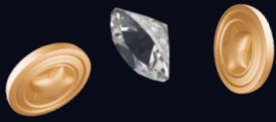


HIGH ROLLER



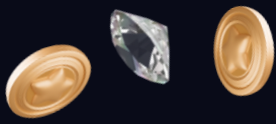
Business Risk Assessment
Highroller
May 2025

HIGH ROLLER



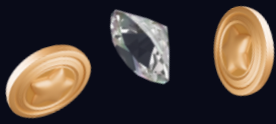
Document Control

Version	Date of Change	Brief Description of Change	Changed by	Approved by	Approved on
1.0	May 2025	Initial Draft	MLRO	Board of Directors	



Contents

Document Control	2
Contents	3
Introduction	4
Collectively known as “Applicable Jurisdictions”	4
European regulations: AMLD Directives, FATF Recommendations.	4
Aim of the Document	4
Sources of Information	5
Methodology & Risk Scoring	6
Inherent risk	7
Analysis of the Effectiveness of Controls	10
Residual Risk	12
Risk Appetite	12
Analysis of Inherent Risk	13
Customers	13
Products and Services	14
Transactions / Payment Methods	14
Geography/Country	14
Interface Risk / Delivery Channels Risk	15
Other Qualitative Risk Factors	15
AML-CFT Business Risk Assessment Results	15
Reporting & Communication of Results	16
Review and Update	17
Annexes	17



Introduction

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 by the Gaming Control Board in Curacao.

Collectively known as “Applicable Jurisdictions”

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.

European regulations: AMLD Directives, FATF Recommendations.

Aim of the Document

Interstellar Entertainment N.V. (“the Company”) has set out the Business Risk Assessment (“BRA”) to identify the risk factors it is exposed to and assesses the likelihood and impact of Money Laundering & Financing of Terrorism (‘ML/TF’) risks. On the basis of this assessment, the Company will be able to determine which areas to prioritise in terms of Anti-Money Laundering/Combating Funding of Terrorism (AML/CFT) and ensure its AML/CFT measures, policies, controls and procedures are commensurate with the ML/FT risks it faces, in order to mitigate the same.

Subject persons (also referred to as “Obligated Entities”) are to take the appropriate steps to identify and assess the risk of being exposed to money laundering (“ML”) or terrorist financing (“FT”).

As a Subject Person, the Company has an obligation to understand how criminals could use the Company to conceal the proceeds of a crime and/or to understand how clients might use funds from a legitimate activity to be laundered to avoid paying tax or to fund terrorism.

The anti-money laundering (“AML”) and counter-funding of terrorism (“CFT”) obligations of the Company are set out under the:



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

The Company is to take appropriate steps proportionate to the nature and size of its business, to identify and assess the risk of money laundering and funding of terrorism that arise out of its activities or business taking into account risk factors including those relating to customers; countries or geographical areas; products, services, transactions and delivery channels and shall furthermore take into consideration any national or supranational risk assessments relating to risks of money laundering and the funding of terrorism”.

In view of its obligations, the Company shall carry out a Business Risk Assessment (“BRA”). This document includes:

- the methodology adopted by the Company;
- the sources of information used and statistics/risk indicators;
- the risk assessment and classification of the risks identified;
- the outcome of the BRA, including the inherent and residual risks

The results pertaining to the BRA will be used by the Company in order to:

- Identify gaps or areas of improvement in the policies, controls and procedures adopted to date (including in respect to new risk factors identified, changes to business model, structures and activities, changes to external environment within which the Company operates);
- Make informed decisions about the Company’s risk appetite; and
- Ensure that the Board is aware of the key risks, control gaps and remediation efforts.

A BRA shall be properly documented and regularly reviewed and kept-up-to-date. Apart from being a regulatory requirement, the BRA assists the Company to identify and assess such risks and to substantiate its obligations on a risk-based approach.

The Company actively promotes the protection of its business from such risks and against money laundering (hereinafter referred to as “ML”) and funding of terrorism (hereinafter referred to as “FT”) assessing the kind of services, products or transactions it intends to offer, the markets it intends to target, the



technologies it will use to deliver the same, and its intended business model and activities. Eventually, the Company undertakes to update its BRA at least annually, unless there are changes that require the Company to review its BRA beforehand. Each BRA review and update is to be documented accordingly and approved by the Directors of the Company.

Sources of Information

In determining the risk factors to consider as well as any change thereto, the Company referred to several sources, including the supranational risk assessment, as well as the national risk assessment.

Apart from these assessments, the Company also consult and make use of:

- a) any relevant reports issued by the FATF, MONEYVAL and other FSRBs;
- b) reports, typologies and other information made available by FIUs or law enforcement agencies;
- c) sectoral risk assessments;
- d) information, reports and guidance made available by the ESAs and competent authorities;
- e) information from industry or professional bodies, including self-regulatory bodies;
- f) information from civil society, such as corruption indices and country reports;
- g) information from international standard-setting bodies, such as mutual evaluation reports or legally non-binding blacklists;
- h) information from credible and reliable open sources, such as reports in reputable newspapers;
- i) information from credible and reliable commercial organisations, such as risk and intelligence reports; and
- j) information from statistical organisations and academia

Methodology & Risk Scoring



HIGH ROLLER



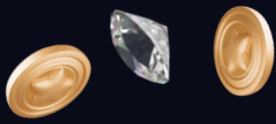
The effectiveness of the risk-based approach depends on the proper understanding of the ML/FT risk to which the Company is exposed.

Risk is defined by the inherent and residual factors. Inherent risk is here understood as being the risk one is exposed to prior to adopting and applying any measures, policies, controls and procedures to mitigate the same. Residual risk is the risk left after applying the measures, policies, controls and procedures to the level of inherent risk one has identified.

The Risk Methodology employed by Company is that of an equal weighting across all five pillars of risk as identified in the sections below.

The Company shall adopt the following methodology:

- (i) In order to identify the risk factors that the Company is exposed to and the vulnerabilities of the Company that may be exploited for ML/FT purposes, the Subject Person shall collect data and information on the risk areas noted above.
- (ii) the Company shall **identify** the risk factors it is exposed to by considering the following risk areas:
 - a. Customer risk
 - b. Countries or geographical risk
 - c. Products/services and transactions risk
 - d. Delivery channel risk
 - e. Other risk factors
- (iii) the Company shall **assess** the likelihood of each risk materialising and its resulting impact (impact would relate to reputational risk, business risk, regulatory risk, legal risk, financial loss and others). The likelihood and impact will determine the level of inherent risk that the Company is exposed to.
- (iv) the Company shall assess the effectiveness of the measures, controls, policies and procedures in place to mitigate the identified risks.
- (v) the Company shall compare the measures, controls, policies and procedures in place against the inherent risk, and calculate the residual risk.
- (vi) the Company shall determine whether the residual risk falls within the Company's risk appetite and assess whether the existing measures, controls, policies and procedures are commensurate with the ML/FT risks it faces to mitigate the same or whether additional controls are to be implemented.



The Company acknowledges that independently of the effectiveness of the measures, policies, controls and procedures adopted, ML/FT risk cannot be completely addressed, avoided or controlled.

Inherent risk

The inherent risk is the risk that the Company is exposed to prior adopting and applying any measures, policies, controls and procedures to mitigate the same.

To assess the inherent risk, it was therefore necessary to take into consideration:

- (i) The vulnerabilities, i.e.; the weaknesses which may be exploited for ML/FT purposes; and
- (ii) The threats, i.e.; the external elements that seek to exploit the Company's vulnerabilities.

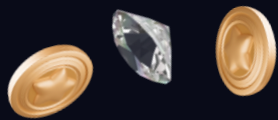
The identification of ML/FT risk considers the following risk areas and factors both from a qualitative and a quantitative point of view:

- (i) Services Risk;
- (ii) Customer Risk;
- (iii) Geographical Risk;
- (iv) Interface Risk; and
- (v) Other risk factors.

This is followed by an assessment of the same by considering the likelihood of risk manifesting itself and the impact any such manifestation would have on the Company.

The scoring is based on the analysis of data provided by the Company taking into consideration the actual business type; the customer base; the services/products offered; the channel used to service customers, the geographical footprint, and other qualitative factors by taking into account the inherent risk as outlined in both the SNRA and the NRA.

The likelihood scale allows the Company to identify the potential of an ML/FT risk occurring within the performance of its role as a remote gambling company. The Company has adopted



HIGH ROLLER



a likelihood scale retaining five different categories, namely Rare, Unlikely, Moderate, Likely and Frequent. Each category is assigned an initial one point with an increment of another one point depending on the severity of the likelihood of a potential ML/FT risk occurring, as follows:

LIKELIHOOD SCALE		
Level		Definition (as defined by the Company)
5	Frequent	Can occur very frequently in the day-to-day management of the Company, extremely high chance
4	Likely	May occur several times per year, very high chance
3	Moderate	Can occur a few times per year, reasonable chance
2	Unlikely	Can occur once per year, small chance
1	Rare	May occur less than once per year, very unlikely

The impact scale refers to the seriousness of the damage which may occur to the Company in the event of a ML/FT breach by one of its customers.

Impact Description					
Level		Generic Definition			
			Local Sectorial Impact	Business Entity	Regulatory/Legal
5	Extreme	Critical impact on the business line, excessive financial loss/damage and significant prosecution, fines and	Extreme impact on the local and/or sectorial business and its reputation which could potentially lead to loss of business.	Failure to meet key strategic objectives; Organisational viability threatened; Major	Large scale compensation payment with significant financial or reputational consequence.

HIGH ROLLER



HIGH ROLLER



		litigation issues		financial overrun.	
4	Major	Severe loss or damage, heavy regulatory action – long-term effect	Serious impact on the local and/or sectorial business and its reputation which could potentially lead to loss of business.	Major impact on Strategy	Regulatory breach with material consequences which cannot be readily rectified.
3	Moderate	Large loss or damage, regulatory action – medium-term effect	Substantial impact on the local and/or sectorial business and its reputation which could potentially lead to loss of business.	Moderate impact on Strategy	Regulatory breach with material consequences which can be readily rectified.
2	Minor	Limited financial loss or damage, minor regulatory action – short-term effect	Some impact on the local and/or sectorial business and its reputation which could potentially lead to possible loss of business.	Minor impact on Strategy	Regulatory breach with minimal consequences which cannot be readily rectified.
1	Insignificant	Negligible financial loss or damage, no regulatory action – no material effect	Negligible impact on the local and/or sectorial business and its reputation.	Negligible impact on Strategy	Regulatory breach with minimal consequences which can be readily rectified.

The inherent risk table below is used to determine the inherent risk by taking into account the likelihood of a risk materialising and the resulting impact.

HIGH ROLLER



HIGH ROLLER



Inherent Risk Matrix					
LIKELIHOOD D IMPACT	1 Rare	2 Unlikely	3 Moderate	4 Likely	5 Frequent
5 - Extreme	Low-Medium Risk	Medium Risk	High Risk	Very High Risk	Very High Risk
4 - Major	Low Risk	Medium Risk	High Risk	High Risk	Very High Risk
3 - Moderate	Low Risk	Low-Medium Risk	Medium Risk	High Risk	High Risk
2 - Minor	Low Risk	Low Risk	Low-Medium Risk	Medium Risk	Medium Risk
1 - Insignificant	Low Risk	Low Risk	Low Risk	Low Risk	Low-Medium Risk

Analysis of the Effectiveness of Controls

Once the inherent risk has been identified and assessed, the internal controls in place to mitigate such risks shall be evaluated to determine how effective they are to offset the overall risks. Control measures are monitored through regular risk-based internal compliance reviews and reports, AML/CFT policies and procedures, and KYC checklists.

Mitigation controls are programmes, policies or activities put in place by the Company to protect against the materialisation of an ML/FT risk, or to ensure that potential risks are promptly identified. Controls are also used to maintain compliance with regulations governing the Company's activities.



HIGH ROLLER



The controls in place are evaluated for their effectiveness in mitigating the inherent money laundering risk and to determine the residual risk rating.

At present, the internal controls include but are not limited to the following:

- Customer Risk Assessment is carried out to gauge the risk of each client
- AML-CFT Manual which includes:
 - procedures on how to compile the business and risk profile of the customer
 - carrying out adequate CDD measures, commensurate with the risk of the customer
 - the Company carries out independent PEP checks
 - obtaining information on the purpose and objectives of the business relationship
 - obtaining information on the source of wealth and source of funds
 - ongoing adverse media and sanctions checks
 - procedures for ongoing monitoring, including transactions monitoring
- Record Keeping & Retention
- Designated AML Compliance Officer / Unit
- Training provided on at least an annual basis
- Procedures on internal and external reporting of STR/SAR
- Jurisdictional Risk Assessment
- PEP/Sanctions Screening Software
- Transaction Monitoring
- Customer Acceptance Policy
- AML/CFT Consultants to provide us with any clarifications and/or assistance when needed

Each area is assessed for overall design and operating effectiveness. The control effectiveness for each risk factor is assigned a score which reflects the effectiveness of the risk mitigating measures. The scoring currently used ranges between 1 and 5, as follows:

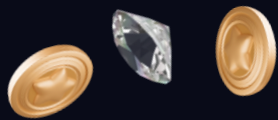
Control Scoring Matrix		
Level		Definition (as defined by the Company)
5	Very Effective	The control is being implemented effectively and is fully operational to manage the associated risk effectively. All evidence associated to the control is being documented effectively.



HIGH ROLLER



4	Effective	The control is in place, but needs minor improvements, the control is still considered effective, but can be improved further to manage the risk to its fullest extent. Currently the risk is managed and there is adequate evidence documented for this control
3	Needs Improvement	The control is in place but needs somewhat improvement to be considered effective to manage the risk. Currently the risk is somewhat being managed and there is sometimes evidence available and documented for this control
2	Ineffective	The control is in place but needs substantial improvement to be considered effective to manage the risk. Currently the risk is not being effectively managed and there is no backing form of evidence documented for this control
1	Non-Existent	No evidence of control, or control have no effect



Residual Risk

Residual risk is the risk that remain after control measures are applied to the inherent risk. In other words, it is the exposure to ML/FT risks that remain after adequate controls, policies and measures would have been out in place.

It is determined by balancing the level of inherent risk with the grading of the risk mitigating actions / controls. The residual risk rating is used to indicate whether the ML/FT risks within the Company are being adequately managed on the following basis:

Residual Risk Matrix					
Control Effectiveness	5	4	3	2	1
Inherent Risk	Very Effective	Effective	Needs Improvement	Ineffective	Non-Existent
Low Risk	Low Risk	Low Risk	Low Risk	Low Risk	Low Risk
Low-Medium Risk	Low Risk	Low Risk	Low-Medium Risk	Low-Medium Risk	Low-Medium Risk
Medium Risk	Low Risk	Low Risk	Low-Medium Risk	Medium Risk	Medium Risk
High Risk	Medium Risk	Medium Risk	High Risk	High Risk	High Risk
Very High Risk	High Risk	Very High Risk	Very High Risk	Very High Risk	Very High Risk

Risk Appetite

The Company defines the term 'Risk Appetite' as the level of residual risk it is prepared to accept in the pursuit of its business objectives and as the level of risk tolerance which it is prepared to consider as acceptable during the operation of its



HIGH ROLLER



business. If this residual risk is not within the boundaries of the Company's risk appetite, additional control measures, reduce the risk in question, or avoid the

risk by ending the activities should be taken. Annex I includes the Company's risk appetite in relation to each risk factor.

Risk Appetite Weighting	
Accept	Mitigating measures are working
Reduce	Reduce risk or improve controls
Avoid	End the activities

The Company acknowledges that independently of the effectiveness of the measures, policies, controls and procedures adopted, ML/FT risk cannot be completely addressed, avoided or controlled.

Analysis of Inherent Risk

The identification of the risk factors the Company is exposed to requires a consideration of the risk areas, both from a qualitative and quantitative points of view. The Company has examined its current business plan and portfolio of products and services, as well as any diversification or expansion plans.

Customers

The Company here shall consider the risk of ML/FT that emanates from players. The Company considers risk exposure emanating from, inter alia, the volume of players involved in industries or sectors where opportunities for ML/FT are particularly prevalent; the number of players who are PEPs; activity from which the player derives their source of wealth or funds; and whether the client structure is complex or opaque.

At present the current customer risk considers the following:

HIGH ROLLER



1. Anonymous UBOs
2. Lack of Identity Verification
3. PEP

4. Sanctions
5. Wagering with Criminal Proceeds
6. Fraud
7. Problem Gamblers
8. Collusion
9. Mule Accounts
10. Customers with links to crime or under investigation
11. Adverse Media
12. Customers with links to terrorism financing
13. Customers not transacting in line with expected profile and or changing or unusual spending patterns
14. Player deposits and withdraws without wagering
15. High velocity of deposit transactions
16. Chargeback/s requested by player
17. Wealth derived from a cash intensive business

Products and Services

The Company considers the complexity of the service.

At present the current risk exposure is to:

- Fixed odds games without hedging – Videoslots, Class Slots, Videopoker, Minigame
- Fixed odds games where hedging is possible – Tablegames, Blackjack, LiveDealer, ScratchCard

Transactions / Payment Methods

The Company considers the element of transparency, payment method involved and the value or size of the associated transaction.

At present the current risk exposure is to:

- Bank Transfers (EEA or equivalent safeguards)
- Debit / Credit Cards issued by banks (EEA or equivalent safeguards)
- Debit / Credit Cards issued by other licensed institutions



- EEA Licensed Payment Service Providers
 - Non-EEA Licensed PSP
 - EEA-Licensed PSPs that can be funded by cash or quasi-cash
-
- Prepaid Cards / Vouchers
 - Peer to Peer transfers
 - Cash
 - Closed Loop Policy compliance
 - Use of higher risk payment methods
 - Frequently changed payment methods or closed loop policy not adhered to
 - Use of stolen cards and/or accounts
 - Smurfing
 - Players using multiple payment methods

Geography/Country

The Company seeks to understand and evaluate the specific risks associated with doing business with players in/from certain geographic locations. Different jurisdictions pose different level of risk. The Company's geographical risk assessment is based on the "know your country"¹ scoring methodology. The Company also monitors the FATF lists of *Jurisdictions under Increased Monitoring* and *High-Risk Jurisdictions subject to a Call for Action* and the EU Commission's list of third countries which have strategic deficiencies in their AML/CFT regimes. In this context, the Company identifies the geographical risk exposure by considering the following:

- the countries our players are based in or operate from;
- where our players obtain their wealth or funding from;
- where are funds coming from (bank jurisdiction);
- how our players are linked to countries through networks, agencies or other related parties;

Interface Risk / Delivery Channels Risk

Some delivery channels/servicing methods can increase the risk of ML/FT as they bring distance between the client and the Company. As a result, the Company may not truly know or understand the identity and activities of the client. Consequently, non-face-to-face relationships or the involvement of third parties, including

¹ <https://www.knowyourcountry.com/>



HIGH ROLLER



intermediaries, as well as the expectation that the relationship will be conducted on a non-face-to-face basis, are all factors that increase the inherent ML/FT risk.

Other Qualitative Risk Factors

The Company also considers how other risk factors can have an impact on operational risks and contribute to an increasing likelihood of breakdowns in key risk controls.

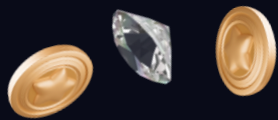
The Company considers the following factors, as directly or indirectly affecting the Company's risk exposure and inherent/residual risk:

- Employees Turnover;
- Emerging risks;
- Outsourced Activities;
- System errors;
- Increased volume of clients;
- Introduction of new products and/or services;
- Insufficient employee awareness of AML/CFT risks
- Outdated policies and procedures
- Impact of Russia-ukraine conflict

AML-CFT Business Risk Assessment Results

From an analysis of the Company's inherent risk and control effectiveness, the following conclusions may be drawn:

	Inherent Risk	Controls Effectiveness	Residual Risk
Customer Risk	High	Effective	Medium
Product, Service and Transaction Risk	Medium	Effective	Low
Geographical Risk	Medium	Effective	Low
Interface Risk	Medium	Effective	Low



HIGH ROLLER



Other Risks	Medium	Effective	Low
Overall	Medium	Effective	Low

The Company's Inherent Risk Scoring is equivalent to **Medium** with **Effective** controls in place, resulting in a residual risk of **Low**.

It is acknowledged that independently of the measures, policies, controls and procedures adopted by the Company, there will remain a degree of ML/FT risk that cannot be addressed, avoided or controlled. The Company will strive to maintain open contact with the FIU, not only to file Suspicious Transaction Reports where obligatory, but also to seek guidance from the regulator when in doubt. The Company strives to maintain effective measures and controls, and to actively seek to keep its policies and procedures updated to reflect its services, the industry and the changes in risk typologies.

This difference in risk is mainly attributed to a number of mitigation factors that the Company has implemented, the risk appetite adopted by the company and also guidance which is constantly being issued by the FIU and other authorities.

Reporting & Communication of Results

The results of the Business Risk Assessment are communicated to the board of directors and to regulatory and supervisory authorities, as may be dictated by Law.

As a result of the volume of data that will underpin any ML/TF risk Assessment, the methodology should be designed so that the results can be presented in a number of different ways, highlighting risks by any factor recorded, for example by product type, geography or client types, amongst others.

This is more than just an averaging of results, as it should be able to highlight inherent and residual risk, as well as control effectiveness, for any part of the Company's business.

Review and Update

It is the responsibility of the MLRO to review this BRA. This BRA shall be reviewed at least annually, or more often should the need arise. Any significant updates



made to this BRA will be distributed to the Company's Board of Directors for their comments / review.

The BRA shall be updated, inter alia, in case of:

- changes in legislation;
- organizational changes within the Company; or
- new internal rules, procedures, or policies within the Company.

Where changes have been made, the Company shall make sure that all employees are made aware of the changes.

Annexes

All Annexes attached hereto form an integral part of this BRA.

Annex I: Risk Factors and Risk Scenarios