# AML Policy of Interstellar Entertainment N.V.

Last updated: 31st July 2024

## For Deposits and Withdrawals.

AML Anti-Money-Laundering policy of www.highroller.com and www.fruta.com.

Introduction: www.highroller.com and www.fruta.com are operated by Interstellar Entertainment N.V. ('Company'), bearing Company Registration number 166178, and registered at Groot Kwartierweg 10, Curacao.

Objective of the AML Policy: We seek to offer the highest security to all of our users and customers on www.highroller.com and www.fruta.com, and therefore, the necessary verifications, as depicted in this Policy, are performed in order to ensure the identity of our customers. The reason behind this is to prove that the details of the person registered are correct and the deposit methods used are not stolen or being used by someone else, which is to create the general framework for the fight against money laundering ('ML'). We also take into account that depending on the nationality and origin, the way of payment and for withdrawing different safety measurements must be taken.

Scope: All employees of Interstellar Entertainment N.V. are within the scope of this policy and hence subject to the policy and procedures and must comply with all provisions listed herein. www.highroller.com and www.fruta.com also put reasonable measures in place to control and limit ML risk, including dedicating the appropriate means.

www.highroller.com and www.fruta.com is committed to high standards of anti-money laundering (AML) according to the EU guidelines, compliance and requires management & employees to enforce these standards in preventing the use of its services for money laundering purposes.

The AML program of www.highroller.com and www.fruta.com is designed to be compliant with the following frameworks:

Curacao: National Ordinance on identification when rendering services (LID)

Curacao: Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction

Curacao: National Ordinance Reporting Unusual Transactions (NORUT)

Curacao: Kingdom Sanctions Law (Rijkssanctiewet)

Curacao: National Sanction Ordinance

Curacao: National Ordinance on Offshore Games of Hazard (NOOGH)

EU: "Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering"

EU: "Regulation 2015/847 on information accompanying transfers of funds"

EU: Various regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods

FATF Recommendations (Financial Action Task Force, European Inter-governmental body)

## Definition of Money Laundering:

Money Laundering is understood as:

- The conversion or transfer of property, especially money, knowing that such property is derived from criminal activity or from taking part in such activity, for the purpose of concealing or disguising the illegal origin of the property or of helping any person who is involved in the commission of such an activity to evade the legal consequences of that person's or entity's action;
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from assisting in such an activity;
- Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points before.

Money laundering shall be regarded as such even when the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

## Organization of the AML for Interstellar Entertainment N.V.:

In accordance with the AML legislation, Interstellar Entertainment N.V. has appointed the "highest level" for the prevention of ML: The full management of Interstellar Entertainment N.V. are in charge.

Furthermore, a Money Laundering Reporting Officer (MLRO) is in charge of the enforcement of the AML policy and procedures within the System. For the avoidance of doubt, the MLRO serves the same functions as the Anti Money Laundering Compliance Officer (AMLCO) as defined in the Regulations for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) issued by the Gaming Control Board, applicable for the jurisdiction of Curacao.

The MLRO is placed under the direct responsibility of the general Management.

## AML policy changes and implementation requirements:

Each major change of www.highroller.com and www.fruta.com's AML policy is subject to approval by the general management of Interstellar Entertainment N.V. and the MLRO.

# KYC Policy

## Introduction

The objective of our KYC process is to prevent the casino from being used by criminal elements for money laundering activities, other fraudulent activity that may result in financial losses to the casino and with the general objective to ensure a safe and responsible gaming environment for our players.

## Customer identification and verification (KYC)

## KYC descriptions

a. Basic due diligence

Involves collecting information about the identity of the customer, such as first and last name, date of birth, email address, phone number, postal address before allowing him to complete the registration process.

b. Politically Exposed Persons (PEP) & Sanctions screening

A Politically Exposed Person (PEP) is a term describing someone who has been entrusted with a prominent public function. A PEP generally presents a higher risk for potential involvement in bribery and corruption by their position and the influence that they may hold. Being a PEP is not a concrete indication of ML/FT, however due to the nature of the customer, his transactions should be scrutinized in further detail.

Sanctions lists contain persons, organizations, or countries that are subject to economic sanctions issued by a government or international organization.

The Company incorporated an automated screening technology to carry out PEP and sanctions checks during the signup process.

PEP & Sanction checks are carried out electronically through our service provider Regily.

The Company is subject to the following sanctions lists:

- UN Sanctions List;
- EU Sanctions List;

The Company also subjects itself to the OFAC Sanctions List.

A full list of sanctions lists that the Company screens against can be found in Annex 1.

If any customer details match details of a PEP or a sanctioned person an alert is received in our back office. A Risk agent will perform identity checks such as name, surname, DOB, address, in order to confirm if the registered person is the same as the PEP or sanctioned person.

If any player details match details of a PEP or a sanctioned person, the account activity would be thoroughly investigated. If investigation concludes that it is indeed a real PEP and/or Sanction match, then the account should be permanently closed and any remaining balance will be paid out after the completion of a full KYC and risk assessment.

c. Age verification

We do not allow underage players to register and play with us, the registration process requires the date of birth to be over 18 years of age and will not permit users to input a date which would contradict that.

d. Standard due diligence

The formal identification of customers on entry into commercial relations is a vital element, both for the regulations relating to money laundering and for the KYC policy.

This identification relies on the following fundamental principles:

A player shall be named as verified in accordance with standard due diligence when the customer has sent in a minimum of ID and proof of address, and in majority of cases also a copy of the payment method used on account.

The customer will undergo standard due diligence if any of the following criteria are met:

- The customer requests or attempts to change registered name and/or address details
- The player is deemed as heightened risk from FRAUD, ML, Bonus abuse or any other perspective
- The player has reached 2,000 euro or more in deposits or withdrawals
- Multiple linked accounts have been identified to the player.

If any of the above is triggered on an account then no further withdrawals will be processed until the verification process has been completed. The regular due diligence process would involve the player and his activity being reviewed and categorized as low, medium or high risk.

Depending on the outcome of such a review the level of KYC documentation requirement may vary. The level of KYC documents required from a player is determined by using a risk-based approach, however at this point the minimum would always be to verify the identity and address details with valid and legible documents.

During the standard due diligence process, the user will be asked to upload the below documents:

- Proof of Identity Document: A copy of the passport, identity card or driving license. All four corners of the ID have to be visible in the same image and all details have to be clearly readable. We may ask for all details or documents if necessary, such as a selfie of themselves holding the ID Document.
- Proof of Address Document: A recent utility bill sent to their registered address, issued within the last 3 months or an official document made by the government that proofs your state of residence. To make the approval process as speedy as possible, players should ensure that the document is sent with a clear resolution where all four corners of the document are visible, and all text is readable. An employee may do additional checks if necessary, based on the situation.
- Proof of Payment Document: This request may vary depending on the payment method used on the account. This may be a bank statement (potentially also showing the proof of deposit), a picture of the front and back of a credit or debit card (showing only the first six digits and the last four digits) or a screenshot of an e-wallet.

**<u>Withdrawal KYC Requirements before 2,000 EUR in deposits or withdrawals</u>**

**Before 2K threshold: Closed loop withdrawals can be approved without KYC if:**

A Basic Risk Assessment has been concluded of account activity and the player has been deemed as low risk from an AML, Fraud and Bonus abuse perspective.

**Before 2K threshold: Non-Closed loop withdrawals can be approved without KYC if:**

The player can’t close loop with last deposit method used and;

- A Basic Risk Assessment has been concluded and recorded in account notes and the player has been deemed as low risk from an AML, Fraud and Bonus abuse perspective.
- No inconsistencies have been identified in registered details or IP-address.
- No linked accounts have been identified to the player
- There are no direct and significant financial risk associated with majority of deposits on account

**<u>Withdrawal KYC Requirements at 2,000 EUR in deposits or withdrawals</u>**

**2K threshold reached: Closed loop withdrawals can be approved without Payment related KYC documents if:**

All players who have reached 2,000 euro in either deposit OR withdrawals need to provide a minimum of ID and Proof of address. In case of an exception from providing payment related documents for players with “closed loop” we need to ensure that a basic risk assessment is carried out. We will not require payment related documents at this stage unless;

- No inconsistencies have been identified in registered details or IP-address

- Account deemed as low risk
- A basic assessment has been carried out and been recorded on account to determine basic Fraud, AML and bonus abuse risk
- Player do not have any linked accounts
- There are no direct and significant financial risk associated with majority of deposits on account

**2K threshold reached: Non-Closed loop withdrawals**

In this instance as a general guideline we should obtain ID, Proof of address and proof of payment ownership. We may ask for additional details such as the proof of deposit.

Things to consider at this stage:

- A basic risk assessment should be carried out
- If we can verify ownership of a payment method used via the Payment Provider back-office then we may not need to request a copy of it (for example. Zimpler)

## e. Enhanced Due Diligence (Source of funds)

The player will undergo enhanced due diligence if any of the following criteria are met:

- The player has received a positive match in our PEP and Sanctions screening which is deemed as accurate.
- Total deposits of 80,000 EUR or currency equivalent
- The player is deemed as high risk when undergoing the standard due diligence step
- The player has deposited substantial amounts in a short period of time and is considered high risk for any other reason.

  The player will be asked to answer the following questions
- What is your employment status? Employed/Self-employed/Unemployed/Other…
- What is your primary occupation?
- In which bracket does your annual income fall? EURO: 13000 - 30000, 30001 - 45000, 45001 - 60000, 60001 - 80000, 80001 - 100 000, 100 000 - 150 000 and 150 000+
- How are you funding your deposits at HighRoller/Fruta? Salary/Savings/Casino Winnings/Credit or loans/Other
- Do you own your residential property?
- Do you have any other sources of income? Please list them below:

The player will also be asked to upload supporting documents in form of:

- Salary/Wage
- Savings
- Inheritance/Gift

● Retirement/Redundancy

● Sale of Property

● Sale of Assets/Company Sale

● Sale of Shares

● Business profits

● Other (Player need to specify)

It is critical that the origin and legitimacy of that wealth is clearly understood. If this is not possible, an employee may ask for any additional document or explanation.

## Risk management:

## Additional measures

*Enterprise-wide risk assessment*

As part of its risk-based approach, Interstellar Entertainment N.V. has conducted an AML “Enterprise-wide risk assessment” (EWRA) to identify and understand risks specific to Interstellar Entertainment N.V. and its business lines. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services the website offers. The Users to whom services are offered, transactions performed by these Users, delivery channels used by the bank, the geographic locations of the bank’s operations, customers and transactions and other qualitative and emerging risks.

The identification of AML risk categories is based on Interstellar Entertainment N.V.’s understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.

The EWRA is yearly reassessed.

## Ongoing due diligence

It is understood that active player accounts will need to be reviewed on an ongoing basis and on a risk-based approach to ensure that the documentation and player profile data held on file is reflective of the present player circumstances.

## Country & Geographical risk

Some countries pose naturally a higher money laundering and terrorist financing risk than others. This is something we have taken into consideration when excluding players from high-risk jurisdictions. All restricted countries from which we do not allow players from, are clearly detailed in our terms and conditions clause 4.1.3. This list of countries is assessed on a regular basis. In order to mitigate this risk, the list of countries in the registration process is restricted to make available only those countries that are allowed to register an account. Other restricted or prohibited countries are removed from the registration process.

## Ongoing Transaction monitoring

The Risk and fraud team uses both external and internal fraud prevention solutions which combine real time monitoring with aggregated reports for manual review.

Our internal risk and fraud management system provided by our platform provider Pragmatic solution offers different rules to highlight suspicious activity on player accounts in real time.

Besides from above we also have via our platform provider and analytic Business intelligence tool “BI+” multiple live reports and aggregated retrospective reports to highlight gaming activity, monetary activity and login activity.

As an extra layer to the above more traditional fraud prevention systems we also have fraud prevention rules setup with our payment gateway provider PaymentIQ to highlight and reject in real time any suspicious transactions. We also use a third party tool called Flows for real time alerts and transaction monitoring.

## Transactional monitoring: Deposits & withdrawals

The Risk & Fraud team and any other trained staff reviews all incoming deposits and withdrawals seven days a week through alerts and daily reports. The monitoring of card deposits and other payment methods with direct financial risk along with large deposits are given preference and extra attention in these checks.

## Deposit patterns & withdrawal patterns:

The selection of transactions to investigate is done using a risk-based approach where things such as deposit value, country of deposit, country of payment method, KYC level, and deposit pattern is taken into account.

The deposit patterns are checked for:

- **Velocity deposits** - Multiple deposits carried out on a single account within a very short time frame
- **Structuring** - Instead of making a single deposit of a substantial amount (example 2,000 EUR) the player is depositing ten transactions of 200 EUR in hope that the player won't trigger any single deposit alert and raise suspicion
- **Multiple payment methods** - The player is successfully or attempting to make deposits with multiple payment methods
- **Geo data discrepancies** - The IP and/or the registered country of the player does not match with each other or the issuing country of the payment method used.
- **Positive balance top up** - Player is carrying out additional deposits despite having a positive balance
- **Non closed loop withdrawals** - The player attempts to withdraw to a payment method different than that used to fund his gaming account.
- **Substantial deposit / withdrawal amounts** - The player has deposited or is attempting to withdraw a substantial amount on his gaming account.
- **"Anonymous" payment method** - Substantial deposit with the use of vouchers, prepaid cards, wallets and/or crypto currency.
- **Third party usage -** Player have used what appears to be a payment method belonging to someone else.

## Alerts and Reports

All Risk & Fraud staff have been trained and have been provided documented guidance on how to identify inconsistencies, how to identify suspicious activity and how to make a selection of accounts to review and how to subsequently carry out a risk assessment of such accounts.

The rules and alerts in place are reviewed daily and one of more of the following actions will be taken:

- Perform a basic, simple or extensive risk assessment
- Highlight a positive match for review, but take no other action.
- Highlight a positive match for review and restrict further deposits.
- Highlight a positive match for review and restrict any further withdrawals.
- Highlight a positive match for review and suspend account

As part of the ongoing monitoring, there are rules in place to detect potential collusion, wherein the specialized Risk & Fraud employees would then investigate whether there is a potential case of collusion. This is done by:

- Manually analyzing transaction patterns to identify any unusual activity.
- Analyzing customer behavior for inconsistencies or anomalies that deviate from their typical patterns.
- Extracting reports based on criteria to identify possible fraud groups.
- Conducting a thorough review of the account to identify any potential third-party usage.
- Providing ongoing training for the Risk & Fraud team to recognize and respond to collusion.

## Third party usage

"Third party usage" is the wording used to categorize deposits and withdrawals which originates from a payment method which is not owned by the registered player.
Whilst it is true that most third party usage happens with the owner of the payment methods' permission (ex. a Friend/Spouse borrowing the card to player), we do not allow this as with such usage there is a heightened risk of ML and Fraud which we take very seriously to prevent.

Any player identified using third party payment methods will be subject to an in-depth risk assessment where the account may get suspended and where the player is contacted and reminded about our terms and condition clause 11.3 and subject to KYC requests in accordance with our internal guidelines for third party usage.
In the event that the Player was found to have used deposit methods pertaining to a third-party, any winnings deriving from such deposits shall be confiscated. Any remaining deposits shall be returned to the same payment method used for the deposit. Any losses will not be returned.

## Game related risk

The Company offers only casino products with game types such as slots and table games which in general is considered as lower risk as it involves playing against the house (the casino) and not against other players such as poker where a deliberate transfer of funds can occur between two players. However, the Company recognizes that games such as Roulette and Baccarat do carry a
heightened risk for the sessions where you are betting together with other players such as live casino tables. The primary risk in these two game types is "Opposite Betting" whereas two or more players would bet on opposite outcomes and in that way ensuring that funds are transferred one way or another. A typical example of this on the roulette table would be if player A would bet on red and Player B would bet on black.

## AML training

All employees of Interstellar Entertainment N.V. have received adequate training in AML to ensure that everyone has basic knowledge and understanding of what Money laundering and terrorist financing is, how an online casino can be used for such said activities and how to report any suspicious activity.

The training and awareness program is reflected by its usage:

- A more in depth AML training program in accordance with the latest regulatory evolutions, for all staff involved with Payments, Fraud, AML and Risk Management processes

- AML learning sessions for employees are given on a risk-based approach depending on such employees' roles and responsibilities.

The content of this training program has to be established in accordance with the kind of business the trainees are working for and the posts they hold. These sessions are given by an AML-specialist working in Interstellar Entertainment N.V.'s Risk, Fraud and AML team.

## Reporting of Suspicious transactions

In its internal procedures, Interstellar Entertainment N.V. describes in precise terms, for the attention of its staff members, when it is necessary to report and how to proceed with such reporting.

Reports of atypical transactions are analysed within the AML team in accordance with the precise methodology fully described in the internal procedures.

Depending on the result of this examination and on the basis of the information gathered, the Risk and Fraud team will escalate the transaction by filing a Suspicious Transaction Report (STR) to the MLRO:

- will decide whether it is necessary or not to send a report to the Curacao FIU, in accordance with the relevant legal obligations;
- will decide whether or not it is necessary to terminate the business relations with the customer.

## Tipping off

At no time should anyone inform the player that a suspicious transaction has been reported, if a transaction or player has been reported to the MLRO then that report should not be disclosed to any other staff than to MLRO and management.

At no time should anyone indicate to third parties that a particular transaction has been reported as suspicious or that information has been requested by the Police on a particular transaction whether or not such transaction was reported as a suspicious one.

MLRO is aware that he may publish information relating with the suspicious transactions/data only to:

1. The management board of Interstellar Entertainment N.V. and employee appointed by the management board;
2. Financial Intelligence Unit;
3. Investigation authorities during the criminal procedure;
4. Court on the basis of the judgement or regulation.

## Record keeping

Records of data obtained for the purpose of identification must be kept for at least ten (10) years after the business relationship has ended.

Records of all transaction data must be kept for at least ten (10) years following the carrying-out of the transactions or the end of the business relationship.

These data categories will be safely encrypted and stored offline and online.

## Auditing

Internal audit regularly establishes missions and reports about AML activities.

The Company shall subject itself to an independent AML audit at least once every 18 months.

## Data Security:

All data given by any user/customer will be kept secure, will not be sold or given to anyone else. Only if forced by law, or to prevent money laundering data may be shared with the AML-authority of the affected state.

Interstellar Entertainment N.V. will follow all guidelines and rules of the data protection directive (officially Directive 95/46/EC)

## Employee Screening:

Once a potential applicant applies to an open job requisition online, the Head of HR and managers/team leaders will review applications to find suitable candidates for the posted job.

Each of the applicants chosen by the Head of HR and managers/team leaders are then contacted to schedule a virtual interview. Candidates who are chosen to move forward in the interview process following the virtual interview, will be asked to attend an in-person interview with team leaders/managers if they are located within the same jurisdiction.

After all interviews with the candidate have concluded, feedback is gathered from each of the interviewers to determine whether to move forward with an offer letter.

Reference letters or confirmations are obtained depending on the level of the role and/or queries identified in the CV. An online search about the candidate is also done by HR.

After a candidate has completed the interview process and has been selected for a job offer, the Head of HR will request that the new employee send their ID, proof of address, and present police records / conduct.

The Company undertakes employee screening by:

- Verifying that the employee has a clean police conduct on employing them with the Company;
- Undertaking a Google Search to verify if there is any adverse media relating to the individual;
- Carrying out screening with screening software to ensure there are no sanctions, PEP hits or potential adverse media on the employee.

Records of all such searches are saved on file and such searches are repeated on at least an annual basis.

## Contact us:

If you have any questions about our AML and KYC Policy, please contact us:

- By email: support@highroller.com or support@fruta.com

If you have any complaints about our AML and KYC Policy or about the checks done on your Account and your Person, please contact us:

- By email: support@highroller.com or support@fruta.com

## Review

This Policy shall be reviewed on at least an annual basis or sooner should there be any substantial change to the operations of the Company.

AML Policy reviewed and signed by the Company Director:

C Drommond

Name: eMoore N.V. Title; Managing Director

Repr. By: Cornelia Drommond – Oomincx

Date: July 31st, 2024

eMoore N.V.
P.O. Box 422
Curaçao
Tel.+5999 7471401