ("CIP"). The CIP consists of procedures for:

- a) Collecting baseline (e.g., wallet address, email address) information at account creation through Stake's user onboarding portal;
- b) Monitoring the risk profile associated with the underlying cryptocurrency wallet used to fund the user's account;
- c) Reviewing FIAT payment methods to ensure they belong to the account holder;
- d) Maintaining records of the information used to identify the user; and
- e) Determining if a user appears on any list of known or suspected terrorists or terrorist organisations provided to the financial institutions based on the above information.

5.4.3 The above steps are operationalised using the following measures:

- a) *Identity and Age Verification*: A third-party service provider will support Stake's ability to determine the legitimacy of the identification information other KYC materials or information provided and will confirm that the user is permissible. The service provider also will confirm that the user does not appear to be located in a comprehensively-sanctioned or otherwise prohibited jurisdiction and will search global sanctions lists to confirm that the user does not appear thereon using onboarding information such as wallet addresses, name, date of birth and addresses.
- b) *Customer Information*: Stake will collect details on each user to form a reasonable belief that Stake knows the identity of its users commensurate with the user's risk profile. For instance, Stake may collect such details as the wallet address, name, address, country, date of birth, or postal code (collectively, "KYC Information"). Stake will collect any of the above KYC Information prior to issuing a Stake funding address (e.g., QR code) to users. Stake does not presently allow users who are non-natural persons. Stake may, at its own discretion, rely on the performance by another institution of some or all of the elements of our CIP.
- c) *Geo-blocking for Prohibited Jurisdictions*: Stake will require contractual client certifications that, through IP address-based geo-blocking, no gaming services will be offered in countries where such activity is not permitted.
- d) *Geo-blocking for Sanctioned Jurisdictions*: Stake also will require contractual client certifications that such users are not subject to United States, European Union, or other global sanctions or watch lists, including individuals or entities associated with the United States' comprehensively sanctioned jurisdictions, such as Iran, Cuba, North Korea, Syria or the Crimean region of Ukraine. Stake will rely on various risk-based measures to verify these representations including as in the below-described know-your-user ("KYC") measures and through IP address-based geo-blocking. Stake maintains a list of restricted jurisdictions outlined in its T&C which may be adapted from time to time.

- e) *Contractual Prohibitions on Users Onboarding from Prohibited Jurisdictions*: Users are notified at onboarding that Stake does not offer services in restricted jurisdictions. Stake's policy on restricting user activity stems from a combination of its risk, fraud prevention, and AML standards, as well as any assessments associated with the permissibility of its services in certain jurisdictions.

5.5 Ongoing Monitoring

5.5.1 Stake performs ongoing monitoring on its users during their player lifetime in order to detect any behaviours or indicators that might raise suspicions in regard to money laundering and terrorism financing practices. For that purpose, Stake has implemented a set of red flag indicators that help it determine such behaviours and require further action from Stake in assessing the customer information.

5.5.2 Whenever one of those red flags is triggered, the user account will be suspended and Stake will pursue enhanced due diligence. Enhanced KYC diligence under this policy is deemed to include, but not limited to, the provision of:

- a) Full legal name;
- b) Country of citizenship;
- c) Permanent Address (which, for an individual, must be a residential street address);
- d) Identification number (either a taxpayer identification number, or, if unavailable, a passport number and country of issuance, alien identification card number or number and country of issuance of another government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard);
- e) Identification Document; and
- f) Source of Funds or Source of Wealth.

5.5.3 Stake may use a third-party service provider to verify any of the above information as determined to establish a reasonable basis to know the true identity of the user where the user's activity warrants such action.

5.5.4 Stake is firmly committed to complying with economic and trade sanctions programs imposed by jurisdictions in which the firm conducts business. For that purpose Stake established a transaction monitoring program with controls and processes to identify and detect any unusual activity in real time and in its ongoing monitoring.

5.5.5 Stake will conduct ongoing monitoring on a regular basis using rule-based systems developed in-house and others from third-party vendors to review user history and patterns of activity to detect and report any unusual activity as required and to develop and implement any additional controls or limits in its platform.

5.5.6 Stake implemented procedures addressing the following two key components of unusual or suspicious activity management:

- a) identification of unusual activity through methods of identification may include employee and customer identification, law enforcement inquiries, other referrals, or transaction and surveillance monitoring system reports; and
- b) alert management that focuses on processes used to investigate, evaluate and document identified unusual or potentially suspicious activity.

5.5.7 Stake will use the following processes to achieve both goals:

- a) *Transaction Monitoring for Sanctioned or Prohibited Jurisdictions:* Stake may in its reasonable discretion impose certain due diligence requests at user balance withdrawal. Stake presently conducts a mixture of manual and automated transaction monitoring processes to identify “red flag” behaviour. Where such red flag behaviour is identified, Stake may refuse to process any withdrawal attempts or collect additional information from the recipient. Stake will further endeavour to limit any attempted user account funding from prohibited jurisdictions (which are identified in the Stake user facing disclosures and updated from time to time internally) where the associated wallet address indicates that the user or the user’s funds are located in such a prohibited jurisdiction. For instance, Stake may prohibit a user from funding their Stake account using a known U.S. based exchange wallet as such assets indicate that the user is a U.S. person. Users will have the ability to rebut any suspension with additional information as part of Stake’s ongoing transaction monitoring and user due diligence standards.
- b) *Screening for Sanctioned Parties:* Prior to issuing a Stake funding address to a user, Stake will screen a user’s wallet address against applicable sanctions databases. Such screening measures will rely on third-party blockchain forensics vendors such as Chainalysis. Stake will periodically re-screen wallet addresses against such databases.
- c) *Identification of Unusual Activity:* Stake will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to its business. Monitoring will be conducted running regular reports of unusual, high risk, or suspicious user activity.
- d) *Anti-Mixing Measures:* Stake will utilise software designed to detect other suspicious deposit or withdrawal patterns. Such instances will be dealt with on a case-by-case basis, depending on the perceived level of risk. In such instances, a user may be required to explain their methodology and purpose for using the platform.
- e) *Chainalysis Review:* Every single crypto deposit or withdrawal both indirect and direct will run through Chainalysis and will be reviewed for signs of fraud or suspicious behaviour. A user’s account may be suspended and reviewed upon alert of potential illicit behaviour. Sufficient proof of wealth may be requested from high-risk accounts. Stake may refuse to withdraw to certain “high-risk” addresses as determined in consultation with Chainalysis risk scoring.
- f) *Withdrawal Threshold KYC:* Additionally, and independently, every account, wherever or with whomever associated, will be suspended until adequate KYC diligence occurs once that account reaches a withdrawal threshold dependent on the accounts risk characterisation over the life of the account.

5.6 Reliance on third parties to perform customer due diligence.

Additionally to the above mentioned controlling procedures, Stake has also implemented the following procedures to complement its know your customer and ongoing monitoring procedures:

- a. **Ban Evasion Detection:** Stake may utilize third-party service provider software designed to detect the use by one user of multiple accounts. This software relies on detection of links between the same devices used to access multiple accounts. Such instances will be dealt with on a case-by-case basis, depending on the perceived level of risk. In such instances, a user may be required to explain their methodology and purpose for using the platform. Stake accounts are funded by users using local (non-custodial) or hosted (custodial) wallets. In addition to a Chainalysis screening, Stake monitors user activity within the Stake platform and any withdrawals must meet Stake’s and its third-party service provider’s verification processes. Stake further restricts peer-to-peer account

transfers within the Stake platform infrastructure. Any attempts to circumvent this restriction will be treated as a red flag.

- b. **Time Zone Monitoring:** Stake has implemented time zone controls that detects the users device information and crosses it with restricted jurisdiction to understand if they are trying to use geo location software to hide the jurisdictions where they are connecting from.
- c. **Products and Services Review:** Stake will establish additional procedures to avoid facilitating user attempts to exploit the Stake platform. Stake has a robust set of user-facing terms that users attest to in order to utilise the Stake platform. Stake will establish certain additional safeguards to mitigate against the risk of such misuse. For instance, Stake may establish policies or procedures for limiting which user assets can be onboarded to the Stake platform. Stake lists the assets that are available for use on the Stake platform. Stake does not allow the use of anonymity enhancing technologies such as mixers, tumblers, or certain coins and tokens. Where Stake becomes aware that an anonymity enhancing technology is being used on the Stake platform, Stake will disallow such use.
- d. **Vendor Management:** Stake works with reputable third-party service providers as part of its compliance infrastructure. Stake will periodically assess the strength of its key third-party service providers to determine if additional services are needed, the third-party service provider is not performing consistent with its contractual obligations, or if other remedial action is necessary for Stake to comply with this policy. Stake may request information from any third-party service provider as part of its vendor review process.
- e. **Compliance Innovation:** In addition to vendor management, Stake will continuously monitor any non documentary compliance mechanisms to determine their viability for the Stake program. Stake may run test or trial programs on a limited basis with such compliance vendors to determine the effectiveness of such programs. Blockchain native compliance tools include fraud prevention services, on-chain KYC providers, and other tools designed to reflect the technological features associated with blockchain platforms.

5.7 Reporting of unusual transactions

Stake is obliged to report any unusual or suspicious transactions, in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Customers that are identified as being on a sanctions list, linked to money laundering or terrorism financing or other criminal activities will be reported as suspicious activity to the regulator.

5.8 Anti-Money Laundering Compliance program

AML and CTF awareness is integral to the protection of the Company's reputation and to the attainment of its strategic objectives. The AML/CTF policy and procedures are designed to combat financial crime through the detection and disruption of money laundering and the financing of terrorism. Each member of staff has a role to play in ensuring compliance with all regulatory requirements and expectations.

Given the importance of managing the risk of financial crime, the Company has designed and implemented a specific detailed approach for AML/CFT, which are aligned with the principles outlined within this Compliance Policy and Framework. Specifically, the Company has developed:

- An AML/CFT program which sets out the key components of how it identifies, mitigates and manages customer risk through a robust customer identification and verification process;
- An ongoing Customer Due Diligence program, including Customer Screening and transaction monitoring; and
- Senior Management escalation procedures.

6. Compliance and Consequences of Non-Compliance

Based on the new National Ordinance on Games of Chance (LOK) that has officially come into effect on the December 24, 2024 and Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction that came to effect on the January 2025.

Legal Implications: Violations of AML/CTF regulations, which this policy is designed to uphold, can lead to significant legal repercussions for the company and its employees. These may include:

- a) **Criminal Prosecution:** Individuals who knowingly or recklessly violate AML/CTF laws may face criminal charges, potentially leading to substantial fines, imprisonment, and a criminal record.
- b) **Regulatory Fines and Sanctions:** The CGA or other relevant regulatory authorities have the power to impose substantial financial penalties on the casino for non-compliance. As outlined in **Article 13.4 (Corrective Order Subject to a Noncompliance Penalty)** and **Article 13.32 (Administrative Fine)**, the casino may be subject to significant monetary fines for failing to adhere to AML/CTF obligations.
- c) **Corrective Orders and Enforcement Actions:** As detailed in **Title 1 and Title 2 of §2 (Remedial Sanctions)**, the CGA can issue corrective orders, potentially subject to noncompliance penalties or administrative coercion, requiring the casino to take specific actions to rectify violations. Failure to comply with these orders can lead to further penalties and enforcement actions.
- d) **Reputational Damage:** Legal proceedings and regulatory sanctions can severely damage the casino's reputation, leading to a loss of customer trust and impacting its ability to attract and retain business.

Business Risks: Non-compliance with AML/CTF regulations poses significant business risks, including:

- a) **Loss of Licenses:** Regulatory authorities have the power to suspend or revoke the casino's operating licenses if it is found to be in serious or repeated violation of AML/CTF requirements. This would have a catastrophic impact on the casino's ability to operate.
- b) **Restricted Operations:** Regulatory scrutiny and enforcement actions may lead to restrictions on the casino's operations, potentially limiting its ability to offer certain services or engage in specific transactions.
- c) **Increased Scrutiny and Oversight:** Following a compliance failure, the casino will likely face increased scrutiny and more frequent audits from regulatory bodies, leading to higher compliance costs and administrative burdens.
- d) **Damage to Banking Relationships:** Financial institutions may be hesitant to maintain relationships with entities that have a history of AML/CTF non-compliance, potentially impacting the casino's access to essential banking services.

It is therefore imperative that all employees understand and strictly adhere to the requirements of this AML/CTF Policy to protect themselves, the casino, and its stakeholders from these serious consequences.

7. Related Information

The legal frameworks or the ordinances on which of the AML policy and AML practices of Stake.com are listed as below:

- a) National Ordinance of the Identification of Clients when Rendering Services (NOIS).
- b) National Ordinance on the Reporting of Unusual Transactions (NORUT).
- c) The Code of Criminal Law (Penal Code).
- d) Sanctions National Ordinance.
- e) AML/CFT/CFP guidelines issued by the Curacao Gaming Control Board (2025).
- f) The National Ordinance on Games of Chance (LOK).
- g) AML/CTF Policy Template.

Contact Information

For any questions regarding this policy, please contact:

Company name and department : Medium Rare N.V. (" Stake "); Compliance Department

Registered Office: Seru Loraweg 17 B, Curaçao.

Email address: legal@stake.com

8. Policy History

Policy Name: Anti-Money Laundering, Anti-Terrorist Financing Policy

Effective Date: 30 May 2025

Version 1.0