

HIGH ROLLER



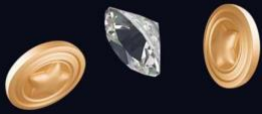
AML/CFT Policy

Highroller

May 2025

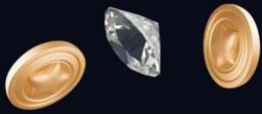
Versio n	Date	Modifications	Updated by	Approved by	Status
1	May 2025	Initial draft	Dirk Urpani	Board of Directors	

HIGH ROLLER



Contents

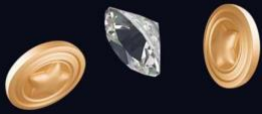
Contents	2
Sources	4
Abbreviations	4
Scope	5
What is the Offense of Money Laundering (ML)?	6
Knowledge vs. Suspicion	7
Objective Test of Suspicion	8
Funding of Terrorism “FT”	8
The FATF	8
Money-Laundering Reporting Officer	8
Detailed Responsibilities	9
Purpose and Obligations	10
Onboarding Process	11
Registration	11
Initial PEP and Sanctions Screening	12
Types of Players not accepted for establishing business relationships	13
The Onboarding Risk Assessment Flow	15
Due Diligence	15
What is CDD?	16
Identification and Verification Procedures	16
Review of Due Diligence Documentation	19
Inability to complete CDD	20
Purpose and Intended Nature of the Business Relationship	21
Source of Wealth and Source of Funds	22
Certification of Documents	23



HIGH ROLLER



Ongoing Monitoring	23
Duplicate Accounts	25
Incoming Deposit Monitoring	27
Withdrawal procedure	28
Enhanced Due Diligence	30
Data Protection	32
Business Turn Away	32
Client Termination Procedure	32
Risk Assessment and Risk Management	32
Risk Assessment	32
Identifying and Handling Suspicious Transactions	33
Identification of Suspicious Transactions	33
Handling of Suspicious Transactions	34
Non-Disclosure / ‘Tipping Off’	34
Complex and/or Unusually Large Transactions	35
a. EDD in Relation to Complex and/or Unusually Large Transactions	36
b. Internal Report	36
Dealing with Non-Reputable Jurisdictions & High-Risk Jurisdictions	36
Determining Non-Reputable Jurisdiction	36
Determining High-Risk Jurisdictions	37
FATF Public Documents	37
The European Commission Delegated Regulations Identifying High-Risk Third Countries 44	38
Assessing and Managing the ML/FT Risk Posed by Non-Reputable Jurisdictions and High-Risk Jurisdictions	39
Restricted Countries	40
Reporting	40
Internal Reporting	40
External Reporting	41



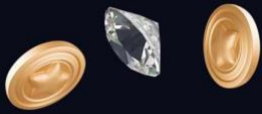
Record Keeping	42
Training	43
Content of Training	44
Training Records	44
Appendix 1 – PEPs and Sanctions Screening Procedure	44
Appendix 2 – Examples of Documentary Evidence	45
Appendix 3 – SOWQ	45
Appendix 4 – Guidelines for disclosure of Source of Wealth and Funds	46
Appendix 5 – Internal Customer Review form	46
Appendix 6 – Internal Customer Review Procedure	49
Appendix 7 – KYC Process	49
Appendix 8 – EDD Procedure	50
Appendix 9 – Restricted Countries List	51
Appendix 10 – Internal Reporting Form	52

Sources

Financial Action Task Force, Recommendation – www.fatf-gafi.org

Abbreviations

AML	Anti-Money Laundering
CDD	Client Due Diligence
DD	Due Diligence
EDD	Enhanced Due Diligence
SDD	Simplified Due Diligence
CFT	Counter Funding of Terrorism



HIGH ROLLER



CRA	Customer Risk Assessment
CRAM	Customer Risk Assessment Methodology
BRA	Business Risk Assessment
JRA	Jurisdiction Risk Assessment
JRAM	Jurisdiction Risk Assessment Methodology
LOC	Letter of Comfort
CFT	Combating Funding of Terrorism
EU	European Union
KYC	Know Your Customer
FATF	Financial Action Task Force
PEP	Politically Exposed Person
STR	Suspicious Transaction Report
T&Cs	Terms and Conditions
SOF	Source of Funds
SOW	Source of Wealth
SP	Subject Person
OE	Obligated Entity

Scope

Interstellar Entertainment N.V. (“Highroller”) is a company registered under the laws of Curacao with registered office at Groot Kwartierweg 10 Livestrong building, Curacao. The Company is licensed in Curacao.

To this effect, the regulatory frameworks under laws of the Applicable Jurisdictions would apply to the Company and its employees. Specifically, in relation to the prevention of money laundering (‘ML’), proceeds of crime and funding of terrorism (‘TF’), reference should be made to the following frameworks.

- Curacao Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction
- FATF Recommendations.

These policies and procedures (“AML/CFT Policy”) are subject to annual review and should also be reviewed in the light of industry developments. The objective of this document is to establish and maintain policies, procedures and controls which deter criminals from using the Company’s facilities for ML and FT.

This AML/CFT Policy is subordinate to the laws of the Applicable Jurisdictions (“Applicable Legislation”) and the Company, the directors, its managers and employees must always refer directly to the Applicable Legislation when ascertaining and implementing its AML obligations in terms of law.

What is Money Laundering (ML)?

ML is the process whereby proceeds derived from criminal activities enter the financial system in order to conceal their illicit source and enable criminals to make use of such proceeds. Often business or trade transactions would be used to disguise ML operations and the origin of the proceeds involved.

Money Laundering is generally defined as:

- the conversion or transfer of property knowing or suspecting that such property is derived directly or indirectly from, or the proceeds of, criminal activity or from an act or acts of participation in criminal activity, for the purpose of or purposes of concealing or disguising the origin of the property or of assisting any person or persons involved or concerned in criminal activity;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect of, in or over, or ownership of property, knowing or suspecting that such property is derived directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;
- the acquisition, possession or use of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;
- retention without reasonable excuse of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;

What is the Offense of Money Laundering (ML)?

An act of ML involves three stages:

- (a) the placement stage - The placement stage represents the initial entry of the "dirty" cash or proceeds of crime into the financial system. Generally, this stage serves two purposes: (a) it relieves the criminal of holding and guarding large amounts of bulky of cash; and (b) it places the money into the legitimate financial system. It is during the placement stage that money launderers are the most

vulnerable to being caught. This is due to the fact that placing large amounts of money (cash) into the legitimate financial system may raise suspicions of officials;

- (b) the layering stage - After placement comes the layering stage (sometimes referred to as structuring). The layering stage is the most complex and often entails the international movement of the funds. The primary purpose of this stage is to separate the illicit money from its source. This is done by the sophisticated layering of financial transactions that obscure the audit trail and sever the link with the original crime;
- (c) the integration stage - The final stage of the money laundering process is termed the integration stage. It is at the integration stage where the money is returned to the criminal from what seem to be legitimate sources. Having been placed initially as cash and layered through a number of financial transactions, the criminal proceeds are now fully integrated into the financial system and can be used for any purpose. There are many different ways in which the laundered money can be integrated back with the criminal; however, the major objective at this stage is to reunite the money with the criminal in a manner that does not draw attention and appears to result from a legitimate source.

The crime of money laundering is committed at each stage of the process, and it is not necessary for the illicit funds to go through all three stages.

Knowledge vs. Suspicion

Actual hard knowledge of activities relating to ML is rare to come across. However, knowledge can broadly be sub-divided into 3 types:

- Subjective knowledge: what we think we know as a result of our experiences such as when we know that money came from criminal activity because we overheard a conversation or came across some evidence;
- Wilful blindness: a person purposely ignores what is right in front of them such as when we do not want to ask questions because of the added work involved around the duty to report;
- Recklessly failing to make an enquiry: avoiding the elephant in the room – we fail to make an enquiry that an honest person would make;

All the above reflect situations where it could be proven that we had knowledge about certain activities.

On the other hand, suspicion falls short of proof, based on firm evidence but must also have a factual basis. The formulation of a suspicion is generally a gradual process where one would typically move from a state of comfort, to concern and eventually suspicion.

An event or a series of events arise within a business relationship or by way of an occasional transaction that trigger a concern. This concern should prompt us to:

- Analyse CDD;
- Discuss with our Managers and/or the MLRO;

- Obtain further information from the client whilst ensuring that the player is not “Tipped Off” i.e., alerting the player of one’s suspicion of money laundering;

Following the above, we will either be comfortable with the replies provided or remain concerned, in which case further action is required. If instead we become suspicious, this should be reported internally to the MLRO (in line with the Internal Reporting Procedure).

All of the above needs to be documented.

Objective Test of Suspicion

The objective test of suspicion requires that an employee ought to have become suspicious and represents a greater degree of risk for employees than the test of knowledge and actual suspicion. This test does not require a prosecutor to prove that a person actually suspected that property derived from crime but that a person should have had a suspicion taking into account the relevant information.

If property is derived from crime, the delivery of a service or product may constitute an act of ML, if the person is aware, suspects or has reasonable grounds to suspect criminality. This would give rise to an offence of ML.

The objective test highlights the importance of CDD information.

Funding of Terrorism “FT”

FT can be defined as the offence of terrorist financing involves the provision, collection or receipt of funds with the intent or knowledge that the funds will be used to carry out an act of terrorism or any act intended to cause death or serious bodily injury. It also includes collecting or receiving funds intending that they be used or knowing that they will be used for the benefit of a terrorist group.

The FATF

The Financial Action Task Force (FATF) is an inter-governmental policymaking body whose purpose is to establish international standards, and to develop and promote policies, both at national and international levels, to combat money laundering and the financing of terrorism. It was formed in 1989 to set out measures to be taken in the fight against money laundering. Since then, the FATF has issued 40 recommendations to fight money laundering and 9 special recommendations to fight terrorist financing.

The FATF Recommendations are the international standards set by the FATF to combat money laundering, terrorist financing, and more recently, the financing of proliferation. They cover the comprehensive set of measures that countries should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and other businesses and professions; measures to ensure transparency on the ownership of legal persons and arrangements; the establishment of competent authorities with appropriate functions, and powers and mechanism for cooperation; and arrangements to cooperate with other countries.

Money-Laundering Reporting Officer

The delegated day-to-day responsibility for the AML policy and operation of effective procedures on the MLRO are:

- Establishing and operating appropriate risk-based internal policies, procedures and controls to prevent money laundering or terrorist financing, consistent with legal and regulatory requirements as set out in the Curacao, EU and international provisions;
- Reviewing, updating and approving AML and CFT policies based on an assessment of risk and its management, ensuring that such assessments are kept up to date;
- Ensuring that priority is given to the implementation of AML / CFT policies and taking ultimate responsibility for the development and operation of procedures that implement policy;
- Maintaining up-to-date documentation detailing the risk-based AML/CFT arrangements operated by the Company.

Responsibility for the review and update of the AML Policy, and applicable sections, rests with the MLRO. Each version of the AML Policy will be reviewed and approved by the Board prior to being issued and will carry a review and approval date.

The MLRO may delegate certain functions, in particular those related to the day-to-day monitoring of procedures and systems to detect suspicious activity, to suitable individuals in the Company.

It is the MLRO's ultimate managerial responsibility to ensure that the provisions of this Policy are enforced. Where the MLRO delegates any activities, he will remain accountable for the operation of the delegated functions.

The MLRO may hold other senior management responsibilities within the Company, to the extent that they do not interfere with their ability to conduct MLRO duties.

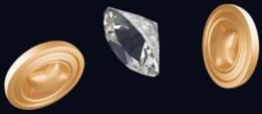
In the absence of the MLRO for a period of less than 12 weeks, the MLRO duties will be temporarily performed by a suitably experienced and qualified individual from within the Company. The MLRO will always remain reachable and in close contact with the head office.

Should the position of the MLRO become vacant (i.e., the MLRO be absent for a period of 12 weeks or more in a consecutive 12-month period), the Board will appoint another suitably qualified individual as its MLRO.

Detailed Responsibilities

Establishing and supervising AML and CFT systems and controls

- Developing and overseeing the implementation of appropriate AML / CFT policies and procedures;
- Determining the level of resources required to execute appropriate AML / CFT policies and procedures;
- Maintaining and developing the risk-based approach to AML / CFT arrangements - carrying out regular assessments of the adequacy of systems and controls;



HIGH ROLLER



- Reviewing the output from the suspicious activity monitoring processes;
- Ensuring that AML / CFT requirements are considered as part of the development of new products or service changes;
- Obtaining Board approval for significant process changes;
- Ensure that policies and procedures are accurately documented in the AML Policy which should be available to staff and used to guide training;
- Ensure that the Board are kept informed of the money laundering risks posed by the business and its activities, and how these are managed and mitigated;
- Reporting to the Board on a regular basis detailing the operation and effectiveness of the systems and controls used to combat financial crime;
- Documenting and ensuring that any actions recommended by the Board are implemented;
- Arranging and assisting with regulatory visits and audit inspections.

Maintaining relevance of the AML systems

- Regularly reviewing developments in applicable legislation and guidance (domestic and international where the business is involved);
- Ensuring that AML/CFT policies are updated to meet changing regulatory and business requirements;
- Ensuring that the operation of systems and controls are monitored and that they implement policy;
- Ensuring that relevant staff are provided with training appropriate for their position (frequency and content) and that all new staff receive training within the specified period. Ensure that training materials remain up-to-date and relevant to the business;

Reporting suspicious activity

- Investigating internal Suspicious Transaction Reports (STRs);
- Deciding, following investigation, whether the internal report gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion and submitting an external STR to the respective regulatory authority, where required;
- Documenting the reasons for not submitting an external STR where an internal report has been made, considered and deemed not to be suspicious;
- Maintain a filing system of all internal STRs, distinguishing between those reported and those that were not reported;
- Ensure that relevant records are retained for the prescribed periods; ● Where required be the main point of contact for law enforcement officials.

Purpose and Obligations

This document was created to provide an understanding of the relevant legislation and obligations as well as to create awareness of the measures required to be followed in the fight against ML and FT.

The provision of AML/CFT training provides a better understanding of the subject and enables employees to identify and handle suspicious transactions.

The obligations of a SP are to:

- a) have in place and implement the following measures, policies, controls and procedures, proportionate to the nature and size of its business, which address the risks identified as a result of the risk assessment, including:
 - i. customer due diligence measures, record-keeping procedures and reporting procedures;
 - ii. risk management measures including customer acceptance policies, customer risk assessment procedures, internal controls, compliance management, communications, employee screening policies and procedures;
- b) take appropriate and proportionate measures from time to time for the purpose of making employees aware of:
 - i. the Company's measures, policies, controls and procedures;
 - ii. the provisions of the Applicable Legislation;
- c) appoint, where appropriate with regard to the nature and size of the business, an officer at management level whose duties shall include the monitoring of the day-to-day implementation of the measures policies, controls and procedures adopted under this regulation;
- d) implement, where appropriate with regard to the size and nature of the business, an independent audit function to test the internal measures, policies, controls and procedures;
- e) provide employees from time to time with training in the recognition and handling of operations and transactions which may be related to proceeds of criminal activity, money laundering or the funding of terrorism;
- f) monitor and where appropriate enhance the measures, policies, controls and procedures adopted to better achieve their intended purpose.

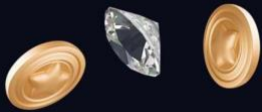
The Company needs to have in place systems and controls that enable it to identify, assess, monitor and manage ML/FT risks and these must be comprehensive and proportionate to the nature, scale and complexity of its activities.

The Applicable Legislation enables the Company to follow and implement a risk-based approach, both in respect of risk management generally, and specifically in respect of customer due diligence measures with the aim of preventing ML/FT.

Onboarding Process

Registration

Players can visit any brand at any time and register as a new player, they are required to provide key information so that we can complete verification and ensure the player is who they say they are and to limit the inherent risks from transactions where the customer is not physically present. Information fields are mandatory during the registration flow so the Company captures the name, DOB and home address which



HIGH ROLLER



can then be verified by obtaining players documents or instantly through integration with a third-party provider.

Before being able to play on the site a customer needs to first register an account. On registration the customer must enter the following details:

- First Name;
- Surname;
- Address;
- Postcode;
- Town;
- Date of Birth;
- Mobile telephone number;
- Password;
- Email Address;

Once the above information is received the team will screen the information for any false or suspicious information, possible duplicate accounts, self-exclusion lists, PEPs and sanction lists. Players from restricted countries are not allowed to register. The IP address from where the traffic originated is tracked by the Company's back-office software. Should traffic originate from countries which are on the list of restricted countries, the account will be blocked.

We do not allow the opening of an account for and on behalf of someone else and players are asked to confirm that they are not wagering on behalf of someone else. Ongoing monitoring is also carried out to ensure that the risk of this taking place is mitigated.

Initial PEP and Sanctions Screening

During the account registration process, the customer's details are screened automatically and cross-referenced with the Sanctions lists within the Infocredit providers using LexisNexis dataset.

Players' details are screened against PEP lists through Infocredit using LexisNexis dataset. Players are then screened regularly against sanctions lists and PEP lists once they have placed their first deposit.

Should any of the customer's personal details be found potentially matching details in the PEP or Sanctions individuals' details, the RPF team will follow the PEPs and Sanction Screening Procedure to mitigate ML/TF risks, including:

- Conducting an initial account and customer review to determine Match / Possible Match / No Match between a customer and a person from the notification;
- Assessing the customer's risk level;
- Requesting identification documents for CDD and EDD;

- Ongoing monitoring of the account;
- Informing senior management of confirmed PEP customers and rejecting the opening of the business relationship; and
- Suspending accounts of sanctioned individuals and informing the MLRO, subsequently the MLRO will pass on this information to the authority responsible for monitoring sanctions.

Further information on the PEPs and Sanctions Screening Procedure can be found in Appendix 1 of this AML/CFT Policy.

The Company's definition of a PEP is derived from the definition provided in Recommendation 12 issued by the FATF, which defines a PEP as:

“A politically exposed person (PEP) is an individual who is or has been entrusted with a prominent function. Many PEPs hold positions that can be abused for the purpose of laundering illicit funds or other predicate offences such as corruption or bribery.”

The below are also to be subjected to the obligations that the Company subjects PEPs to:

- Family Members of PEPs; o The spouse, or a person considered to be equivalent to a spouse; o The children and their spouses, or persons considered to be equivalent to a spouse; and
 - o The parents.
- Close Associates of PEPs:
 - o A natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement, or any other close business relationships, with that PEP;
 - o A natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.

The Company is required to know who its customers are in order to comply with various UN Security Council Resolutions and EU Regulations imposing financial sanctions upon individuals or entities known to be involved or linked to terrorism or the financing or proliferation of weapons of mass destruction. In most cases, these financial sanctions impose requirements on any person or entity to freeze funds and financial assets, therefore, for the purposes of fulfilling such requirements, the Company has systems in place which detect whether applications for business and beneficial owners (on an ongoing basis) are subject to sanctions.

If any player details match details of a PEP or a sanctioned person, an alert is received in our back office where the agent will handle. Identity checks must be completed to confirm if the registered person is the same as the PEP or sanctioned person by checking details such as name, surname, DOB, address.

In the case that a sanctioned person is identified to have opened an account on any of our brands, the account will be closed immediately and the MLRO will be notified through an internal suspicious transaction report. No funds will be returned to the player until approval is granted.

All Players are checked against Sanctions' Lists by the time they register on the website. If a player is on a Sanctions' List, full restrictions are applied on the account, a tag called "Sanctioned" is added & full KYC

is requested. Once received, the account will be forwarded to be reviewed by management for a decision to be made to confirm if we should terminate our relationship with the customer.

Types of Players not accepted for establishing business relationships

The following list details the type of players who are not accepted for establishing a business relationship with the Company;

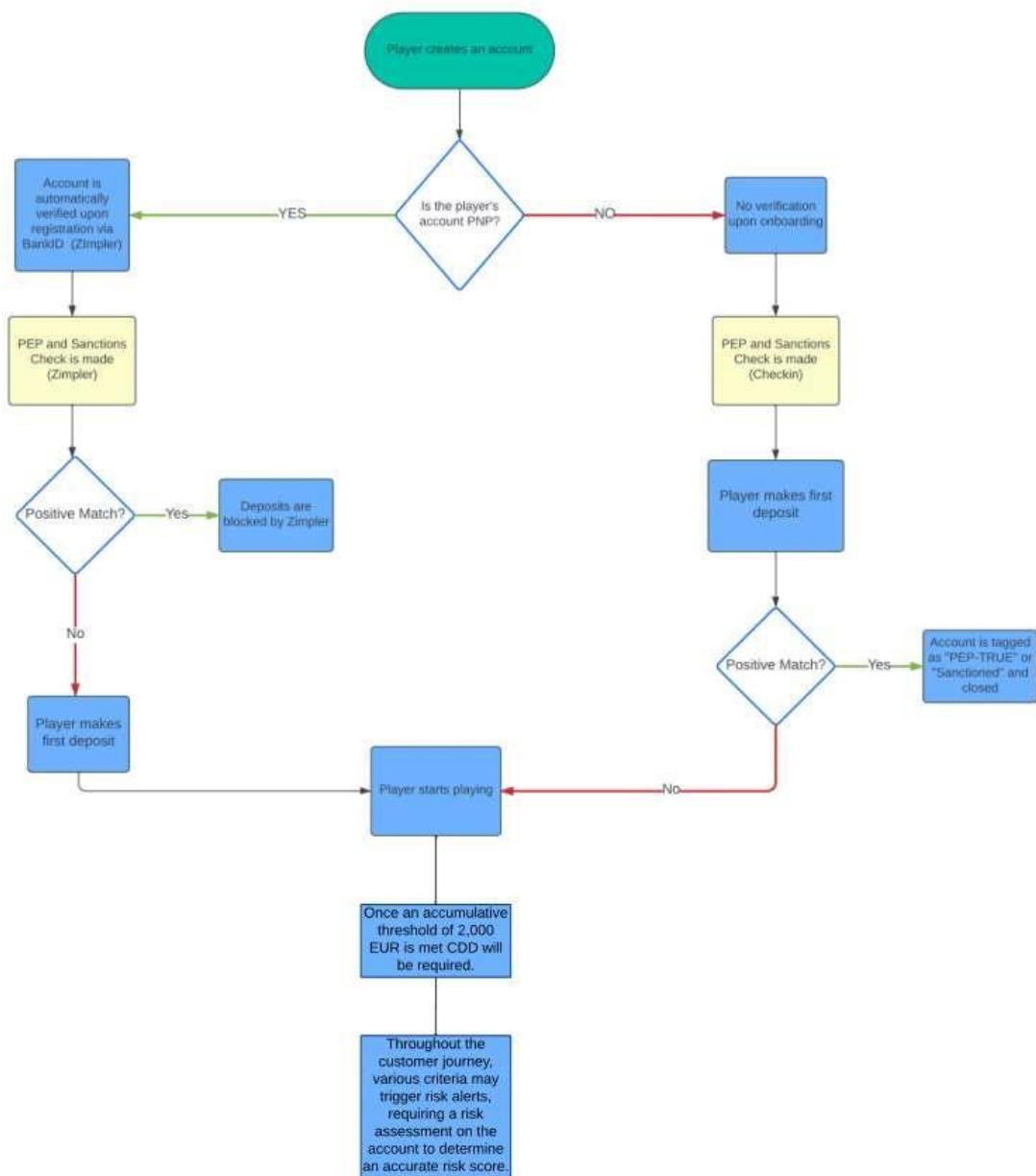
- a) Players who fail to fill in the initial registration form on the website;
- b) Players who ask to open anonymous or numbered accounts or accounts in names other than the customer's name stated in official identity documents or who provide insufficient, unsatisfactory, misleading or seemingly false information and/or documentation;
- c) Players who want to transact in cash;
- d) Legal entities;
- e) Accounts opened in the name of a third person;
- f) Players who provide fake or stolen documents for identification;
- g) Players (or their beneficial owner/s) who are residents, domiciled, established or have involvements/connections to a restricted/high risk jurisdiction in terms of the Jurisdiction Risk Assessment (JRA) and the AML Policy;
- h) Players who were involved in the financing of terrorism or anti-money laundering activity;
- i) Sanctioned individuals;
- j) Persons who are under eighteen (18) years of age;
- k) Players with negative publicity or who are under investigation by a relevant authority;

- l) Players who are classified as Politically Exposed Persons (PEPs) or are close business associates or family members of PEPs;
- m) Players not resident in jurisdictions where the Company is not authorised to provide gaming services;
- n) Players that carry out high risk activities including but not limited to:
 - a. Players associated with criminal activities;
 - b. Players who do not make available clear documentation in relation to source of wealth, source of funds and their origin;
 - c. Players who do not provide the required and relevant information and necessary documentation;
 - d. Players on whom serious adverse or negative information is found;
 - e. Sanctioned individuals and entities;
 - f. Individuals or businesses based in or having strong ties with jurisdictions which the FATF classifies as "High Risk and Other Monitored Jurisdictions";
 - g. Individuals or businesses who refuse to provide the required information or documentation, or which provide conflicting information or forged documentation;
 - h. Individuals or businesses that make it impossible to verify the legitimacy of their activities;
 - i. Individuals involved in illicit activities;
 - j. Player's trading in arms;
 - k. Players supplying technology or parts connected with Defence and National Security;



- 1. Players providing Military Security services.

The Onboarding Risk Assessment Flow



Due Diligence

What is CDD?

The Company is required to carry out customer due diligence on their customers and collect information on the purpose and nature of business to be able to assess the risk profile of the client.

The risk-based approach allows the Company to vary the extent of the CDD measures applied based on the risk presented by the particular client. However, as regards the timing of these measures, it is important that the Company carries out the same prior to the initiation of any business relationship or prior to carrying out an occasional transaction. As an ongoing process the Company should also monitor clients for as long as the business relationship continues. Transactions carried out by the client should be monitored to ensure they are consistent with the knowledge, risk profile and, where applicable, source of wealth and source of funds. Due diligence documentation collected should be kept up to date, for example, identification documents (Passports, ID Cards etc.) should not be expired. CDD measures can be divided into the following categories, each of which shall be discussed in more detail below:

- Identification of the customer, and the verification of the identity of the customer on the basis of documents, data or information obtained from a reliable and independent source/s;
- Assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship, and establishing the business and risk profile of the customer; and
- Conducting ongoing monitoring of the business relationship.

As part of CDD measures, the Company obtains an understanding as to why a prospective customer is seeking to establish a business relationship with them. This consists of determining the purpose and intended nature of the same.

In addition to the above, the Company collects sufficient information, and where necessary, documentation to establish a prospective client's source of wealth as well as the source of funds to be used for his expected outlays. Following the CRA, where the risk is medium or lower, a declaration from the customer with some details can suffice. Where the risk of ML/FT is higher, or the Company doubts as to the veracity of the information collected, the information obtained would need to be supplemented by means of independent and reliable information and documentation.

For more information refer to examples of documentary evidence to be collected to evidence SoW in Appendix 2 of this AML/CFT Policy.

Identification and Verification Procedures

The aim of implementing customer identification and verification of identity procedures is for the Company to be satisfied that it knows, and has verified that the customer exists, and that the customer is who he/she purports to be. This process also seeks to ascertain that the player is not acting anonymously or under a fictitious or stolen identity. The Company will also obtain confirmation from the player that they are playing and transacting on their behalf, through the Company's terms and conditions. The Company has systems in place to detect possible instances where the player is playing on behalf of third parties, whereby the system would check whether withdrawals and deposits would be made to the same credit cards.

The customer/s may be a player, or a group of players ("syndicate") and funds being wagered are collected from multiple persons who share in any winnings, and in such a situation the Company will consider all persons involved as clients, and therefore undertake the necessary CDD measures.

The identification and verification of the identity of a customer needs to be carried out on the basis of documents, data or information obtained from a reliable and independent source. Such procedures should be applied with reference to the ML/FT risks that are posed by the relevant customer; indeed, their application may vary from case to case so long as the Company may demonstrate that the procedures are commensurate to the risk of ML/FT identified through undertaking the CRA.

Identification takes place by obtaining the person's details and other relevant information in relation to that person. Information which must be collected is outlined in the onboarding section of this AML/CFT Policy.

The identification information collected may vary on a case-by-case basis depending on the risk categorisation.

Verification takes place by making reference to documents, data or information obtained from the applicant for business. In order for verification to be completed, the documents obtained from clients need to satisfy the following criteria:

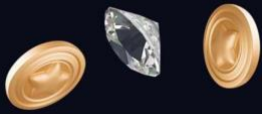
- i. They have to be reliable; and
- ii. Issued from an independent source, such as a government authority, department or agency; a regulated utility company such as telephone companies, water and electricity providers (not a mobile utility company) or any other document the Company may deem fit.

When identification documents of individuals are viewed in original, employees should:

- i. Examine the optical security features that are present on the document and confirming that these can be seen;
- ii. Examine the lamination of the identification document to check for any signs, such as borders around the photographic image of the document or raised surfaces that might be indicative of the fact that the document has been tampered with;
- iii. Check for any uneven document colours and non-uniformity of text, font or typeface that would be indicative of a potentially counterfeit document.

In case of doubt, you can refer to the following sources which can assist in establishing whether the documentation provided is authentic or otherwise:

- i. www.edisontd.net;
- ii. https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/elibrary/documents/policies/borders-andvisas/schengen/docs/handbookannex_23_part_1_and_2.pdf;
- iii. <https://www.consilium.europa.eu/prado/EN/prado-start-page.html>.



HIGH ROLLER



Government-issued documents containing photographic evidence of identity include a valid and unexpired:

- a. Passport;
- b. National or other government-issued identity card;
- c. Residence card; or
- d. Driving license.

When the player is not available for verification purposes (i.e., non-face to face transaction), EDD measures are not mandatory. However, in order to verify the identity of the client, one or more of the following measures to verify the identity of the client:

- i. Obtain a certified true copy of the identification document in order to verify the identity of the client; or
- ii. Obtain two copies of identification documents to verify the identity of the client; or iii.
Require the customer to send a photograph clearly showing the customer's face and the image on the identity document being held in the same picture to demonstrate this actually belongs to the customer; or
- iv. Ensure that the first payment or transaction into the account is carried out through another account held by the same customer in his/her name with a credit institution or a financial institution authorised in a reputable jurisdiction.

For Low and Medium Risk cases the timing and extent of CDD measures can vary. However, in all cases, we verify all our customers when they reach the 4,000 NAf threshold (deposits and/or withdrawals cumulatively amounting to 4,000 NAf since the player first deposited).

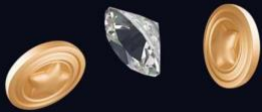
Moreover, to ensure the proper functioning of AML/CFT controls, the first CDD measure – identification and Sanctions screening is carried out upon registration, which includes the collection of personal details. Once a player submits their first deposit screening is done on an ongoing basis.

Upon reaching the 4,000NAf threshold, customers are required to provide documents to verify their personal details collected before. As a rule, verification of identity has to be carried out by making reference to an unexpired government-issued document containing photographic evidence of the customer's identity.

We accept the following documents:

- Proof of Identity:
 - o Copy of Passport;
 - o Copy of National ID or other government-issued identity card;

 - o Copy of Residence Card; o Copy of Driving License.
- Proof of Address:
 - o Copy of a Utility Bill; o Copy of Bank Statements (including mortgage, credit card) o Other Government-issued documentation proving address;
- Proof of Payment Method:



HIGH ROLLER



- o Copy of the credit card used; o Screenshot of e-wallet; or o Recent bank statement.
- Source of Income (Source of Funds / Source of Wealth):
 - o Bank Statement; o Payslip/s;
 - o Income Tax Return;

The lists above are not exhaustive and other documentation may be accepted on a case-by-case basis.

The following systems are in place in order to determine the right timing for the application of CDD measures:

- i. When a user's cumulative threshold (deposits and withdrawals) reaches or exceeds 4,000 Naf, the customer is required to submit KYC (CDD) documentation, that is proof of identity (ID) and proof of address (POA). This will be requested by the RFP team.
- ii. If the customer reaches the specified threshold without having their ID and POA verified, the account will be restricted from making deposits or withdrawals. The customer will only be able to place bets with any remaining balance in the account.
- iii. The users have a 30-day window to submit their documents otherwise they would be at risk of having their account fully limited (Deposits, withdrawals & gameplay).
- iv. After the 30-day window has elapsed, if the account is still not verified, any remaining balance on the account would need to be manually refunded back to the same payment method that was used to deposit if this is technically possible & the account will be fully limited.
- v. If the account is verified during or after the 30-day window, the account will be reassessed and any restrictions can be removed.

N.B. - It is important to keep in mind that the thresholds are considered across all of our existing brands.

Example: If the customer has made a deposit of €1,000 on High Roller & a deposit of €1,000 on Fruta then they are required to submit ID & POA.

Once the 4,000 Naf threshold has been reached and we are notified, we perform a CRA, create a customer risk profile and meet the remaining CDD obligations, through the collection of information such as that obtained through the SOWQ, attached herein as Appendix 3.

- i. Other:

KYC may also requested in the following scenarios:

- Where there is evidence of an IP geo-location mismatch;
- On deposits effected with a 3rd party credit card;
- On certain credit cards that do not contain a card holders name;
- Non-Closed Loop on withdrawal;
- When suspicious activity is detected on the account.

When the player hits €80,000 in lifetime deposits or there are AML concerns about the player's income the Company requests the player to following the EDD Procedure, as per Appendix 8.

Review of Due Diligence Documentation

Due diligence information will be reviewed as follows to ensure that it remains up to date:

- Low Risk Customers: Once every 2 years
- Medium Risk Customers: Annually
- High Risk Customers: Semi-Annually

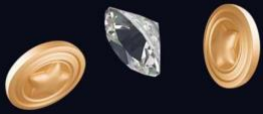
Inability to complete CDD

If the player has not provided the requested CDD within the timeframe set, the following procedure is followed:

- Keep records (in client file) of all attempts made to collect CDD;
- Terminate business relationship with the player, i.e., do not allow any activity of any kind on the account held in the player's name or provide any other service to the player. To this end, the Company may decide to either close the account or to keep it blocked and suspended in its entirety. In the latter case, the Company is to ensure that the account has a NIL balance at the time it is blocked and suspended, with any funds standing to the credit of any such account being disposed of as set out hereunder;
- Consider whether there are any grounds giving rise to suspicion of ML/FT i.e., consider all factors and information on file, including for example the payment method used, the games played, and the customer's playing trends and patterns, any information on the customer already held, including his/her jurisdiction of residence, and information which can be obtained through sources such as the internet etc. If there are grounds to suspect ML/FT, then the Company may decide to submit a STR to the respective authority within the required timeframe;
- Where there are no grounds to suspect ML/FT or the transaction has not been suspended by the respective authority or by operation of the law, nor is there an attachment or freezing order, the Company would have no reason rooted in the AML/CFT regime justifying the retention of any such funds. Thus, where funds are to be remitted back, the Company should:
 - o Consider whether there is any other legal impediment to the remittance of the funds; and
 - o Remit the funds to the same source through the same channels used to receive the funds (if unable to remit the funds to the same source through the same channels, the Company will inevitably have to request fresh instructions from the customer. In the event that these instructions give rise to a suspicion on the part of the Company, it should submit a STR and suspend the remittance pending the FIU expressing its opposition or otherwise to the said transaction);

In the circumstances described above, whenever the Company is remitting funds, it is to also, to the extent that this may be possible, indicate in the script / instructions accompanying the funds that these are being remitted due to their inability to complete CDD.

In the event that the customer makes the requested information and/or documentation available to the Company following the closure or the suspension and blocking of the gaming account, the Company has



HIGH ROLLER



to consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.

HIGH ROLLER

Purpose and Intended Nature of the Business Relationship

The Company is required to assess and, where appropriate, obtain information and/or documentation on the purpose and intended nature of the business relationship. For such purpose, the Company should have a good understanding of how the business relationship will be used to carry out proper monitoring, as well as to be able to determine that the service requested makes sense in view of the player's profile.

The Company is also required to establish the player's business and risk profile. Bearing in mind the principles of the risk-based approach, the Company is additionally required to collect information that will allow it to further strengthen its CRA as well as to have an idea of what it can expect to take place in the course of a business relationship in terms of activity and/or funds transacted using its services and/or products. To this end, the Company must collect information on and, where necessary, verify it with documentation such as:

- i. Information on the nature of and details concerning the customer's business / occupation / employment;
- ii. Any other activity in addition to (i) above from which the customer derives his / her wealth;
- iii. The expected source and origin of the funds to be used throughout the business relationship; and
- iv. The anticipated level and nature including expected value and frequency of transactions that is to be undertaken throughout the relationship.

The Company should refrain from requesting information and documentation that is disproportionate, excessive or irrelevant. Excessive or irrelevant data is data that does not add any value to the business and risk profile, does not serve to mitigate any risks, or does not provide any reassurance relevant to ML/FT risks.

In developing the customer business and risk profile, the Company may consider statistical data to develop behavioural models against which to gauge a customer's activity rather than collect source of wealth information, as per the below sources:

- i. Official economic indicators such as average national income, average disposable income issued by national public bodies or reputable financial institutions. These indications should allow the Company to determine the average wagering power of players from a given jurisdiction; or
- ii. Data collected over a period of time by the Company itself and which allows the Company to create the profile of an average player. This will only be considered by the Company when the customer-base is wide enough to allow the creation of an average profile. This option shall not be used in relation to customers that are deemed to pose a high risk of ML/FT.

The Company shall clearly establish the purpose for the establishment of the business relationship and the extent of activity which is expected from such a business relationship in order to be able to monitor in a proper manner the business relationship.

The nature of information gathered will vary according to the customer's risk profile and the gaming products being used. The level of information to be obtained, and whether this information should be backed up by documents, will depend on the CRA of the particular case at hand.

Where the collection of this information is deemed relevant, the Company should not limit itself to obtaining information of a generic nature, such as business or employment would never be deemed sufficient to meet this obligation, independent of the risk presented. Sufficient detail is to be obtained on the relevant profession, source of wealth and (expected) source of funds in order for the Company to be able to undertake the ongoing monitoring function in a meaningful manner.

Information in relation to the anticipated level of transactions to be expected throughout the business relationship is also required to be obtained. This will help the employees of the Company to monitor in a more meaningful manner the relationship with the client. On an ongoing basis and as part of the transaction monitoring. The Company will monitor the amounts being gambled by the client to ensure that these do not exceed the amounts indicated. Where discrepancies are identified, the necessary clarifications are to be obtained and additional documentation will need to be obtained on a case-by-case basis.

Source of Wealth and Source of Funds

Source of Funds – refers to the activity, event, business, occupation or employment generating the funds used in a particular transaction, or to be used in future transactions. The Company identifies the expected source and origin of the funds to be used in the business relationship depending on the risk classification as per the CRA, and on reaching the threshold set out above, and to undertake ongoing monitoring in accordance with its obligation of ongoing monitoring as described in further detail below.

Furthermore, the Company shall always identify the client's source of funds for a particular transaction if there is knowledge or suspicion that the application for business or the person on whose behalf he is acting may have been, is, or may be engaged in ML/FT whether this is in the context of ongoing monitoring or not.

Source of Wealth - the economic activity or activities that generate the customer's wealth. This may be comprised of, for instance, income through employment or business, or inheritance. The SOW will be identified depending on the risk classification in line with the CRA, and on reaching the threshold as set out above and the information thereon should be updated where new material developments arise in the course of the business relationship.

A risk-based approach should be adopted, and the Company shall consider requesting further supporting documentation where there is a suspicion of ML/FT or where the explanation provided by the client does not make sense or is not convincing. Furthermore, the extent of the information obtained on the SOF and SOW and the anticipated level and nature of the activity will depend on the type of client and such information shall be obtained on a risk sensitive basis.

In all instances, the Company should be satisfied that the client has generated his wealth through legitimate sources. The determination as to whether documentation is to be obtained

shall be determined on a case-by-case basis depending on the risk profile and the circumstances of the customer, including the extent of information which one can obtain through open sources.

In cases where the SOF of the client are generated through an activity which differs from the SOW or the profession/activity of the client, the Company should seek to obtain sufficient information, and on a risk sensitive basis, documentation to verify the source of funds. Judgement needs to be applied by the employee handling the CDD of the client to ensure that the SOF is a legitimate activity and to ensure that the SOF is sufficiently aligned with the risk profile of the client. Any discrepancies are to be thoroughly assessed in order to ensure that the SOF is duly verified.

The Internal Customer Review Procedure, attached herein as Appendix 6, is used to be able to collate all information on a player's income and wealth when undertaking a player review. Guidelines for disclosure of SOW and SOF can be found in Appendix 4, whereas examples of documentary evidence to be collected to evidence SOW can be found under Appendix 2.

Certification of Documents

Where the Company obtains certified true copies of original documents in lieu of the original copy of the particular document, the Company should ensure that the certifications are undertaken by an official of the Company or by a legal professional, accountancy professional, a notary, a person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another reputable jurisdiction. The certification has to be evidenced by a written statement as per the below:

“Certified true copy of the original as seen and verified by the undersigned on the dd/mm/yy”

In case of the documents bearing a photograph, the above statement must be followed by the following statement:

“The photo is a true likeness of (Insert name of individual)”

The certification must be signed in original by the certifier. The certifier must also provide his name, surname, address, contact details (contact number and/or contact email) and capacity.

The Company should ensure that the documents obtained are authentic and have not been forged or tampered with.

Documents in Foreign Languages – Any documentation obtained by the Company which is in a language not understood by the employees of the Company, should be translated. The translation should be dated, signed and certified by an independent person of proven competence confirming that it is a faithful translation of the original, and the original kept on file.

Ongoing Monitoring

The Company is required to monitor the business relationships with its players on an ongoing basis, initially to monitor the point at which the threshold is reached and subsequently on an ongoing basis. This should enable the Company to identify any unusual transactions that may involve ML/FT and ensure that players do not avoid the application of CDD measures by circumventing the threshold, through the Company's systems allowing:

- i. All accounts held by a customer with the licensee are to be linked, irrespective of the platform used or the brand under which the customer makes use of the Company's services; and ii. The detection of the opening of accounts by the same customer but using third party identities, be they real or fake.

The Company's ongoing monitoring obligations will also mitigate the risk of the opening of accounts by persons who input manifestly false details.

Ongoing monitoring of a business relationship involves:

- i. The monitoring and scrutiny of transactions to ensure that they are consistent with the knowledge which the Company has of its clients and the risk profile of the client as established by the Company, including the SOF. In doing so, the Company shall pay special attention to large and complex transactions that have no apparent economic or lawful purpose, unusual patterns of transactions with no apparent economic or lawful purpose and transactions which are particularly likely to be related to ML/FT such as transactions with persons from non-reputable jurisdictions; and
- ii. Ensuring that documents, data or information held by the Company as part of its CDD obligations are kept up to date.

Where such ongoing monitoring reveals a significant divergence between a player's risk profile and the established patterns of activity, for which there is no apparent economic reasons or lawful purpose, the Company shall ensure that the necessary action is taken in accordance with its internal and external reporting procedures.

Transaction monitoring comprises the scrutiny of transactions undertaken in the course of a business relationship to ensure that these are consistent with the Company's knowledge of the customer and of his/her business and risk profile.

Various open-source information is used to conduct the player reviews and are documented including the link/URL of the information found.

If the review is satisfactory, details are inputted in our back office for further monitoring.

If the review is inconclusive, details would be put in our back office for further monitoring.

At this stage the following financial thresholds would trigger EDD.

- Revenue of €80,000 - lifetime deposits minus lifetime withdrawals.

Players may be requested to submit proof of their income.

The following risk factors would constitute as red flags and would thus trigger a review of the player file as part of the ongoing monitoring process:

- High velocity of deposit transactions
- Single deposits with large amount (over €1,000);
- €2,000 deposited within 24 hours; - €5,000 deposited within a week; and - Deposit and withdrawal without playing.

Through the monitoring of customer transactions or activities, the Company should be in a better position to:

- Identify behaviour or transactions that diverge from the usual pattern of transactions that do not fit within the customer's profile, or are otherwise not in line with what is normally expected from the customer, and which therefore need to be questioned in further detail;
- Identify suspicious activity in relation to which the Company may decide to file an STR; and
- Determine whether the initial risk assessment requires updating, and whether, in view of the updated risk assessment or other considerations, the business relationship remains within the Company's risk appetite and, if so, understand whether the level of CDD needs to be adjusted in view of any changes from the initial risk understanding.

The level of data to be obtained should allow the Company to come to a reasonable conclusion on the legitimacy of the transaction, but should not be excessive, disproportionate or irrelevant, and the requests should make sense in the context of the transaction and the player.

Where notwithstanding the information and/or documentation received, the Company is not satisfied with the explanations provided, or the explanation does not make business or economic sense, or there are doubts on the veracity of the documentation provided, the Company has to consider whether there are sufficient grounds to file a STR.

The Company adopts a risk-based transaction monitoring process and screens transactions through:

- a. A risk-based process whereby players that have been classified as being of a high risk to the Company have their transactions monitored more regularly than medium or lower risk players;
- b. Employees of the Company will focus on transactions that in their own right present a higher risk and would exhibit certain red flags;
- c. Obtaining further data throughout the business relationship to build more accurate customer transaction profiles to be able to improve monitoring based on customer transactions trends analysis.

The KYC processes to be followed are detailed in Appendix 7 – KYC Process.

Duplicate Accounts

In-brand Duplicates

Players are only allowed to hold one account in each Brand that falls under Interstellar Entertainment N.V.

Daily, automatic tools are in place, where if a player that could potentially be the same as another player who has an account on one particular brand, an alert would be received in our back office and the agent would handle the alert as per internal processes.

The rules in place to identify potential duplicate accounts are based on a combination of matching criteria between the players:

- Name;
- Surname;
- Date of Birth;
- Address;
- Registration IP;
- Phone Number;
- Email Address;
- Password;

Players which are deemed as duplicates are closed and player is referred to use his existing account.

Checks are in place to ensure that in-brand duplicate accounts are not created or closed.

The team reviews the accounts created in the previous 24 hours that have an in-brand duplicate account identified by the system.

From the alerts received, the team close the accounts that would have “Duplicate accounts” listed as a reason, unless they are automatically closed by the system.

The team also look at both the first account created and the duplicate one to assess the situation accordingly and then decide which account should be kept open or closed and whether confiscation is needed.

Cross-Brand Duplicates

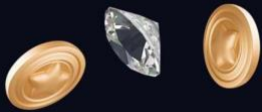
Players can hold one account in each of our brands.

As an extra Fraud Control, automatic tools are in place, where if a player that could potentially be the same as another player who has an account on any of our brands, who has been marked as High Risk, an alert would be received in our back office and the agent would handle the alert as per internal process.

With High Risk we mean players who have been tagged with the following flags:

- Confirmed Fraud Suspect Fraud Bonus Abuse
- Syndicate Betting
- Arbitrage Betting Pending Investigation Gambling Problem Self-Excluded
- Players that are deemed as duplicates or potentially duplicates are handled as per internal procedures.

Alerts are in place that trigger when there is a match for duplicate accounts, strong links between one user and another and when a user has any link to a user who is self-excluded that is reviewed to make sure that the account is not operated by the 3rd party self-excluded user.



HIGH ROLLER



Other Monitoring

Going hand in hand with the above-mentioned monitoring, each account which is deemed as potentially high risk will be assessed manually by the trained agents to determine what action is needed to be taken on the account.

This monitoring and assessment include:

- Account profile
- Linked Accounts
- Country Risk level
- Country, IP, Language, Currency
- Method of deposit
- Method of withdrawal
- Deposit Amount
- Number of deposit attempts in a defined period
- Aggregate number of cards in use in a defined period
- KYC status of the account (verified or unverified)
- Age of the account
- Credit card status (unverified, verified, blacklisted) - Is there a 3rd party payment method in use?
- Date since last activity
- IP shifting
- Change in activity
- Gameplay
- Betting Pattern

The above checks will assist the Company in knowing its customer and actions will be taken depending on the risk identified which could result in:

- Completely Block Account;
- Limit Account until necessary further KYC is provided;
- Escalate player's gameplay to third party provider to check for legitimacy; - Phone / Video call player to verify him; and - Any other action as deemed necessary.

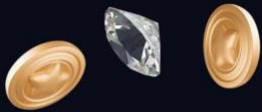
Incoming Deposit Monitoring

Rules are in place in our payment gateway to alert the agents of any deposit, in real time, that could be potentially fraudulent or that needs to be considered.

The alerts go in a queue in our Back Office and the agents handle as per internal processes.

The Rules are based upon the following criteria:

- Credit Card - Deposit with High Balance:
 - o This rule will send a notification when a customer successfully deposits while already having the following as available balance (300 EUR, 10,000 SEK, 10,000 NOK, 300 CAD, 1,000 USD, 300 NZD, 1,000 GBP, 1,000 AUD, 40,000 INR).



HIGH ROLLER



- Credit Card – Velocity:
 - o This rule will trigger when a customer makes a total of 5 successful non 3Ds deposits within an hour;
- All payment Methods - High Depositors
 - o This rule will trigger when a customer makes one or accumulative deposits of €1,000 within 24 hours.

Other Fraud Control & AML Triggers

- Deposit with Balance:
 - o This rule will send a notification when a customer successfully deposits while already having the following as available balance (300 EUR, 10,000 SEK, 10,000 NOK, 300 CAD, 1,000 USD, 300 NZD, 1,000 GBP, 1,000 AUD, 40,000 INR).
- Payment Method Limits:
 - o No rule is included but if the customer exceeds the limit he/she will not be allowed to place a deposit with the new payment method.
- Payment Method in Use:
 - o This rule will send a notification when a customer attempts a transaction with a payment method that is already in use by another customer.

Withdrawal procedure

- A player with a balance on his gaming account can request a withdrawal when he is logged in to his account from the website at any time by going to the withdrawal page.
- Currently, most withdrawals for players go into pending status, meaning that they must be reviewed and processed by the RPF Agents.

To facilitate this process, a set of automatic rules/indicators are in place to help the agents easily identify which withdrawals need more attention.

Automatic Rules/Indicators

- 1st Withdrawal:

HIGH ROLLER

- o Being the first withdrawal more attention should be given to the pay-out. The 1st withdrawal is sent to RPF team for manual review and is not processed automatically.
- Duplicate Account:
 - o Alert will be on if player is linked to other players
- Other Fraud Alerts:
 - o If the customer is linked to a fraudulent account or has met a possible fraudulent criteria an alert will be sent out.
- KYC:
 - o Alert will be on if player should be verified before being paid out

Manual checks done before processing Withdrawals

The above-mentioned indicators help us differentiate between the withdrawals and they are automatically placed in different queues in our back office.

All first withdrawals and other withdrawals that would have triggered any rule or indicator may be checked by the agents. Checks done may include the following:

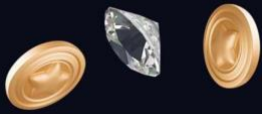
- Account Profile
- Age of account
- Linked Accounts
- Verification of documents received
- Transaction Pattern
- Verification of longevity of customer with the company
- Verification of the number of payment methods used and of the name of their holder
- Verification of the number of and total amount of deposits

- Verification of the amounts deposited and wagered prior to withdrawal
- Verification that withdrawal is being requested to the same deposit payment method
- Provenience of winnings
- A review of the account's gameplay

Once withdrawals are assessed and defined for pay-out, they are put in a separate queue to be processed through our payment gateway.

Most withdrawals will be set successfully to be paid out.

Other times withdrawals might be rejected due to customer not closing the loop, and he will be sent an email to request the withdrawal again to the correct payment method.



HIGH ROLLER



Withdrawal sign-off policy

RPF Agent - Up to Eur 20,000

RPF Senior - Up to Eur 40,000

RPF Team Leader - Up to Eur 100,000

Director of Operations/Chief Operating Officer - Above Eur 100,000

Enhanced Due Diligence

EDD is to be applied whenever the Company identifies any high-risk situations. EDD entails taking more stringent steps in the application of CDD as well as requesting more detailed information on SOW and SOF.

There are certain types of players and certain situations which are deemed to be high risk, independently of the risk assessment results, when the application of EDD measures is required as soon as reasonably possible and irrespective of whether the threshold has been reached or not.

Mandatory high-risk situations;

- i. PEP players, their family members or their close associates;
- ii. Players from high-risk and non-reputable jurisdictions (FATF list and European Commission Third Countries List);
- iii. In situations where the Company develops a suspicion or has reasonable grounds to suspect that activity in the account or a player is linked to ML/FT;
- iv. Where we discover that a player has provided false or stolen identification documentation or information and the Company proposes to continue to deal with the player;
- v. When there are questions on the funding method being used by the player, or when there are doubts as to whether the payment method used actually belongs to the player;
- vi. Where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or a transaction or transactions have no apparent economic or legal purpose;
- vii. When suspicious behaviour is identified through daily fraud controls;
- viii. In any other high-risk situations determined by the Company from time to time, taking into account current trends.

The EDD measures include:

- i. Obtaining copies of the documents to verify the identity and address of a player; ii. Obtaining additional information on the player;
- iii. Obtaining a copy of the second form of identification to corroborate details; iv. Obtaining a photo of “Identification Document + Face”;
- v. Verification of the payment methods used for transactions in the account.

Obtaining information on the SOF and SOW of the player:

- a. SOF – how the funds used for a particular transaction were obtained by the player (e.g., transfer from the bank account owned by the customer or someone else, loan, winnings from the other companies);
- b. SOW – the origin of the customer’s entire body of wealth:
 - i. Business Income;
 - ii. Employment;
 - iii. Inheritance; iv. Investments.
- c. For the list of documentation that can be requested as Proof of Wealth refer to Appendix 2 – examples of documentary evidence to be collected to evidence SOW.

Researching in additional independent, reliable source to verify information provided or made available to the company:

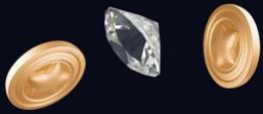
- a) Local or open-source information, such as press reports;
- b) Search in the Infocredit using LexisNexis datasets for any Law Enforcement / Adverse Media.

Taking additional measures to understand better the background, ownership and financial situation of the customer, such as:

- Carrying out an online and media search – Instagram, Facebook and other social media platforms to build the customer’s profile, including looking at available photos online regarding customer’s occupation, hobbies and activities;
- Internet search on the customer’s name, email address and phone number. The information could be useful to see whether the customer’s name is linked to another person’s identity or to some negative publicity, illegal activities etc;
- Google Map Search – in order to check the address, registered in the account and evaluate the financial situation of the player

Increasing the monitoring of the business relationship (enhanced ongoing monitoring), including greater scrutiny of transactions.

The EDD Procedure can be seen in Appendix 8.



Data Protection

Of key importance is the requirement to inform clients about the purpose for collection and processing of personal data and to stringently abide by that specific purpose.

Business Turn Away

In circumstances, whereby one cannot adequately complete customer due diligence or the results are not satisfactory, a business relationship will not be established, or the business relationship will be terminated if it is an existing relationship. No transactions will be carried out with or for that player, subject to MLRO discretion.

The Company shall refuse all potential clients that are captured within the categories as specified in the “Types of customers not accepted for establishing business relationships” Section of the Company’s Customer Acceptance Policy.

Client Termination Procedure

If CDD is not completed within 30 days from a KYC request being made, the Company should terminate the relationship. Employees should keep the MLRO apprised when business is being turned away, and a record of such action kept on file. The MLRO may submit a STR in view of undue secrecy or suspicious behaviour.

A formal termination procedure is required and should be the date used from when the 5-year retention period must commence. In case the relationship is not formally terminated, 5 years will commence from the date of the last transaction.

In case an STR has been submitted and unless advised otherwise, the 5-year period starts from the date when the STR was submitted.

Risk Assessment and Risk Management

The Company has procedures in place for the risk assessment and management of players.

Risk Assessment

Risk Assessment includes the identification and assessment of ML and FT risks posed by the player, service, interface and geographical location. The Risk Assessment process involves, amongst other things, consideration as to whether a client should be accepted and if so whether EDD and other additional measures are required.

The Company has a customer acceptance policy in place for instances when a player is categorised as a PEP or otherwise poses a high risk.

The purpose and nature of the business relationship must always be identified, monitored and recorded in line with the level of risk posed by particular players. In situations where anonymity is part of the service required by the customer, which in turn raises the risk level, obliged entities must not proceed unless they have requested sufficient information to mitigate that risk and are totally satisfied with the legitimacy of the purpose and nature of the relationship and services required.

The Company has in place a:

- Customer Risk Assessment;
- Customer Risk Assessment Methodology; - Business Risk Assessment; and - Jurisdictional Risk Assessment.

The CRA is an assessment of the particular risks the company is exposed to in providing its services or products in the course of a business relationship to a specific player.

The CRAM details how the CRA will take place.

The BRA's purpose is to identify and assess the company's ML and FT threats and vulnerabilities and thus evaluates identified risks to determine priorities for addressing them.

The JRA details how the assessment of the risk posed by a specified jurisdiction will take place and the risk ratings afforded to each country.

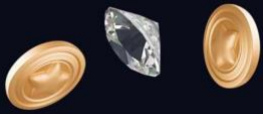
Risk mitigation activities, i.e., the development of appropriate internal controls, flow from the findings of the risk assessments.

Identifying and Handling Suspicious Transactions

Employees should be on the look-out for transactions suspected as being related to ML or FT and should be able to identify and handle such transactions.

Identification of Suspicious Transactions

The following is a non-exhaustive list of possible red flags which the Company considers:



HIGH ROLLER



- Customer does not cooperate in the carrying out of CDD;
- Customer attempts to register more than one account with the Company;
- Customer deposits considerable amounts during a single session by means of multiple pre-paid cards;
- Customer deposits funds well in excess of what is required to sustain usual betting patterns;
- 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 the account of another customer or to a bank account held in the name of a third party; and
- Customer displays suspicious behaviour in playing games that are considered as high risk.

Handling of Suspicious Transactions

If a suspicious transaction is identified or suspected an internal report, on the appropriate form, to the MLRO should be made without delay. Please refer to the Company's internal and external Reporting Procedures. The MLRO will consider such reports and decide how best to proceed.

Non-Disclosure / 'Tipping Off'

Once a transaction is deemed to be suspicious the client must be handled tactfully, never disclosing to the client or a third party that a suspicion arose or that any steps are being taken in that regard. When communicating with the client care should be taken not to tip off the client about the suspicion. In case of doubt, one may always speak to the MLRO of the Company for guidance.

The MLRO is responsible for ensuring that all the employees of the Company are aware of how to prevent 'tipping off'.

Complex and/or Unusually Large Transactions

The Company should be identifying suspicious customer transactions, including:

- unusually large transactions;
- complex transactions; and
- unexpected patterns of transactions that do not seem to have a legitimate purpose.

The Company outlines the risk-based systems and controls to monitor customer transactions while considering its level of money laundering / terrorism financing risk. In this context, transaction monitoring is a key control in the Company's AML/CFT policies and procedures:

- When on-boarding players, the Company is required to perform a risk assessment and due diligence checks to identify and mitigate any prospective ML/TF risks, including proliferation financing risks, at the onset;
- In the case of risks manifesting later, over the course of the player's business relations with the Company, ongoing monitoring should be in place;
- While these risk factors may be obscured at the on-boarding stage and during the Company's performance of regular screening or periodic updates of customer information, they can often be detected through the robust conduct of transaction monitoring.

The Company examines the background and purpose of all complex and/or unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. In this regard, examples may include transactions or patterns of transactions that are:

- Larger than the Company would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs;
- Of an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or
- Very complex compared with other similar transactions associated with similar customer types, products, or services; and the Company is not aware of an economic rationale or lawful purpose or doubts the veracity of information it has been given.

If you identify suspicious complex and/or unusually large customer transactions, you must apply EDD measures and consider making an Internal Report by following the procedure outlined in the Company's Internal and External Reporting procedures.

a. EDD in Relation to Complex and/or Unusually Large Transactions

Where Employees detect complex / unusual transactions / unusual patterns of transactions, they should apply EDD measures sufficient to help the MLRO determine whether these transactions give rise to suspicion. Such EDD measures should at least include:

- Taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and
- Monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail.

b. Internal Report

Internal Reports are made to the MLRO who will consider what action to undertake. The Internal Reporting Procedure can be found in the Company's Internal and External Reporting procedures.

Dealing with Non-Reputable Jurisdictions & High-Risk Jurisdictions

A non-reputable jurisdiction is one that has deficiencies in its national AML/CFT regime or has inappropriate and ineffective measures for the prevention of ML/FT.

In assessing the aforementioned elements, one is to take into account any accreditation, declaration, public statement or report issued by an international organisation which lays down internationally accepted standards for the prevention of ML/FT, or which monitors adherence thereto, as well as whether the jurisdiction has been included by the European Commission in the list published in terms of Article 9 of the 4th AMLD.

One must make reference to KnowYourCountry through which the Company assesses the risk posed by a specified jurisdiction. Website link to KnowYourCountry - <https://www.knowyourcountry.com/ratings-table/>

Determining Non-Reputable Jurisdiction

The list of sources that the Company takes into consideration in this regard is very much exhaustive:

1. Financial Action Task Force (FATF) Public Documents’;
2. Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 Identifying high- risk third countries with strategic deficiencies; and
3. Statements and/or Declarations issued by the FATF or by and FATF-Style Regional Body.

Determining High-Risk Jurisdictions

The factors and sources that the Company takes into consideration in this regard are numerous and non-exhaustive. Below is an indicative and non-exhaustive list of factors and sources:

- Level of Transparency & Rule of Law (e.g., of source/s include Word Justice Project Rule of Law Index, Freedom in the World and Freedom of the Press, issued by Freedom House;
- Level of Corruption (e.g., of source/s include Corruption Index, issued by Transparency International);
- War-torn countries/Civil unrest (e.g., of source/s include UN list of Embargoed Countries);
- Significant level/s & type/s of crime/s (jurisdictions known for high level of different types of crimes, including drug trafficking, arms trafficking, human trafficking, jurisdictions known to be a hub for terrorist groups);
- Significant level of terror threat (e.g., of source/s include the Global Terrorism Index, issued by the Institute for Economics and Peace);
- Mutual Evaluation Report (MERs) issued by the FATF or any FSRB; and
- Other notable sources (e.g., of source/s include the Basel AML Index, issued by the International Centre for Asset Recovery).

FATF Public Documents

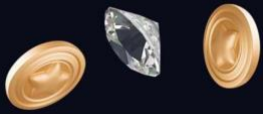
The FATF issues two public documents that provide a list of jurisdictions considered to pose a higher risk of ML/FT in view of a number of identified strategic deficiencies within their respective AML/CFT regime. One of the said lists pertains to jurisdictions currently identified as a call for action and the other pertains to jurisdictions under increased monitoring. It is to be noted that the FATF documents are issued several times a year and, as a result, the list changes depending on the level of progress achieved (or the lack of it) by each jurisdiction in addressing the deficiencies identified in their respect.

Categories identified by FATF, as of June 2024:

Category 1 – Jurisdictions currently identified as call for action:

- North Korea; ● Iran;
- Myanmar.

Category 2 – Jurisdictions under increased monitoring (“greylist”):



HIGH ROLLER

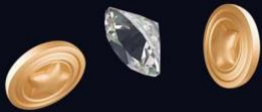


- Algeria
- Angola
- Bulgaria
- Burkina Faso
- Cameroon
- Cote D'Ivoire
- Croatia
- Democratic Republic of Congo
- Haiti
- Kenya
- Lebanon
- Mali
- Monaco
- Mozambique
- Namibia
- Nigeria
- Philippines
- South Africa
- South Sudan
- Syria
- Tanzania
- Venezuela
- Vietnam
- Yemen

The European Commission Delegated Regulations Identifying High-Risk Third Countries

The Commission Delegated Regulations identifying high-risk third countries provide for a list of jurisdictions that can be found hereunder. Therefore, third countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing frameworks are as follows:

- Afghanistan;
- Barbados;
- Burkina Faso;
- Cameroon;
- Democratic Republic of the Congo;
- Democratic People's Republic of Korea (DPRK);
- Gibraltar;
- Haiti;
- Iran;
- Jamaica;
- Mali;
- Mozambique;
- Myanmar;



HIGH ROLLER



- Nigeria;
- Panama;
- the Philippines;
- Senegal;
- South Africa;
- South Sudan;
- Syria;
- Tanzania;
- Trinidad and Tobago;
- Uganda;
- United Arab Emirates;
- Vanuatu;
- Vietnam; - Yemen.

Assessing and Managing the ML/FT Risk Posed by Non-Reputable Jurisdictions and High-Risk Jurisdictions

The Company conducts risk assessments through the use of relevant CRA to manage ML/FT risks posed by its customers, products and services, transactions and delivery channels, as well as countries and geographical areas.

When dealing with natural persons linked with a non-reputable jurisdiction, appropriate EDD measures apply accordingly, when on the basis of risk assessment, it is determined that the

business relationship or any transaction represents a high risk of ML/FT. Needless to say, the requirement to apply commensurate EDD measures in this regard arise when the high-risk level determined is attributed and pushed by jurisdictional links.

The Company may, with respect to business relationships involving non-reputable or high-risk jurisdictions, consider applying the following EDD measures:

1. obtain additional information on the player;
2. obtain additional information on the intended nature of the business relationship;
3. obtain information on the source of funds and source of wealth of the player;
4. obtain information on the reasons for the intended or performed transactions;
5. obtain the approval of the MLRO to establish or continue the business relationship;
6. conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
7. introduce an enhanced, relevant reporting mechanism or systematic reporting of financial transactions; and

8. limit business relationships or transactions with natural persons or legal entities from non-reputable jurisdictions.

Restricted Countries

The Company has a list of Restricted Countries, whereby individuals from those jurisdictions will be prevented from wagering.

The current list of Restricted Countries can be found in Appendix 9.

The list may be extended to include any other jurisdictions in which the Company does not operate or in which the Services are deemed unlawful under the applicable laws.

The list is reviewed periodically and updated whenever necessary.

Players from these countries are not allowed to open an account with us. If any player from any of the restricted countries is identified through IP, account will be closed by the RPF Agent.

Reporting

The Company should be on the lookout for complex or large transactions with no apparent economic or lawful purpose or which are likely to be ML or FT. If a transaction is deemed suspicious, or there are reasonable grounds for such suspicion, the Company's MLRO takes the necessary action. Special attention must be given to business relationships with clients not situated in a reputable jurisdiction.

The purpose of the internal and external reporting procedures is to set out the steps to be followed when an employee of the Company becomes aware of any information or matter that in their opinion gives rise to knowledge or suspicion that a person or transaction is connected to ML or TF.

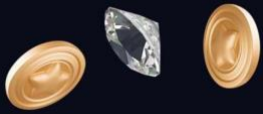
The said procedures describe the responsibilities of the MLRO of the Company, an internal evaluation process and steps of external reporting by the MLRO as well as any necessary follow-up actions.

The below is a brief overview of the steps one should take in case of suspicion of ML or FT matters.

Internal Reporting

Employees should constantly be on the lookout for any suspicious transactions. Once a suspicious transaction is suspected or identified an Internal Report should be made by following the procedure in the Company's internal and external reporting procedures. Internal Reports are made to the MLRO who will consider whether the suspicious transaction requires further action.

On becoming suspicious of a certain transaction, the relevant employee should:



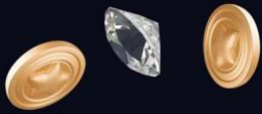
- Flag the main suspect's account;
- Leave a note on the back office stating that if the customer contacts support, he/she should be referred to management, ensuring that there is no reference to indicate that the customer is under suspicion;
- Check for any linked accounts and imposed limits;
- Fill in and submit an Internal Reporting Form, as per Appendix 10;
- Send the completed forms to dirk.urpani@highroller.com

If you have any questions, contact the MLRO directly who will provide you with support: +35699296883

Once the above actions are taken, extreme care must be exercised in any customer interactions to avoid tipping off.

External Reporting

If a requested transaction is known or suspected to be ML or FT, the transaction is not to be carried out until the MLRO gives the go ahead. In such situations the MLRO is to be contacted without delay and the MLRO will then decide what action is necessary, depending on the respective jurisdiction and applicable legislation.



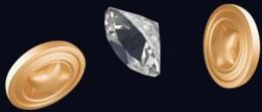
Record Keeping

The Company keeps records in respect of all business relationships and occasional transactions for a period of 5 years after termination of the business relationship.

The following records are retained:

- a. records of the actions taken to adopt and implement the risk-based approach, which are to include the following:
 - i. a copy of the BRA, changes thereto, as well as a record of any decision taken with respect to that assessment;
 - ii. a copy of the Company's most recent controls, policies, measures and procedures; and
 - iii. a copy of each CRA carried out by the Company and of any revision/s thereof.
- b. the CDD information and documents obtained for identification and verification of identity purposes. The records to be maintained are to include the following:
 - i. where the Company views the original CDD documents, the original documents themselves (where it is possible to retain originals) or a true copy of these original documents, signed and dated by an officer of the Company or a scanned copy retained of the same;
 - ii. when the Company receives a copy of the CDD documents listed in, this copy should be maintained;
 - iii. when the Company uses commercial electronic data providers to verify the identity of any individual, the results of the search should be maintained; ‘
 - iv. when the Company use video conferencing tools, identity verification software, or E-IDs to verify the identity of any individual, the records listed in those sub-sections should be retained;
 - v. when the verification of the residential address of any individual is carried out by visiting that individual at the address indicated, a record of the visit should be maintained;
 - vi. when verification of the residential address of any individual is carried out by sending correspondence or codes via registered mail or other mail courier service, the records listed in that section should be retained;
- c. records containing details relating to the business relationship that is formed and all transactions carried out in the course of a business relationship. These records are to include the following:
 - i. information gathered on the purpose and intended nature of the business relationship and information gathered to establish the business and risk profile;
 - ii. files related to accounts held by the subject person, where applicable, and all business correspondence of the Company exchanged in the course of a business relationship or in carrying out an occasional transaction;
 - iii. details on all transactions, whether international or domestic, carried out by the customers.

The details should include:



HIGH ROLLER



- the customer's: o name; o address; or o other identifying information that is usually used by the Company to identify parties to a transaction;
- the nature and date of the transaction;
- the type and amount of currency involved;
- the type and identifying number of any account involved in the transaction;
- the volume of funds flowing through the account; and
- the origin of the funds, where necessary, and the form in which the funds were placed or withdrawn; and
- any supporting evidence and records necessary to reconstruct all transactions carried out or facilitated by that the Company in the course of a business relationship.

Such records should either consist of original documents or copies that are admissible in court proceedings.

The Company should also retain the following records:

- Internal reports made to the MLRO;
- A record of any unwritten determinations made by the MLRO and the designated employee, including the reasons for not filing an STR with the FIU;
- STRs made by the SP to the FIU, and any follow up submissions made in connection thereto;
- A record of AML/CFT training attended by the sole practitioners:
 - o Date; o Type of training; o Names of persons receiving the training; o Results of any assessments; o Copy of training material;
- Records of conduct certificates or other documentation obtained in carrying out employee screening;
- Records of any outsourcing agreements entered into and other documentation that provides evidence of the Company's adherence to its outsourcing obligations;
- Records of any reliance agreements entered into and of any related assessments undertaken on the other company or third party;
- Any reports by the MLRO or by the officer entrusted with the monitoring function made to senior management for the purposes of complying with the obligations under the Applicable Legislation, such as recommendations on internal procedures, PEPs, among others;
- Records of any internal audit reports or assessments dealing with AML/CFT issues; and
- Any other records that are necessary to demonstrate compliance with obligations under the Applicable Legislation.

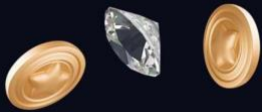
Internal reports are to be kept in respect of all business relationships.

Records are to be kept for a period of five years, even after termination of the business relationship.

Training

Awareness and training is provided to all employees and other company officials, irrespective of their level of seniority. This includes:

- Directors;



HIGH ROLLER



- Senior Management;
- MLRO and designated employee(s);
- Compliance staff; and
- All members of staff involved in the activities of the Company.

Content of Training

Through training measures, the Company seeks to ensure that relevant employees are knowledgeable of its:

- CDD measures;
- Record-keeping procedures;
- Internal reporting procedures;
- Risk management measures, including:
 - o Customer acceptance policies; o CRA procedures; o Internal controls; o Compliance management; o Communications; o Employee screening policies and procedures;
 - o Any other relevant policies and procedures concerning AML/CFT;
- and - The ML/FT risks posed by the business and/or activities of the subject person.

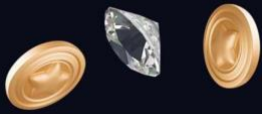
Training Records

The Company maintains records of the training provided to monitor which employees have received training, how frequently, and the nature of training provided. Training records are to include:

- the details of the training provider;
- the date on which training was delivered;
- the nature of the training;
- the names of the employees who received training; and
- where available, a copy of any training material provided.

Appendix 1 – PEPs and Sanctions Screening Procedure

- An alert is received on Slack through "Flows" example below:
- "HighRoller - highroller user from {{AddressCountry}} EcrID 621991729767524 with PEP-warning tag has now made a first deposit, carry out due diligence checks to establish whether true match or false positive"
- A tag is added on the users profile in Pragmatic called "PEP-warning".
- An adverse media search is carried out by the team to confirm if this is a real pep or not.



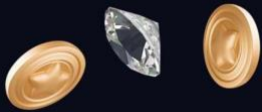
Appendix 2 – Examples of Documentary Evidence

Source	Document
Savings	Bank statement (s) demonstrating deposit / gifted monies
Sale of investments	Statement from investment provider or bank statement showing settlement from investment provider
Sale of property	Signed letter from – Solicitor / Advocate or Estate Agent or Contract of Sale / Settlement Statement
Loan	Loan Agreement or Statement
Inheritance	Copy of Will, signed letter from solicitor, Grant of Probate or letter from Executor
Maturity or surrender of life assurance policy	Closing statement or letter from the policy provider
Insurance Claims	Letter from the insurance provider
Dividends or Profits from company	Latest audited company accounts / dividend statement
Divorce	Copy of court order / judicial separation agreement
Other court aware (e.g. compensation)	Court order or signed letter from solicitor / advocate
Lottery / Gambling win	Evidence from the lottery company / cheque / winnings receipt
Gift	Document showing who gave the gift, when and why (E.g. letter from donor), plus verification of identity of the donor, and information about the source of their wealth.

Appendix 3 – SOWQ

Form can be found here:

<https://drive.google.com/drive/folders/1OgLhINYAfYf-ZDhGbqRgshqu9j4Tl9be>



HIGH ROLLER



Appendix 4 – Guidelines for disclosure of Source of Wealth and Funds

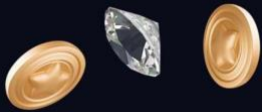
These guidelines are indicative and should be used to give the applicant an idea of the type and detail of information required and expected in order to complete the due diligence process:

- Professional salary: o Name of Employer; o Occupation; o Country; o Number of years in Employment; o Gross Annual Income.
- Capital of company/Dividends or income from business:
 - o Please provide the details, including company name and amount;
- Gift/Inheritance:
 - o Please give details, including origin, date received and amount;
- Profit from sold or maturing investments:
 - o Please provide the date of liquidation/sale and sale amount;
- Profits from property sale:
 - o Please provide the date and total sale amount;
- Profits from sale of company/business:
 - o Please provide the name and nature of the company, date and amount of sale:
- Compensation payment:
 - o Please provide details on the type and amount of compensation received:
- Pension/s:
 - o Please provide details on the number, frequency and amount of pension received:
- Any other sources of funds:
 - o Please specify

Appendix 5 – Internal Customer Review form

Player's details	
Full Name	
DOB	
Address	
Country	

HIGH ROLLER



HIGH ROLLER

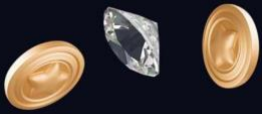


Registration Date	
KYC Verified	
KYC held on File	
ID Number	
SOWQ Collected	
PEP check	

Account's Details	
Total Deposit Amount	
Total Withdrawal Amount	
Pending WD	
Payment methods	
AML Category	
RG Category	
Game Type	

SOI/SOW Information	
Home Price Estimate:	
Employment:	
Employer Website	

Adverse Media	
Google	
Facebook	
LinkedIn	



HIGH ROLLER



Department	Agent	Date

HIGH ROLLER

Appendix 6 – Internal Customer Review Procedure

1. User ID:
2. Name:
3. Short Bio of Client:
4. Country:
5. Age:
6. KYC: True/False
7. PEP Check: Yes/No
8. AML Category: Low/Medium/High 9. RG Category: Low/Medium/High 10. Home Price Estimate:
11. Employment:
12. Employer Website:
13. Estimated Salary:
14. Social Media: (Link) 15. Gameplay: (Type of Games) 16. Join Date:
17. Roll Back: Yes/No
18. Average Bet:
19. Payment Method:
20. Total Deposit Amount:
21. Total Withdrawal Amount:
22. Balance:
23. Total Bonus Amount:

Date of Completion of Review:

(Insert Name of Agent undertaking review)

Appendix 7 – KYC Process

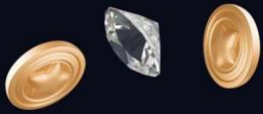
Upon submission of documents by a user, an alert is automatically generated to initiate the review process.

The alert is assigned to a designated team member for further examination and action.

The assigned team member conducts a comprehensive review of the submitted documentation to identify potential risks, validate authenticity, and ensure full compliance with regulatory standards.

Documentation is cross-verified against internal records and other relevant sources to ensure consistency and legitimacy.

Once the review process is complete, the alert is resolved. The case is documented with a detailed note in the user's account, necessary tags are updated, and the customer is notified of the outcome in a timely and appropriate manner.



HIGH ROLLER

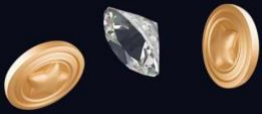


Appendix 8 – EDD Procedure

Link to EDD Procedure can be found here:

<https://highroller.atlassian.net/wiki/spaces/HIGHROLLER/pages/490274834/EDD+guide+line+process>

HIGH ROLLER



HIGH ROLLER

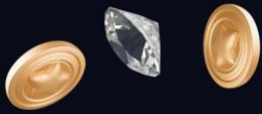


Appendix 9 – Restricted Countries List

Link to Restricted Countries List can be found here:

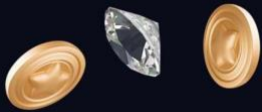
<https://docs.google.com/spreadsheets/d/13GkLAoJqU4ePilux630MTlRVi3eo3W3q/edit?gid=2130014674#gid=2130014674>

HIGH ROLLER



Appendix 10 – Internal Reporting Form

Instructions:	
If you have any knowledge or suspicion that money laundering or terrorist financing activity has taken place you must complete this form. Please email this form to the MLRO via dirk.urpani@highroller.com	
Employee submitting report	
Name:	
Department:	
Email:	
Phone:	
Line Manager:	
Details of your suspicion	
Customer ID:	
Date range of suspicious activity:	
Connected accounts:	
Why are you suspicious? :	
Have you any recorded communication with the customer that may help us understand why you are suspicious?	
Does the customer know an investigation is under way?	
Transaction activity: Note: export any suspect transactions into a CSV/excel file	



HIGH ROLLER



Any other
information relevant
to the
case?

Contact Information

For any questions regarding this policy, please contact:

eMoore N.V.

Legalcompliance Department

Groot Kwartierweg 10, Livestrong Building

Willemstad, Curaçao

Telephone: +599 9 7471401

Email: legalcompliance@the-emgroup.com

HIGH ROLLER