

KYC 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.

1.2 In accordance with the 2025 Regulations for Anti-Money Laundering and Combating the Financing of Terrorism¹ 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.

1.3 To prevent Money Laundering/Terrorism Financing (ML/TF) , Stake implements “Know Your Customer” (KYC) measures which are detailed within this policy and other internal procedures, which are a critical component of Stake’s broader AML/CTF framework.

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_terrorism_version_january_10_2025.pdf

The Company's KYC procedures are designed to verify the identity of customers and assess their risk profile, aligning with international best practices. Stake continues to periodically review KYC policies to be aligned with institutions such as the Financial Action Task Force ("FATF") and Curaçao Gaming Authority, and will take necessary action as it deems appropriate to reflect changes in law.

2. Purpose

This document outlines Stake's obligation to comply with all applicable AML/CTF regulations, requirements, and best practices. The core purpose of these policy requirements, including an effective KYC framework, is to significantly enhance the detection, prevention, and deterrence of potential money laundering and terrorism financing activities. By implementing these KYC measures and technology controls, Stake aims to prevent customers from exploiting Stake for illicit purposes. These KYC procedures and measures are essential to understanding who Stake's customers are, assessing their risk profiles, and monitoring their activities to ensure compliance with global and local AML/CTF standards.

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 (MLRO) and Compliance Team;
- Customer facing employees (Customer Operations/Services Team Payments Team);
- Finance and financial partners;
- Marketing and business development.

4. Definitions

- **AML** (Anti-Money Laundering): Refers to a set of procedures, laws, and regulations designed to stop the practice of generating income through illegal actions.
- **CTF** (Combating the Financing of Terrorism): Encompasses measures and efforts to prevent the funding of terrorist activities, organizations, or individuals.

- **EDD** (Enhanced Due Diligence): A more intensive level of customer due diligence required for higher-risk customers or activities, involving deeper inquiry into the source of funds/wealth and other verifying documents.
- **FATF** (Financial Action Task Force): An intergovernmental organization that develops and promotes policies to combat money laundering and terrorist financing.
- **IP Geolocation Tracking**: A system that tracks Internet Protocol (IP) addresses to verify a user's access point aligns with their declared country of residence, preventing circumvention of jurisdictional restrictions.
- **KYC** (Know Your Customer): A critical process and set of measures implemented by Stake to verify the identity of its customers, assess their risk profiles, and monitor their activities to prevent money laundering and terrorist financing.
- **MLRO** (Money Laundering Reporting Officer): The designated individual and the Compliance department responsible for coordinating the implementation of the KYC Policy and program, and for developing the KYC Policy to align with preventing ML/TF.
- **ML** (Money Laundering): The process of concealing the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses.
- **PEP** (Politically Exposed Person): An individual who is or has been entrusted with a prominent public function, presenting a higher risk for potential involvement in bribery or corruption.
- **POA** (Proof of Address): A document that confirms an individual's residential address, usually issued by a third party and containing their name and current physical address.
- **POI** (Proof of Identity): A document or set of documents used to verify an individual's identity, typically including their full legal name, date of birth, and a unique identifier.
- **Sanctioned Individual**: A person whose name appears on global sanctions lists, meaning their accounts must be immediately closed to prevent illicit activity.
- **SOF** (Source of Funds): Documentation or information evidencing the legitimate origin of the specific funds being used in a transaction.
- **SOW** (Source of Wealth): Documentation or information evidencing the legitimate origin of a customer's overall economic resources and total net worth.
- **TF** (Terrorist Financing): The provision of financial support to terrorists or terrorist organizations to enable them to carry out terrorist acts.

5. Policy Implementation

5.1 The MLRO and the Compliance department are responsible for coordinating the implementation of the KYC Policy and the KYC program/procedure. The Compliance Officer's duties also include developing the KYC Policy to align with preventing ML/TF. This also includes working with other stakeholders to periodically review this KYC policy, assessing new regulatory requirements, recognising red flags, and adhering to the Company's KYC procedures.

5.2 To ensure full compliance, Stake provides regular AML training to all employees. This ensures that the Company's AML program and KYC procedures are implemented into daily operations. These measurements prevent Stake from financial crime and to thoroughly investigate any potentially suspicious or unusual activity that arises.

6. KYC Process

6.1 The Company's KYC framework is structured into four levels, triggered by customer activity and other risk factors, ensuring that the depth of due diligence corresponds to the associated risk.

6.2 KYC Level 1: Initial Customer Identification

Upon account sign-up, every customer is required to provide foundational identity information. This baseline data collection is critical for establishing a verifiable profile:

- **Full Name:** As it appears on official identification documents.
- **Permanent Residential Address:** A physical street address (P.O. Boxes are not accepted).
- **Date of Birth:** To confirm age and identity to ensure no third party or minors are opening accounts.
- **Place of Birth:** Providing an additional data point for identity verification.
- **Nationality:** Essential for sanctions screening and jurisdictional compliance.
- **Industry/Occupation:** To understand the customer's economic background, potential source of income and risk profile.

6.3 KYC Level 2: Transactional Access Verification

Before a customer can deposit funds, engage in betting activities, or initiate withdrawals, enhanced verification is required. This level focuses on authenticating the individual's identity:

- **Proof of Identity (POI):** Customers must provide a clear, government-issued photo identification document (e.g., passport, national ID card, driver's license etc.)

- **Third-Party Verification:** The provided identification is meticulously verified and reviewed by a specialised third-party tool. This process ensures the authenticity of the document and confirms its legitimate ownership by the account holder, significantly mitigating identity fraud risks.

6.4 KYC Levels 3 & 4: Enhanced Due Diligence (EDD)

As a customer's engagement with Stake evolves, particularly with increased spending or betting volumes, or if other specific risk factors are identified, the relevant team will initiate further Enhanced Due Diligence (EDD). These deeper levels of inquiry are crucial for maintaining an accurate risk assessment and complying with anti-money laundering regulations:

- **Source of Funds (SOF)/Source of Wealth(SOW):** Customers may be required to provide documentation evidencing the legitimate origin of their funds or overall wealth.
- **Proof of Address (POA):** Supplemental documentation, such as recent utility bills or bank statements, may be requested to corroborate the permanent residential address on file.

This multi-tiered KYC process ensures that Stake maintains a comprehensive understanding of its individual customers, preventing misuse of Stake's platform while adhering to stringent compliance standards.

Note: Only individuals are permitted to hold a Stake account; business entities are prohibited. Furthermore, for all Proof of Address documents, Stake does not accept P.O. Box addresses; a permanent residential address is strictly required.

7. PEP and Sanctions

7.1 Upon customer sign-up, every individual's details are checked against independently maintained third party databases. This process aims to identify if a customer's name and date of birth match those of any individuals on global sanctions lists or designated as a Politically Exposed Person (PEP).

- If a customer is confirmed as a sanctioned individual, their account will be immediately closed to prevent any illicit activity.
- If a customer is confirmed as a PEP, their account will be suspended pending a thorough Enhanced Due Diligence (EDD) review. This internal review will assess the individual's risk profile to determine if the relationship can be accepted in accordance with the Company's risk appetite and regulatory obligations.

7.2 To ensure continuous compliance, the Company conducts regular, ongoing checks of Stake's entire customer database. This systematic re-screening process identifies if any existing customer has become a sanctioned individual or a PEP since their initial sign-up.

- Should a customer be identified as a sanctioned individual or a PEP during these ongoing checks, the Enhanced Due Diligence (EDD) process will be immediately initiated. This ensures that any change in a customer's risk status is promptly addressed and appropriate action is taken to mitigate potential financial crime risks.

8. Advanced KYC Measures and Technological Controls

8.1 To enhance the Company's ability to detect and prevent suspicious activities, Stake employs below technological controls:

- **Device Fingerprinting:** Stake utilises advanced device tagging software to identify and track the unique digital fingerprints of devices associated with each account. This technology is instrumental in detecting patterns indicative of fraud, account takeovers, or other potentially high-risk behaviours by linking suspicious activity across multiple accounts or devices.
- **IP Geolocation Tracking:** This is the tool that tracks Internet Protocol (IP) addresses to verify that a user's access point aligns with their declared country of residence. This helps ensure customers are not attempting to circumvent jurisdictional restrictions or mask their true location.
- **Payment Method Verification:** For fiat transactions, the Company verifies that the payment methods used, such as bank accounts, legally belong to the account holder. This direct match between the payment instrument and the registered customer's identity is a critical control against financial fraud and money laundering.
- **Independent Database Verification:** When required, the Company leverages specialised third-party tools to cross-reference and verify customer identity information against independent, authoritative databases. This provides an additional layer of assurance regarding the authenticity of customer-provided data.

8.2 Furthermore, Stake will not accept and will block 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

Stake reserves the right to block and suspend player(s) for any other reasons at its own discretion.

9. 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

10. Policy History

Policy Name: KYC Policy

Effective Date: 30 May 2025

Version 1.0