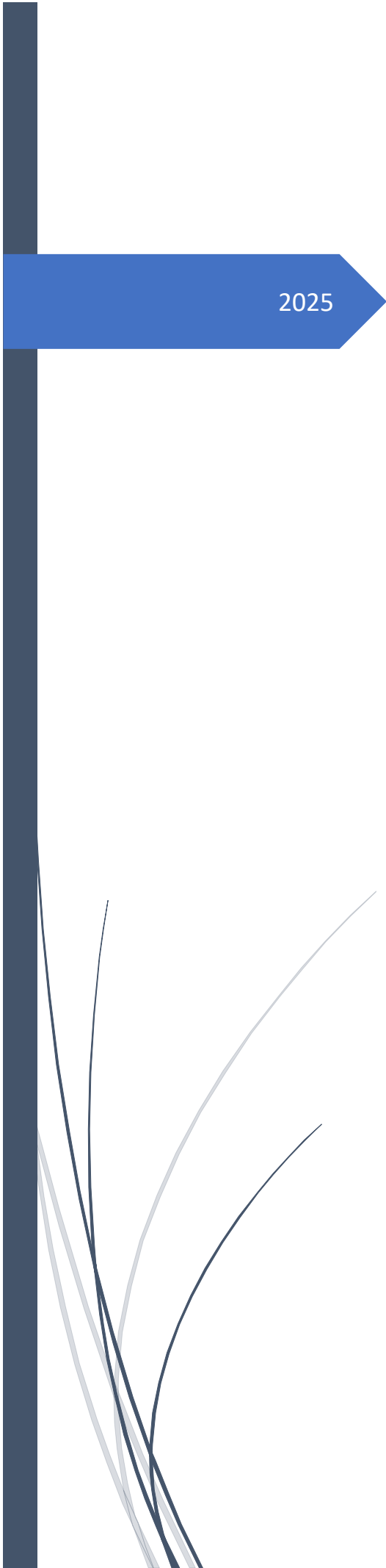




2025

AML/CFT Risk Assessment Policies and Procedures

Neil Caruana
PRETENSE FLIP N.V

Policy History

[illegible]

CONTENTS

1	Introduction	5
1.1	about this document	5
1.2	Policy Statement.....	5
1.3	Objective	5
1.4	Scope	5
1.5	Audience.....	5
1.6	Definitions	6
2	Regulatory FRAMEWORKS	7
2.1	National Regulations	7
2.2	International Regulations	7
3	Combating Money Laundering and Financing of Terrorism	9
3.1	threats facing the online gambling sector	9
3.2	the need to combat money laundering and financing of terrorism.....	10
3.3	Procedures	10
4	Risk Based Approach.....	11
4.1	Setting up Risk Factors.....	11
4.2	Higher Risk Customers.....	11
4.3	Risk Analysis and Evaluation.....	11
4.3.1	Numerical Classification	12
4.3.2	Customer Risks	13
4.3.3	Risks RELATED to distribution channels.....	15
4.3.4	GEOGRPAHICAL RISKS.....	17
4.3.5	Payment Instrument Risks	19
4.3.6	Product Risks	21
4.3.7	Internal Risks	24
4.4	Risk Profiles	25
4.4.1	Low Risk.....	25
4.4.2	Medium Risk.....	26
4.4.3	High Risk.....	26
4.4.4	Payment Method Risks.....	28
5.	PEP's. Sanctions and Adverse Media	29
5.1	Politically Exposed Person Checks	29
5.2	Sanction Checks.....	30
5.3	Adverse Media	31

5.4	Sources	31
5.5	Reliance on Third Parties to Perform Customer Due Diligence.....	31
6	Customer Due Diligence.....	33
6.1	Simplified Due Diligence.....	33
6.2	Customer Due Diligence	34
6.3	enhanced due diligence	34
6.4	Source of Funds/Wealth.....	35
6.5	Source of Wealth Questionnaire/Documentation	35
6.6	KYC Documentation Review	36
6.7	Clients refusing to send documents.....	36
7	Monitoring	37
7.1	Daily Monitoring.....	37
7.2	Suspicious Behavior.....	38
7.3	Customer Risk Assessment.....	39
7.4	Customer Business Profile (expected level of activity)	40
8	General Policies.....	41
8.1	Customer onboarding process	41
8.2	Transaction Monitoring Process.....	41
8.3	Suspicious Activities	42
8.4	Wagering Requirements.....	42
8.5	Withdrawals	42
8.6	Cryptocurrency transactions	43
8.7	Security Review	44
8.8	Financial Institutions	44
8.9	Shell Banks.....	45
8.10	Internal Fraud	45
8.11	Testing	46
8.12	Problem Gambling.....	47
9	Money Laundering Reporting and Training.....	48
9.1	The Money Laundering Reporting Officer (MLRO).....	48
9.2	Reporting of Suspicious Transactions.....	48
9.3	Record Keeping.....	48
9.4	Staff due Diligence.....	49
9.5	Staff AML Training	49
9.6	Procedures and Policy review	49
9.7	MLRO Contact	49

10	Compliance and Consequences of Non-Compliance	50
10.1	Compliance Obligations.....	50
10.2	Breeches of Policy	50
10.3	Disciplinary Measures	50
10.4	legal and regulatory consequences.....	51
10.5	reporting concerns	51
11	Related Information	52
11.1	Internal Policies and Procedures	52
11.2	Legal and Regulatory frameworks	52
11.3	External Guidance and tools	52

1 INTRODUCTION

1.1 ABOUT THIS DOCUMENT

This document describes the AML/CFT policies and procedures used for Pretense Flip N.V. This AML/CFT policy has been developed to ensure that our business is in compliance with all relevant laws and regulations related to preventing money laundering and financing of terrorism. It outlines the measures we have implemented to identify and mitigate the risks of money laundering and terrorism financing, and to detect and report suspicious activity.

1.2 POLICY STATEMENT

Pretense Flip N.V. is committed to the highest standards of integrity in the prevention of money laundering, terrorist financing, and proliferation financing. This policy sets out the Company's framework and approach to comply with all applicable anti-money laundering and counter-terrorist financing (AML/CFT) laws and regulations, including those mandated under the laws of Curaçao, the Financial Action Task Force (FATF), and relevant international standards.

The policy applies to all Company employees, contractors, third-party agents, and business units involved in customer interaction, transaction processing, compliance, and risk management. It aims to ensure that adequate systems, controls, and procedures are in place to detect, prevent, and report any suspicious activity that could compromise the integrity of the business.

1.3 OBJECTIVE

The Company is a limited liability company, duly incorporated and registered in accordance with the laws of Curaçao. This policy is written based on the national legislation on AML, CFT and the penalization of predicate crimes of Curaçao and applicable international standards set by the FATF. Combined these regulations provide a solid, internationally accepted standard for the procedures maintained for the prevention of the misuse of the Services provided by the Company. Proper Identification of Account Holders, verification of the identity, monitoring of Player activities and reporting of unusual activities are part of the measures the Company has in place in an effort to prevent, deter or mitigate industry related risks.

1.4 SCOPE

The Company is committed to the highest national and international AML and CFT standards when providing its Services and requires management and employees to follow these standards.

1.5 AUDIENCE

This policy applies to the following stakeholders involved in the operations of Pretense Flip N.V.:

- All full-time and part-time employees
- Compliance and Risk personnel

- Customer support and onboarding teams
- Payments and finance departments
- Contractors and consultants handling customer data
- Third-party service providers engaged in KYC/AML functions

All individuals listed above are required to read, understand, and adhere to the provisions of this policy

1.6 DEFINITIONS

Below are key terms used throughout this policy:

- **AML** (Anti-Money Laundering): Refers to laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income.
- **CFT** (Counter-Terrorist Financing): Refers to efforts to detect, prevent, and report the financing of terrorist activities.
- **PEP** (Politically Exposed Person): An individual who is or has been entrusted with a prominent public function, as well as their immediate family members or close associates.
- **CDD** (Customer Due Diligence): The process of verifying a customer's identity and assessing their risk level based on relevant data.
- **EDD** (Enhanced Due Diligence): Additional verification measures applied to high-risk customers, such as PEPs or customers from high-risk jurisdictions.
- **SOW** (Source of Wealth): The origin of a customer's entire body of wealth — how it was accumulated over time.
- **SOF** (Source of Funds): The origin of the specific funds used in a transaction or gaming account — e.g., salary, inheritance, investment proceeds.
- **STR/SAR** (Suspicious Transaction/Activity Report): A formal report submitted to the Financial Intelligence Unit (FIU) when a transaction is suspected of being related to money laundering or terrorist financing.
- **CRA** (Customer Risk Assessment): An internal risk profile created for each customer based on jurisdiction, behavior, and financial patterns.
- **FIU** (Financial Intelligence Unit): A national center responsible for receiving, analyzing, and disseminating financial information related to suspected money laundering or terrorist financing.

2 REGULATORY FRAMEWORKS

2.1 NATIONAL REGULATIONS

Pursuant to the National Ordinance of Money Laundering (1993), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others:

- a) the Code of Criminal Law (Penal Code) (N.G. 2011, no. 48), as lastly amended by N.G. 2015, 74.
- b) the National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2015, no. 68 (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations, specifically the National Decree containing general measures on the execution of articles 22b, paragraph 7, and 22j, paragraph 2, of the NORUT (N.G. 2021, 69).
- c) the National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2015, no. 69 (N.G. 2015, no. 84) (NOIS), with the consolidated text published in N.G. 2017, no. 92, together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations, specifically the National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the NOIS (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
- d) the National Ordinance on the Prolongation of the sanction's national decrees (N.G. 2018,34)
- e) the Sanctions National decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);
- f) the Sanctions National decree North Korea (N.G. 2015,30).
- g) the Sanctions national decree Libya (N.G. 2015,28); and
- h) the National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

2.2 INTERNATIONAL REGULATIONS

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting international standards by regularly implementing these standards in its national legislation.

On international level, the FATF plays a very important role in the combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Although Curaçao is not a EU member, the Company, in addition to the FATF rules, where applicable, adheres to AML rules issued in directives by the European Union. Subsequently the present policy is a combination of the FATF, EU and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

3 COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM

3.1 THREATS FACING THE ONLINE GAMBLING SECTOR

In any quantification of the threats facing a given sector there will be a natural emphasis on the threats that have been revealed from investigations and an absence of information on those threats that criminals have been able to keep hidden.

The threats facing the gambling sector are as follows:

- Money Laundering
 - criminals use the platforms to move illicit funds. This can occur through a variety of means, including the use of stolen credit cards, fraudulent transactions, and the purchase of chips or virtual currency with dirty money.
 - Criminal ownership, infiltration or coercion of an online gambling licensee to either launder on an ongoing basis or to launder a limited number of large transactions (perhaps to associated, unlicensed companies) before simulating business failure and surrendering the licence.
 - Undetected, high-volume, systematic laundering by organised crime of an online gambling platform.
 - Opportunistic laundering by individuals or dedicated criminal rings on an online gambling platform, including instances where the predicate offence (e.g., Credit card theft, cheating) first occurs on the platform.
- Fraud
 - Criminals use stolen identities, fake documentation, or other means to create accounts and engage in illegal activities such as cheating, collusion, or bonus abuse.
 - Use by hackers of stolen passwords to transfer value from hacked online accounts to other withdrawal mechanisms or confederates.
 - Use of an online gambling platform to benefit from manipulation of outcomes in sport.
 - Use of an online gambling platform as an informal payroll, banking system or money/value transfer system (“MVTs”) for criminals or terrorists (including use by Peps, etc) to transfer value across borders where currency controls exist.
 - Collusion with business to circumvent statutory restrictions in another jurisdiction.
 - Introduction of proceeds of crime on to an online gambling platform as part of criminal lifestyle spend.
 - Use of an online gambling platform to generate personal or corporate income without declaring it to tax authorities (including by licensees).
 - Use of high street shops affiliated with online operations to place dirty cash into the online environment.
 - Extension of credit in order to create then exploit debt.
 - Introduction of proceeds of crime to an online gambling platform by gamblers who steal money to fund gambling.
 - Use by hackers of stolen passwords to transfer value from hacked online accounts to other withdrawal mechanisms or confederates.
- Cybersecurity Threats: Online gambling websites are vulnerable to cyber-attacks, including hacking, phishing, and distributed denial of service (DDoS) attacks. These attacks can result

in the loss of customer data, financial losses, and damage to the reputation of the online gambling business.

3.2 THE NEED TO COMBAT MONEY LAUNDERING AND FINANCING OF TERRORISM

The Company has three main concerns:

- Reputation Risk
- Regulatory Risk
- Litigation Risk

3.3 PROCEDURES

We have conducted a risk assessment of our online gambling operations to identify the money laundering and terrorism financing risks that we face. Based on this assessment, we have implemented the following measures to mitigate those risks:

- Customer Due Diligence (CDD) measures: We conduct customer due diligence checks on all customers when they sign up, and periodically throughout their relationship with us. We verify the identity of our customers using reliable and independent sources, and we assess their risk level based on factors such as their jurisdiction, transaction history, and source of funds.
- Enhanced Due Diligence (EDD) measures: We conduct enhanced due diligence checks on customers who are deemed to be high-risk, such as those who make large deposits, those who are politically exposed, or those who have complex ownership structures. This includes obtaining additional information and documentation to verify their identity and source of funds.
- Monitoring and Reporting: We monitor customer transactions on an ongoing basis to detect any suspicious activity. We have implemented transaction monitoring systems to identify unusual or high-risk transactions, and we report any suspicious activity to the relevant authorities in accordance with our legal obligations.
- Training and Awareness: We ensure that all staff members who are involved in our online gambling operations receive appropriate training on AML/CFT regulations and our internal policies and procedures. This includes regular training on the risks of money laundering and terrorism financing, how to identify and report suspicious activity, and the consequences of non-compliance.
- Record Keeping: We maintain accurate and complete records of all customer transactions and due diligence checks. These records are kept for a minimum of five years and are made available to relevant authorities upon request.
- Internal Controls: We have implemented internal controls to ensure that our AML/CFT policies and procedures are effective and that they are being followed. This includes regular reviews and audits of our policies and procedures, as well as the appointment of a designated AML/CFT compliance officer to oversee our AML/CFT program.

4 RISK BASED APPROACH

4.1 SETTING UP RISK FACTORS

The Company made a list of risk factors to determine a client's risk profile in relation to ML & CFT.

The list includes the following:

- A list of countries which the FATF considers applying deficient AML/CFT controls;
- A list of countries which in the licensee's opinion represent heightened ML/FT risk (which may or may not be on the first list).
- A value which represents the upper value of a typical player's transactions.
- A list of payment channels which are considered higher risk.
- A list of any other indications which in the opinion of the licensee's MLRO indicates higher risk.
- A list of the subjects of AML/CFT related warning notices; and
- Screening for politically exposed persons, sanctions and adverse information.
- Product risk (Casino, Live Casino)

Irrelevant of how money is transferred to our casino, there is always a risk that this money would have originated from illegal activities, such as credit/debit card fraud, theft from player's employer or even narcotics trafficking. Hence, by paying greater attention and increase monitoring of high spenders, the Company will be able to mitigate this risk.

4.2 HIGHER RISK CUSTOMERS

Where participants are flagged with a notification after the account opening, accounts are locked until customer due diligence procedures are in place. Some of the possible notifications that can be triggered are:

- A client who is a Politically Exposed Persons (PEPs), their family members or close business associates ("persons linked thereto")
- A client flagged on the sanctions list.
- SIPs, Watch list.
- A client residing or located in a country, the AML/CFT credentials about which the Company has doubts.
- A client who has been the subject of a disclosure.
- A client depositing/ gambling/withdrawing big amounts.

4.3 RISK ANALYSIS AND EVALUATION

Below is all the risk which were Identified, The Impact, Measures and Controls

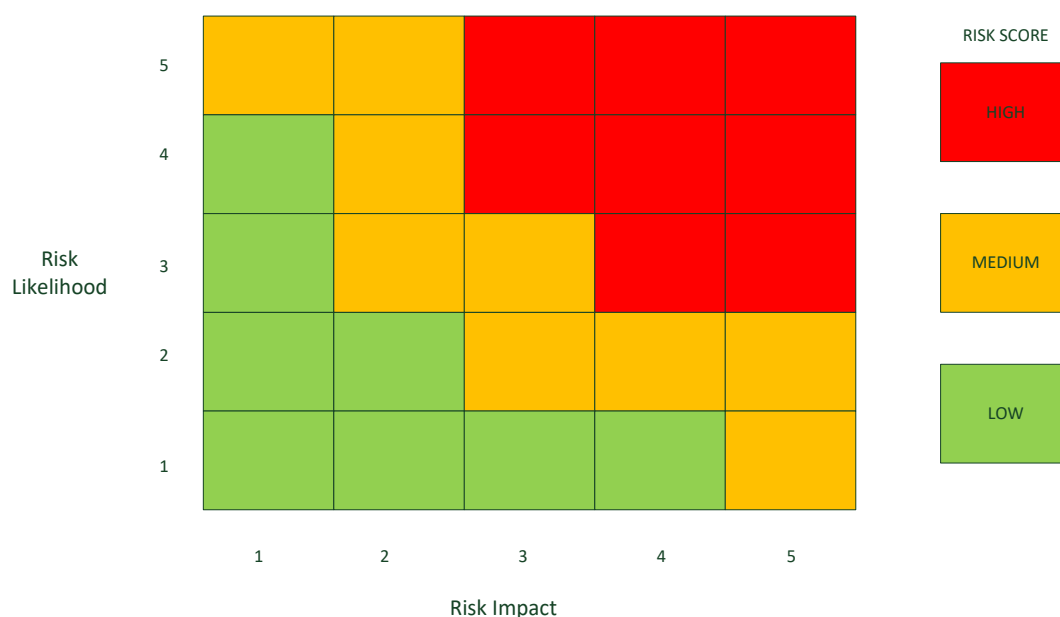
4.3.1 NUMERICAL CLASSIFICATION

To assess the risk and determine the appropriate treatment, the company has examined the threats, vulnerabilities, the likelihood that the threat will take place and the impact of it should it occur. A 5-point Scale has been used to describe the likelihood of a risk occurring and also to describe the impact that it is likely to have.

The 5-point scale for the likelihood ranges from 1 = Low Risk to 5 = High Risk.

The risk matrix shown below illustrates the scales and allows us to prioritise our risks so that they can be managed more effectively.

Risk Matrix Chart



The Risk classification used is the score obtained from multiplying the likelihood that the risk will occur and the impact it is likely to have. Both scales range from 1 to 5, so the minimum score will be 1 and the maximum score will be 25 as showing in the Risk Matrix Chart above.

Each risk has been allocated a classification based on its score as follows:

- LOW – 1 to 4 inclusive
- MEDIUM – 5 – 10 inclusive
- HIGH - 12 or more

The rationale for indicating the likelihood and impact ratings allocated has been given so that we can easily identify where the risks are the highest and prioritize our efforts accordingly but also so that the scoring can be assessed in the future to see if they have materially changed. This will also assist in ensuring consistency and repeatability in risk assessments.

4.3.2 CUSTOMER RISKS

Vulnerabilities and Threats	Likelihood
Remote Gaming operators are subject to the vulnerability of not being able to physically meet and assess customers as all the activity takes place over distance communication. The operator's ability to verify that the person behind the monitor or mobile device is the person that is opening an account with the company is therefore always more complex and difficult to achieve. The possibility of gambling anonymously has been identified by Pretense Flip N.V as an indicator of high-risk money laundering. Transactions and financial flows of complex and high values as well as the use of e-wallets increase the vulnerability. However, remote gaming operators do not carry out one-time or ongoing anonymous relationships. All clients are obliged to provide identification details upon registration and in this way their long-term activity is recorded, monitored and evaluated. This process alone is not enough to protect against the following threats, which are given a score depending on the likelihood of their occurrence: - Fake registrations and/or use of fake documents (5) - Identity theft using stolen identity details or documents (4) - Customer's data becoming invalid in long-term relationships (4) - Account takeover (4) - Account made available to third parties or otherwise or accessed from other geographical locations (4) - Customer's activity not raising suspicions if not properly monitored (3) - Customer's deposits or spend being high or otherwise irrational and not being able to be tackled (3) - Politically Exposed Persons (PEPs) or persons subject to financial sanctions attempting to use the services of the remote gaming operator (1)	Medium – High (1-5) Whilst some threats are a frequent occurrence, like fake registrations, other customer threats have been only experienced on a very small scale, such as registration of a small number of PEPs and Sanctioned customers. The use of third-party identities through the use of multiple IDs is considered medium/high.
	Impacts High (5) The Impact of the threats not being sufficiently addressed are considered to be high.
	Risk Evaluation High (5 – 25)
Measures	

The company has in place a combination of both technological and organisational controls to mitigate the above risks. These include:

- Automated and ongoing screening for PEPs and Sanctioned Persons. These screening procedures are carried out automatically by specialised service providers at registration and on a daily basis. This enables the company to catch any newly registered customers and also potentially existing customers should they become subjects to PEP & Sanctions lists.
- Customer risk assessment. Every customer gets assigned a risk level depending on their level of gambling and other factors which allows us to follow the higher risk customers thoroughly and detect suspicious behaviour. The company continuously follows up on the risk assessment/classification of its customers and adjust the risk levels when necessary.
- Customer Due Diligence Procedures. Customers, depending on their risk level and also at key stages in their relationship, are further looked into by the company and when deemed relevant, requested to provide documentation and/or evidence of their Source of Funds and Source of Wealth. The level of verification will depend on the individual customer's risk classification. Employees are provided internal guidance and use open sources to ensure that customer documentation is valid. Where required, additional information is obtained through electronic databases or additional commercial intelligence providers.
- Systems flagging considerable variation, frequency and volume. To identify large numbers of transactions and turnover, the company has systems in place flagging these events as well as unusual individual transactions and every flagging is addressed by the AML officers.
- Systems flagging customers who are attempting to create multiple accounts, use of bots, Proxy or VPNS and trying to mask their IP address
- Suspicious Transaction Reports. Where a customer transaction is identified as being suspicious, or there are reasonable grounds to suspect that the customer could be engaging in Money laundering or Terrorist Financing, an internal escalation process is triggered whereby a Suspicious Transaction Report is escalated to the Money Laundering Reporting Officer.

Controls	Actual Risk
- Customer Risk Assessments by AML Analysts - Analyst quality control by Seniors and Manager - Weekly Team Meetings - Internal Audit Function review of system controls in place and relevant process documentation	Medium (10) The risks are mitigated primarily through the risk level assigned to customers by our Analysts. The ongoing monitoring of players substantially reduce the likelihood of the risks occurring. However, controls are being updated and reviewed on an ongoing basis.

4.3.3 RISKS RELATED TO DISTRIBUTION CHANNELS

Vulnerabilities and Threats	Likelihood
Remote gaming operators are subject to the vulnerability of not being able to physically meet and assess customers as all the activity takes place over distance communication. Transactions and financial flows which are large, and complex add to the vulnerability as do the use of electronic money and digital currencies. The possibilities of third parties using a gambling account also increases. These are all threats and vulnerabilities which are naturally related to both the customers and the distribution channel, but we have chosen to include and describe them in detail above and in connection with the risks associated with our customers. Risk factors related to distribution channels concern whether the operator has control over its' products and services when they are provided to consumers. In some cases, a third party might have such control. In relation to Pretense Flip N.V's products and services, there are two threats identified and which are specific to distribution channels. The first one concerns Live Casino. When it comes to Live Casino, the actual gambling experience is provided by a game provider. In this regard, Pretense Flip N.V does not have full control over issues such as: statements in chat indicating money laundering or other suspicious behaviour when engaging with the third-party game provider. However, the third-party game providers work closely with Pretense Flip N.V to make sure any suspicious behaviour gets reported. In conclusion, the following threats have been identified as specific to the distribution channel. - Statements in the Live Casino chat indicating money laundering or other suspicious behaviour (5)	Medium (3) There could be instances where suspicious statements are made in the Live Casino that does not get reported to us. For this reason, we are continuously improving our cooperation with the game providers.
	Impacts
	High (5) The Impact of the threats not being sufficiently addressed are considered to be high
	Risk Evaluation Medium (5)
Measures	
The company has in place a number of both technological and organisational controls to mitigate the above risks. These include:	

- Due Diligence of Third-Party Providers. Pretense Flip N.V only work with third party providers which are well renowned, well-trusted and compliant with applicable regulation related to game providers. Furthermore, Pretense Flip N.V's MLRO is updated with industry newsfeeds to detect if any third-party provider can be suspected of not being compliant. - Communication with service providers. Service providers make available to the company support personnel that can assist to provide specialised assistance by reviewing customers' activity on their platforms. The company has the ability to contact them to get insights into the customer's activity on a specific platform and relate it to behaviour indicative of money laundering. - Suspicious Transaction/Activity Reports. Internal procedures include escalation of STR/SAR reports when due diligence checks indicate a suspected, known or it is reasonably expected to suspect a client or a transaction to form part of an attempted or potential case of ML/FT. - Deposit and Withdrawal Reviews. These provide step by step instructions on the checks to be carried out on customer's deposits and withdrawals, including checks on the payment instrument to confirm that it matches the customer's origin.	
Controls	Actual Risk
- Analyst quality control reviews by Seniors and Managers - Internal review of third-party providers - Weekly team meetings - Internal Audit Function review of internal procedures and process documentation	Low (4) The risks are mitigated through our due diligence processes and close cooperation with third party providers. These substantially reduce the likelihood of the risks from occurring. Although the risks can never be completely eliminated the controls are tweaked on an ongoing basis to improve through lessons learnt.

4.3.4 GEOGRAPHICAL RISKS

Vulnerabilities and Threats	Likelihood
The nature of the remote gaming services industry provides individuals anywhere with the ability to access services provided in any country. The advantage is that it enables companies to offer their services at a global level, but the negative side is that this can result in operators being exposed to potential customers whose aims may be to misuse the company's services. There is always a potential risk that customers from blocked/ High Risk countries use our services or allow others to use our services. Furthermore, customer accounts could be highjacked and used by parties in blocked/high-risk countries or attempts can be made to deposit money from abroad or withdraw money to a foreign account. Another issue which has been highlighted and discussed when conducting the general risk assessment is the possibility to transfer funds from other countries through casino games, such as poker. However, such transfers are not possible at Pretense Flip N.V as our games are not peer-to-peer. Player losses are not transferred to other players, which makes it impossible to transfer funds to other accounts through such games. There is also a risk of money being transferred across national borders however this is mitigated as all withdrawals are checked before being processed and we enforce a closed loop policy. Common threats considered: - Customers registers with fake details or allows the account to be used by third parties, from high-risk/blocked countries (4) - Customer accounts being high-jacked and used by malicious parties in high-risk/blocked countries (4) - Deposits or withdrawals to/from high-risk countries (4)	High (5) There is always the possibility that customers from high-risk/blocked countries try to use Pretense Flip N.V's services. There is also a possibility that customer accounts become high-jacked by parties in high-risk/blocked countries. The risk for the transfer of funds across borders from high-risk/blocked countries is also considered as a possibility
	Impacts
	High (5) The Impact of the threats not being sufficiently addressed are considered to be high.
	Risk Evaluation High (12)
Measures	

The company has in place a number of both technological and organisational controls to mitigate the above risks. These include:

- System alerts in place to trigger when a customer registers from a high-risk/blocked country.
- System alerts in place to trigger if a customer uses VPN, Proxy or Bots to register.
- The non-offering of Peer-to-Peer gambling. By not offering Peer-to-Peer gambling, Pretense Flip N.V ensures that their products cannot be used for the transfer of funds from high-risk countries.
- Deposit and Withdrawal Reviews. These provide step by step instructions on the checks to be carried out on customer's deposits and withdrawals, including checks on the payment instrument to confirm that it matches the customer's origin.
- Suspicious Transaction/Activity Reports. Internal procedures include escalation of STR/SAR reports when due diligence checks indicate a suspected, known or it is reasonably expected to suspect a client or a transaction to form part of an attempted or potential case of ML/FT.

Controls	Actual Risk
- Analyst quality control reviews by Seniors and Manager - Weekly AML team meetings - Internal Audit Function review of process documentation	Medium (10) The risks are mitigated through overlapping and meshed processes and automated checks which substantially reduce the likelihood of the risks from occurring. Although the risks can never be completely eliminated the controls are tweaked on an ongoing basis to improve through lessons learnt.

4.3.5 PAYMENT INSTRUMENT RISKS

Vulnerabilities and Threats	Likelihood
In contrast with land-based operators, remote gambling operators do not accept cash deposits. Pretense Flip N.V only allows deposits to the gambling account from a payment service provider and thus never accepts cash. Most remote gaming operators, and Pretense Flip N.V in particular, where possible, return funds and winnings to customers by using a Closed Loop methodology. This restricts the possibility of laundering the funds though may still be used for layering purposes. However, some deposit methods are considered to be closely related to cash. The use of prepaid vouchers is one such payment method. Some payment instruments do not perform identification details screening when a payment is requested and thus may be used by third parties who may not have the full ownership details of the payment instruments. Mobile payment services are prone to be used in criminal activity and due to the possibility of making transactions in real time with high amounts. Some payments instruments may not offer, or a customer may choose to turn off, security measures designed to ensure a high level of security in processing of transactions (e.g. Two-factor authentication). Another consideration is the speed in which multiple transactions may be made and the expectation by customers of immediately being provided access to their funds at deposit or withdrawal stage. This increases the pressure on remote gambling operators to carry out their responsibilities without delaying a customer's experience. Common threats considered: - Customers using third party payment instruments, with or without the holder's permission, including stolen or hacked payment instruments (5) - Customers letting other people send funds to their account, when the funds originate from crime. (5)	Medium – High (1-5) The company and most of the remote gaming industry have suffered fraud in the past at the hands of criminals. The relative ease of customers to obtain multiple payment instruments, makes it also more likely that they will use more than one payment method.
	Impacts High (5) The Impact of the threats not being sufficiently addressed are considered to be high.
	Risk Evaluation
	High (5-25)

- Customers using prepaid vouchers (5) - Multiple payment instruments used by the same customer, and withdrawals requested to different payment instruments from those which were used to deposit (4) - Payment instruments being used to move funds for terrorist related activities (1)	
Measures	
The company has in place a number of both technological and organisational controls to mitigate the above risks. These include: - Closed Loop Policy. The company applies, to a large extent, a closed loop policy where customers are allowed only to withdraw to payment instruments that they have used to deposit. Since the customer's payment methods are verified, a withdrawal cannot be made to an unverified method. In view of cases where this cannot be performed due to payment instrument limitations or other events (such as payment card expired, does not allow withdrawals, or has been cancelled), the company requires that a customer completes due diligence procedures. - Deposit and Withdrawal Reviews. These provide guidelines on the checks to be carried out on customer's deposits and withdrawals, including due diligence checks on the payment instrument to confirm ownership, source of funds and source of wealth, real use of funds for the expected activity, provenance of winnings, legitimacy of losses, wagering patterns etc. - Suspicious Transaction/Activity Reports. Internal procedures include escalation of STR/SAR reports when due diligence checks indicate a suspected, known or it is reasonably expected to suspect a transaction to be part of an attempted or potential ML/FT transaction. - Daily, Weekly and Lifetime Reports. The company has in place customer risk assessments and creates reports that provide oversight for customers' total deposits and withdrawals on a daily, weekly and monthly basis. These reports also identify customers whose financial activities reach thresholds set internally or by applicable legislation. Analysts review these reports on a daily basis to identify the overall risk that clients present to the business and for ML/FT risks.	
Controls	Actual Risk
- Analyst quality control reviews by Seniors and Manager and approvals to be obtained for large withdrawal transactions. - Weekly team meetings. - Internal Audit Function review of process documentation;	Medium (10) The risks are mitigated through overlapping and meshed processes which substantially reduce the likelihood of the risks occurring. Although risks can never be totally eliminated the controls are tweaked on an ongoing basis to improve through lessons learnt. There is also always a factor of human error to take into account.

4.3.6 PRODUCT RISKS

Vulnerabilities and Threats	Likelihood
The company provides the opportunity for customers to place bets on three main verticals: live casino table games, non-live table games, table games and electronic casino games (e.g., slots). These are provided via different game suppliers which have all been certified. The company has identified that gaming products may have a potential vulnerability to be abused for the purpose of money laundering. Commercial online gambling is a form of gambling which is characterized by a high turnover and a very high number of transactions. Large sums are frequently in use. This can make the products vulnerable for money laundering since criminals may use money from criminal activity to play the games for entertainment purposes (consumption of illegally obtained money) or in order to turnover illegally obtained funds and thereby conceal their true origin. This is the main risk connected with Pretense Flip N.V.'s products. The many transactions and turnover puts high demands on Pretense Flip N.V. as an operator to monitor and follow up on suspicious patterns and other behaviour outside the normal use of a gambling account. Gambling accounts may also be used to deposit and store illegally obtained funds, and such funds may be transferred to a different bank account than used for deposit. Such funds can sometimes be used for gambling to conceal the real reason for deposit and is something that Pretense Flip N.V. is exposed to due to the use of gambling accounts. A vulnerability occurs in particular when players' funds may be willingly lost to another player (collusion) or when a game pot is won by a single individual or shared between the winners. Live Casino table games (Untreated risk level = High)	High (5) The risk of money laundering is considered to be high due to its products are characterised by high turnover and a large number of transactions. There is a risk that criminals spend illegally obtained funds on the products offered by the company for self-enjoyment.
	Impacts
	High (5) The Impact of the threats not being sufficiently addressed are considered to be high.
	Risk Evaluation High (10-20)

When it comes to collusion, this is not possible when it comes to Pretense Flip N.V Live Casino offering. When it comes to live casino games, the games are never purely peer-to-peer. When a player loses, he loses to the house. In other words, all games are played against the house, and hence not against other players. A players' funds are therefore never passed on to another player directly.

The intensity of transactions related to Live Casino table games is relatively high. The games are played at relatively high speed and a big number of bets can be made in a short period of time. This indicates higher risk.

In general, the stakes and potential winnings related to Live Casino table games are somewhere in the middle from an online operator industry perspective. The potential winnings per placed bet are not generally to be regarded as high. The actual placed stakes per bet are, however, usually higher compared to other forms of gambling. This also indicates higher risk.

Electronic Casino games (Untreated risk level = High)

When it comes to collusion, this is not possible when it comes to Pretense Flip N.V Electronic casino games offering (slots). Electronic casino games are never peer-to-peer, as the games are single player and purely based on RNG. When a player loses, he loses to the electronic casino. In other words, all games are completely computer simulated, and hence not against other players. A players' funds can therefore never be passed on to another player.

The intensity of transactions related to electronic casino games is high. The games are played at a high speed and a significant number of bets can be placed in a short period of time. Furthermore, the turnover of said games are high. This indicates high risk for money laundering. However, the stakes placed in electronic casino games are not usually very high per bet. However, the potential winnings related to Electronic Casino games are the highest from an industry perspective. The potential winnings per placed bet is high, but so are the odds per placed bet.

The company understands that there are specific money laundering risks related to gambling products. The two biggest risks the company is exposed to are 1) gambling with money from criminal activity for entertainment purposes, 2) being used for the purpose of depositing illicit funds (with or without connected turnover of said funds Common threats considered: - Customers making use of proceeds of crime for self-enjoyment (5) - Customers depositing illegally obtained funds on their account with the purpose to conceal its origin (5)	
Measures	
The company has in place a number of both technological and organisational controls to mitigate the above risks. These include: - The non-offering of Peer-to-Peer Gambling. By not offering Peer-to-Peer gambling, Pretense Flip N.V makes sure that their products cannot be used for collusion purposes. It should also be noted that Pretense Flip N.V does not offer poker. - Customer Acceptance Policy (CAP). This defines the general policy of the company about which customers it is willing to accept to enter into a business relationship with. Customers are only accepted for the purpose of being provided with entertainment through a remote betting and gaming service. This policy clearly defines that the company is not willing to-accept individuals who want to be anonymous, who are otherwise considered to want to use a gambling account to conceal funds with illicit original, against whom there are sanctions or who emanate from high-risk jurisdictions. The CAP establishes the requirement for approval by Senior Management of potential PEP clients and enhanced due diligence process and ongoing monitoring for such customers. The CAP also specifies that the company is to conduct ongoing monitoring of accepted customers and does not allow the use of clients' accounts by third parties or through the use of obfuscating technological means. - Deposit and Withdrawal Reviews. These provide guidelines on the checks to be carried out on customer's deposits and withdrawals, including due diligence checks on the payment instrument to confirm ownership, real use of funds for the expected activity, provenance of winnings, legitimacy of losses, wagering patterns etc. - Suspicious Transaction/Activity Reports. Internal procedures include escalation of STR/SAR reports when due diligence checks indicate a suspected or known transaction or it is reasonably expected to suspect a transaction to be part of an attempted/potential ML/FT transaction. - Daily, Weekly and Lifetime Reports. The company has in place customer risk assessments and creates reports that provide oversight for customers' total deposits and withdrawals on a daily, weekly and monthly basis. Analysts review these reports on a daily basis to identify the overall risk that clients present to the business and for ML/FT risks.	
Controls	Actual Risk
- Analyst quality control reviews by Seniors and Manager and approvals to	Low (4)

be obtained for large withdrawal transactions. - Weekly team meetings. - Internal Audit Function review of process documentation	The multiple levels of checks carried out on an ongoing basis lower the likelihood of any money-laundering occurring specifically related to the products the company offers.
--	--

4.3.7 INTERNAL RISKS

Vulnerabilities and Threats	Likelihood
The company understands that although ML/TF mainly occur as a result of external risks, it must mitigate against the internal risks as these may lead to the company being used for such aims. The company is not heavily dependent on automation for identifying suspicious ML/FT activity. Most measures rely on human intervention and thus the company is more exposed to the human element rather than technology. Common threats considered: - Employees not suitable for positions where they are key to AML/CFT controls' effectiveness (2) - Employees colluding with customers (1) - Tipping off (in/voluntarily) (1) - Employees slacking in AML/CFT procedures (2) - Employees not trained to effectively mitigate ML/TF Risks (1) - Technology tools used in AML/CFT measures and controls not operating properly (1) - Risk of infiltration or direct ownership of gambling companies by organised crime (1) - There is a risk of Gambling Companies being used as tools for criminal owners wanting to launder money. (2)	Low (1-2)
	Impacts
	High (5) The Impact of the threats not being sufficiently addressed are considered to be high.
	Risk Evaluation
	Medium (5-10)
Measures	
The company has in place a number of organisational controls to mitigate the above risks. These include: - Screening. All new employees at engagement stage are requested to provide references and Police issued criminal conduct certificates. - Training. All new/reassigned employees are provided induction and, on the job, coaching during their initial assignment period. This is assessed by Seniors and employees provided additional training on the job. All relevant employees have completed AML/CFT	

awareness training. AML/CFT Procedures are explained and available for all employees to access on Confluence system. - Assessments. Regular assessments are made of employees' performance. - Senior approvals. Significant withdrawals necessitate a Senior's approval. - Whistleblowing procedure. The company has in place a whistleblowing procedure which can be used for whistleblowing on irregular practices by fellow employees or supervisors, inappropriate systems etc. - Staffing levels. The company maintains sufficient staff to cover tasks efficiently and these would be matters for which the company can mostly plan in advance depending on sporting calendars and seasonality.	
Controls	Actual Risk
- Analyst quality control reviews by Seniors and Managers and approvals to be obtained for large withdrawal transactions - Authorisation by Seniors of large transactions - Bi-weekly AML team meetings.	Low (4) Pretense Flip N.V Ltd's employees are provided the necessary training to perform their job and the company carries out the necessary monitoring and controls to ensure that Policies and Procedures are correctly adhered to.

4.4 RISK PROFILES

Below is a guide to what we deem to be a certain risk level based on trigger alerts or monitoring of customers account.

4.4.1 LOW RISK

Customers who sign up and have either not deposited or triggered any trigger events via there deposit method is automatically assigned a Low-Risk customer. Due to the nature of the business these customers are usually just one-time depositors or occasional customers who do not exceed any of our stipulated threshold to warrant further investigations.

Additionally, customers who have been given a higher risk rating can be set back to low risk if their identities have been fully verified and/or their source of wealth has been well defined. This is always dependent on each customer's specific pattern.

4.4.2 MEDIUM RISK

Customers who pose a higher than average risk to the business may be assigned Medium Risk. This is always dependant on their Country of Origin, IP, Registered country, Deposit amounts/pattern and trigger events.

Medium Risk Factors Include:

- Non closed loop withdrawal attempt
- Payment Method Used
- 3K Deposit Threshold Limit Reached
- Third Party Deposit
- Velocity Limits
 - CC Deposits of 500 euros within 24 hours
 - CC Fraud Risk (5 failed deposit via CC due to Card expired, no funds on card, 3DS/CVV failure)
 - Deposit of 5000 euros accumulated and payment method is not verified
- Bin - Country Mismatch
- Stolen/Restricted Card Used
- IP Mismatch with Country
- IP Link with other customers
- Multiple deposit attempts via different payment methods
- Multiple deposit attempts via CC in a descending pattern

For all customers who have been assigned a medium risk tag the Analyst will

- Request KYC as applicable
- If KYC was requested before, the re-check will be applied and a note will inform of the date and outcome
- Proceed with Enhanced Due Diligence if required
- Conduct CRA
- Based on 2K Deposit Threshold alert profiling will be conducted on customers' accounts. If no profiling is found the Source of Funds Questionnaire will be requested.
- Restrict player's account as required until a satisfactory outcome has been achieved
- Leave pending Withdrawal in a n ON-Hold Status to prevent it from being paid out

4.4.3 HIGH RISK

Players who are identified as "High Risk" may be subject to enhanced/intensive due diligence measures based on their risk assessment.

High Risk Factors Include:

- Fake/Photoshopped Documentation received
- Customer refusing to send documents (CDD, EDD, SOF, SOW etc.)

- Payment Method Used
- Unclear SOW received
- Deposits above average amounts from countries defined as High Risk
- Customers triggered as a Politically Exposed Person or is on a Sanctioned List
- Customers account Hacked or created by third party
- IP Login from non-reputable jurisdiction (Not accepted as clients)
- Players residing in non-reputable jurisdictions (Not accepted as clients)
- Registrations under legal age confirmed through KYC (Not accepted as clients)
- Fake Registration Information
- 15K (Net Deposits), 40K, 100K+ accumulated Deposits (Dependant on payment method risk)

For all customers who have been assigned a high risk tag the Analyst will

- Request KYC as applicable (Place of Birth and Nationality)
- Proceed with Enhanced Due Diligence if required
- Send SOW questionnaire and request SOW supporting documentation as applicable
- Restricted player's account as required until a satisfactory outcome has been achieved
- Leave any pending Withdrawal in an ON-Hold Status to prevent it from being paid out.
(There is an automatic rule in place that any customers who has tag assigned DC:RPF_PendingDocs will have any future withdrawals set to On-Hold status – Agents cannot pay this out without removing this status)

4.4.4 PAYMENT METHOD RISKS

	Low	Low-Medium	Medium	Medium-High	High
Bank transfers (EEA or equivalent safeguards)	X				
Debit/credit cards issued by banks (EEA or equivalent safeguards)	X				
Debit/credit cards issued by other licensed financial institutions		X			
EEA-licensed payment service providers			X		
Non-EEA licensed PSP				X	
EEA-licensed PSP that can be funded with cash or quasi-cash				X	
Prepaid cards/vouchers					X
Cryptocurrencies					X
Peer to Peer transfers					X
Cash					X

5. PEP'S. SANCTIONS AND ADVERSE MEDIA

5.1 POLITICALLY EXPOSED PERSON CHECKS

The Company must carry out PEP checks at the first possible opportunity.

When a player is a confirmed PEP, it will be classified as high risk and senior management approval will be sought before any business is undertaken. In such cases, adequate measures will be taken to establish the source of funds and source of wealth involved in the prospective business relationship. If senior management decides to establish a relationship with the PEP, enhanced ongoing monitoring will be carried out in order to mitigate this high risk.

As a general company policy, the Company prefers not to accept any Peps, however senior management has discretion to alter the policy.

Politically Exposed Person is defined as any of the following resident in any country:

(a) a natural person who is or has been entrusted with prominent public functions, including —

- a head of state, head of government, minister or deputy or assistant minister;
- a senior government official.
- a member of parliament.
- a senior politician.
- an important political party official.
- a senior judicial official.
- a member of a court of auditors or the board of a central bank;
- an ambassador, chargé affairs or other high-ranking officer in a diplomatic service;
- a high-ranking officer in an armed force.
- a senior member of an administrative, management or supervisory body of a State-owned enterprise;
- a senior official of an international entity or organisation; and
- an honorary consul.

(b) any of the following family members of a person mentioned in sub-paragraph (a) —

- a spouse.
- a partner considered by national law as equivalent to a spouse.
- a child.
- the spouse or partner of a child;
- a sibling.
- a parent.
- a parent-in-law.
- a grandparent; or
- a grandchild.

(c) any close associate of a person mentioned in sub-paragraph (a), including —

- any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;

- any natural person who has sole beneficial ownership of a legal entity or legal arrangement that is known to have been set up for the benefit of such a person;
- any natural person who is in a position to conduct substantial financial transactions on behalf of such a person.

These clients are classified as High risk.

Any client which is flagged in these lists:

- Will have his account locked.
- the client may be asked for enhanced due diligence to verify the customer.

Clients in this list are required to send:

- Passport/Driver's licence
- Send an original utility bill not older than 3 months.
- Any other documentation that is deemed necessary.

5.2 SANCTION CHECKS

Sanction checks are carried out upon registration.

If in the event a Sanction check was missed and a transaction has occurred, or in the event a current customer is now on the Sanctions List and previous transactions have occurred, the account will be marked as high risk and the account will be frozen (all transactions will be stopped from going through).

An email will be sent to management and the MLRO to inform of this occurrence.

Sanctions List means the "Specially Designated Nationals and Blocked Persons" list maintained by OFAC, the Consolidated List of Financial Sanctions Targets and the Investment Ban List maintained by HMT, or any similar list maintained by, or public announcement of Sanctions designation made by, any of the Sanctions Authorities.

As a general company policy, the Company will not accept any Sanctioned Individuals

These clients are classified as High risk.

Any client which is flagged in these lists:

- Will have his account locked.
- the client may be asked for enhanced due diligence to verify the customer

Clients in this list are required to send:

- Passport/Driver's licence/ID
- Send an original utility bill not older than 6 months.
- Any other documentation that is deemed necessary.

5.3 ADVERSE MEDIA

Adverse media, from a compliance perspective, is generally considered to include allegations found in reputable news and other publications that link a person or entity to involvement in money-laundering, corruption, sanctions exposure, terrorism and threat financing, or other unlawful activity.

These checks can include news articles, social media posts, legal documents and other sources. They can help us identify any potential risks or red flags associated with a person or entity.

These clients are classified as High risk.

Any client which is flagged in these lists:

- Will have his account locked.
- the client may be asked for enhanced due diligence to verify the customer

Clients in this list are required to send:

- Passport/Driver's licence
- Send an original utility bill not older than 3 months.
- Any other documentation that is deemed necessary.

5.4 SOURCES

The tables below outline the sources provided along with their individual definitions:

Sources	Summary
HMT	Office of Financial Sanctions Implementation HM Treasury (www.gov.uk)
OFAC	Office of Foreign Assets Control (www.treasury.gov)
UN	United Nations Security Council Sanctions List (www.un.org)
EU	European External Action Sanctions list (http://eeas.europa.eu)
AUSTRAC	Australian Transaction Reports and Analysis Centre (www.austrac.gov.au)

5.5 RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE

Pretense Flip N.V. may utilize specialized external service providers to assist in the collection and verification of customer identity information, including Politically Exposed Person (PEP) screening, sanctions screening, document validation, and adverse media checks. These providers include systems such as Sumsub, Hooyu, and SEON, which are integrated into the onboarding and ongoing monitoring processes.

While such providers are used to enhance operational efficiency and accuracy, the Company retains full responsibility and accountability for meeting its AML/CFT obligations under Curaçao law. The use of these services does not constitute legal reliance as defined under Article 3(3) of the National Ordinance on Identification of Clients (NOIS), but is instead a technical support measure to facilitate internal controls.

The Company ensures that:

- All data provided by third-party systems is reviewed and validated by internal analysts;
- A full audit trail of verification checks is maintained;
- Manual review is conducted where automated results are inconclusive;
- Third-party systems are vetted regularly to ensure they comply with applicable data security and AML standards.

6 CUSTOMER DUE DILIGENCE

Following international standards and local applicable legislation, it is imperative for a company to know its clients. An individual cannot participate in a game for money unless that individual has registered and has been provided with a Player Account. Only one Player Account is permitted per person, per family and per Shared Environment.

6.1 SIMPLIFIED DUE DILIGENCE

A Simplified Due Diligence process will be the first stage of a risk based process. Simplified Due Diligence is carried out on Registration.

An individual cannot participate in a game for money unless that individual has registered and has been provided with a Player Account. Only one Player Account is permitted per person, per family and per Shared Environment.

To be registered as a Player and be able to deposit, an individual must register personally and submit the following KYC information:

- Date of Birth
- Country of Residence
- Player's first and last name.
- Player's full residential address.
- Player's valid email address.
- a username and a password

On registration, a geographical location check is carried out on the applicant's computer IP to ensure that person is in a permitted jurisdiction. If the applicant is not in a permitted jurisdiction, he/she will not be allowed to continue the registration process. The Company proceeds to review the information provided and may request additional documentation in order to verify the provided information. The Player Account may be put on hold until satisfactory information has been received or terminated if the Company finds the information contained in the Player Account to be false or misleading.

The Company reserves the right to refuse to open or close a Player Account at its own discretion following review of the provided KYC information.

Log in details

It is not permitted for a Player to share the login details to access the system with a 3rd party. The Company reserves the right to cancel, without refund, a Player Account if the login details were disclosed to a 3rd party.

6.2 CUSTOMER DUE DILIGENCE

In order to verify the details on their account, the company must ask the customer to send a photo or scan of one document from each of the categories listed below:

- Identity Card
- Valid Passport
- Driver's License

Address Verification - one of the following:

- 1) Utility bill (within last 3 months)
- 2) Current photo-card Driver's License (Provisional or Full) (Applies for UK DL's)
- 3) Current Full Driver's License (old style paper version)
- 4) ID card with address + Passport or additional ID
- 5) Bank/Credit Union/Building Society/Credit Card statement or passbook (within last 6 months)
- 6) Council tax bill or payment book (within last 6 months)
- 7) Recent mortgage statement (within last 6 months)
- 8) Current local council rent card or tenancy agreement (private tenancy agreements are not acceptable)
- 9) Home Insurance certificate or policy
- 10) Motor Insurance certificate or policy
- 11) Electoral roll
- 12) Credit reference agency
- 13) Mobile bills are not accepted.

Customer Due Diligence is conducted in the following cases:

- anytime during the Player onboarding.
- upon a request for withdrawal.
- when a threshold of a cumulative withdrawal of 2,000 €/ CAD or equivalent is reached;
- anytime at the discretion of the Company.

6.3 ENHANCED DUE DILIGENCE

Following a risk-based approach for customer due diligence, certain triggers or thresholds will require enhanced due diligence to take place. The triggers for the enhanced due diligence process to take place are as follow-:

- Customer identified as politically exposed persons (Peps);
- Lifetime customer deposits exceeding EUR 100000
- Customer identified as high risk when carrying out Risk Assessment.
- Customers identified at medium risk (if necessary)
- Standard Due Diligence identifies heightened risks.
- Significant anomalies in gaming or funding activity.

- Source of Wealth provided by customer cannot be verified following soft verifications and the customer is a High Spender or has Disproportionate Spending.

When performing Enhanced Due Diligence on a customer we always make sure to:

- Ask for additional ID Verification which include document showing Nationality and Place of Birth (Eg: Passport if only ID/DL is available)
- Ask for additional Proof of Address
- Ask for Payment methods proof.
- Ask for Source of Funds/Wealth
- Validation of documents – we can request certified copies of documents to validate name, address, date of birth and source of funds; and/or
- Internal corroboration of user identity – this could emanate from a variety of sources from customer monitoring, other databases, gaming activity etc.; and/or
- External corroboration – this can entail the use of a 3rd party solution to provide enhanced soft background checks on public records.

6.4 SOURCE OF FUNDS/WEALTH

Source of Funds refers to how the funds to be used in a particular transaction (or future transactions) will be generated.

Source of Funds checks consisting of the following:

- Last 3 Payslips
- Employment Contracts
- Proof of Deposits
- Bank Statements
- Inheritance Confirmations/Wills
- Investment gains
- Deed of Donation
- Sale of Real Estate
- Gambling Winnings
- Any additional document deemed necessary to deem how funds were generated.

6.5 SOURCE OF WEALTH QUESTIONNAIRE/DOCUMENTATION

Customer due diligence is an ongoing process and as a result there are trigger events which warrant the collection of supporting documentation.

Source of Wealth refers to how someone generated their wealth throughout their lifetime.

Upon classifying a player as High risk the client will be requested to complete a Source of Wealth (SOW) questionnaire and if warranted the client will be asked to provide SOW documentation.

6.6 KYC DOCUMENTATION REVIEW

It is understood that the players may not have at hand the requested information thus the company has determined an acceptable timeframe of 30 days shall pass before we close the customer's account.

During this period, the players' account will remain partially operational.

Once all documentation is at hand, period reviews will be performed on customers KYC.

Risk Rating	Frequency from date of last review or customer interaction	Registered through conventional channel
High	Every 3 months or upon withdrawal	Check Identification document expiry date, collect new one was warranted and assess if an updated SOW document needs to be collected
Medium	Every 6 months or upon withdrawal	Check Identification document expiry date, collect new one was warranted and assess if an updated SOW document needs to be collected
Low	As triggered through the transaction monitoring process	Check Identification document expiry date, collect new one was warranted and assess if an updated SOW document needs to be collected

6.7 CLIENTS REFUSING TO SEND DOCUMENTS

Any client who refuses to send documents will have their account disabled.

Customer Support will try to explain to the client the importance of receiving and verifying their documents, however if the client is still refusing to listen and will not send documents, the customer's account will be reviewed for any suspicions of AML/CFT.

The MLRO will be notified if any accounts are deemed suspicious and will then review the clients account and communications and consider whether to submit an STR to the FIAU, providing all details and information as appropriate, if the MLRO decides not to submit an STR they need to include their reason/s in the suspicious register.

Once it is stipulated that their account is of no risk the customer's funds will be remitted back to the same source and channels used for depositing.

7 MONITORING

7.1 DAILY MONITORING

A number of on-going monitoring checks are done on a daily basis that prevents fraudulent and/or unwanted clients.

These checks include:

- **Peps and Sanctions** – Triggers alerts if a customer is a PEP or on a Sanctions list.
- **Velocity Checks** – Different trigger alerts depending on the Deposit pattern of customer.
- **Possible Stolen Card** – Report showing customers who tried to deposit, and we receive an alert stating card might be issues as Stolen, Lost, Pickup, Special or Restricted
- **Bin Mismatch** – Credit Card Bin is difference to the Registration Country of the customer.
- **Same Payment method used** – Customer has deposited with account details of another customer already in the system.
- **Credit Card Name Mismatch** – Customer Name on Credit Card deposit is different that customers account name.
- **Threshold Report** – Customers who exceed DepositThreshold limits.
- **CRA** – Customer Risk Assessment
- **Multiple IP** – Customers logging in and created accounts from the same IP address.
- **Duplicate/Multiple Accounts** – Customers creating accounts with similar data as another account already in the system.

Security technologies are in place generating automated alerts which are thereafter thoroughly investigated by the department. The presence of any irregular, suspicious, inappropriate or fraudulent activity or any attempt thereto, will cause the pertaining Player to be classified as High risk for which EDD procedures are implemented.

Player accounts are reviewed and monitored for the presence of any of the following situations:

- the provision of fake, false, incorrect, misleading, non-existing, KYC information which do not belong to the Player or are unable to be verified.
- provision of fictitious names such that the true beneficial owner is not known.
- the detection of inappropriate play and/ or fraudulent activity
- the detection of irregular Player activity including but not limited to the placing of zero-risk or even bets.
- complex or large transactions or groups of transactions which are likely, by their nature to be related to money laundering or the funding of terrorism.
- upon suspicion of a Player attempting to or having created multiple Player Accounts in multiple different names
- upon suspicion of Player(s) being part of a syndicate of Players colluding to gain an advantage over the Company
- at the detection of any irregular, suspicious, inappropriate, or fraudulent activity
- anytime, at the discretion of the Company
- fraudulent or unlawful use of the system by Players, to break into or otherwise circumvent the security measures set up by the system.
- The use of any software program endowed with Artificial Intelligence
- attempt to log in from a Non-reputable Jurisdiction or a High-Risk Jurisdiction.

As a rule, all withdrawals are checked before being processed. These checks include:

- Ensuring withdrawal is following the close loop policy where possible.
- Checking lifetime deposits and withdrawals as some additional KYC might be required.
- Ensuring KYC documentation is still valid and not expired.
- Checking Wagering was done, and turnover of all deposited funds was achieved.
- Assessing gameplay patterns
- Making sure no issues are relevant in previous notes on account.

7.2 SUSPICIOUS BEHAVIOR

Below provide some examples of what the Company considers suspicious in relation to a client's behaviour or transactions.

Suspicious Indicators:

- Information provided by the client contains a number of mismatches (e.g., email domain, telephone or postcode details do not correspond to the country);
- The registered credit card or bank account details do not match the client's registration details;
- The client tries to open multiple accounts under the same name;
- The client tries to open several accounts under different names using the same IP address;
- The source of funds being deposited appears to be suspicious and it is not possible to verify the origin of the funds; or
- The client has links to previously investigated accounts.
- Suspicious Transactions
 - Deposit high and low amounts from multiple payment methods
 - Deposit in a descending pattern from the same CC and all are failed.
 - Multiple failed CC deposits for Incorrect information entered.
 - Abnormal number of High withdrawals
- The client logs on to the account from multiple countries.
- Different clients are identified as sharing bank accounts from which deposits or withdrawals are made.
- E-wallets that are registered with different names.

As explained in Section 4 of the risk based approach, all customers are reviewed depending on certain triggers or reports received.

CRA's are conducted if a customer:

- Appears in any fraud report that requires the need for documents.
- Any period in customer lifetime that we deem necessary.

CRA's are not only conducted once but are conducted at every trigger event mentioned above.

All CRA's are given a score, depending on customers score we request the appropriate documentation and follow the necessary actions as highlighted below.

Customers marked as:

LOW

- Monitor for unusual activities at the withdrawal stage, and verify the information is up to date.
- Report any Suspicious cases of ML/FT

MEDIUM

- Make sure we have verification of personal details and payment methods.
- On-going monitoring to detect unusual activities, and keep information and profile updated
- Search social media sites and negative search for additional information. If none is found regarding customers' income, Source of Wealth Questionnaire is sent.
- Report any Suspicious cases of ML/FT

HIGH

- Make sure we have verification of personal details and payment methods.
- Collect Source of Wealth Documentation
- Enhance ongoing monitoring to detect unusual activities, and keep information and profile updated.
- Review the account in-depth to address and identify any other potential risk.
- Report any Suspicious cases of ML/FT

In addition to the above all High Risk accounts are reviewed on a 3-month basis by agents

7.4 CUSTOMER BUSINESS PROFILE (EXPECTED LEVEL OF ACTIVITY)

We develop a customer risk and business profile in order to detect unusual activity in course of business relationship with the customer.

In order to build a profile and to predict expected level of activity, we collect information via search of social media sites, negative searches online and public records.

In case if no evidence can be found via media searches, we will ask the customer to fill in the SOW questionnaire.

8 GENERAL POLICIES

8.1 CUSTOMER ONBOARDING PROCESS

Customer onboarding is an important part of our operational procedures which define our approach when onboarding customers and setting rules for managing the customer relationship.

All customers are required to enter their Email, Country, and Date of Birth upon registration.

Before a deposit can be made customer is then required to enter their Name, Surname, Address, and phone number. Customers will also be reviewed for PEP and sanctioned status following their first effective deposit. We do not accept business from either of these.

Customers will not be able to deposit or withdraw any funds if they have not entered this information. Customers are also forbidden from having anonymous account or account with fictitious names.

This is the general process of identification for customers which happens prior to the business relationship. Verification of the customer is done at a later stage.

In addition, at the very beginning of the customer relationship we have defined that a minimum of the following customers cannot be allowed to register.

- Persons residing in countries outside our risk appetite.
- Players under the age of 18

8.2 TRANSACTION MONITORING PROCESS

The purpose of the transaction monitoring process is to detect and prevent any suspicious or fraudulent activities, ensure compliance with AML regulations and maintaining the integrity of our platform.

All deposits are monitored automatically with the help of velocity checks which include alerts for customers who

- Deposit while having a large balance
- Deposit over 1000 in 24 hours and payment method is not verified
- Deposits over 3000 and payment method and kyc is not verified
- Has more than 10 failed CC deposits with 1 hour by the same card.
- Deposit using a CC with a stolen/pickup card alert
- Deposit with a card already registered to another account

At withdrawal stage a manual review is conducted of the customer's account and ensure that the name of the depositing and withdrawal methods match the name on the account.

In any instance of any other type of fraud is noted, documents will be requested to verify account.

8.3 SUSPICIOUS ACTIVITIES

If an Account Holder has unusual deposits and gets flagged by the system, the Company will perform an investigation in which the Account Holder may be requested to provide further information. The Company will suspend the account until further documentation is in place. If the Account Holder has not provided satisfying information within 30 days, the account will be terminated. The MLRO will proceed with the reporting of the unusual transaction to the relevant authority.

8.4 WAGERING REQUIREMENTS

For every deposit made we enforce wagering requirements on customers. We expect all customer to fully wager (Turnover) their deposited funds. By requiring customer to wager their funds we can establish a transactional history and paper trail of the customers activity.

This transactional history and paper trail can be useful in identifying and detecting suspicious or unusual activity, which can be a sign of money laundering or other illegal activities. By analyzing the customer's transactional history and gambling patterns, we can identify any unusual or suspicious activity, such as a sudden increase in the amount of money wagered or frequent deposits and withdrawals, which may indicate money laundering or other illegal activities.

These wagering requirements also provide a layer of protection against fraud and other financial crimes by ensuring that customers cannot simply deposit funds and withdraw them without engaging in any activity. This can help to prevent customers from using our services to launder money or transfer funds to illegal sources.

When a customer refuses to wager any funds these accounts are reviewed and escalated to the MLRO. No withdrawal will be made without approval of the MLRO.

8.5 WITHDRAWALS

Withdrawal requests must be made from a Player Account. Withdrawal requests sent by any other means of communication will not be processed.

The Company will not deposit withdrawn funds to another source from which it was originated. If for any reason this is no longer possible, the Company will request additional verification documentation evidencing the details and ownership of the new withdrawal method.

Transfers or pay outs will only be made to the Player. Transfers to third parties are not permitted.

Before processing any withdrawals, the Company will conduct additional review of the Player Account for any irregular activity such as money laundering or suspicious play such as:

- the placement of a deposit without having placed any bets, or only to receive free spins. A Player must have always placed at least his deposit amount in bets before proceeding to withdraw the funds.

- the possible creation of multiple Player Accounts in multiple different names
- possible collusion between Players.

Upon the occurrence of any of the instances mentioned above, the Company may decide to withhold funds and proceed to further request EDD documentation or conduct further investigation and resolve to:

- suspend the Player Account until receipt of sufficient verification information, where still applicable.
- immediately block the access of a Player to the system or to his/ her account and seize all funds held in the account.
- close or terminate a Player Account and seize all funds held in such account,

Followed by the report of the activity to the MLRO.

8.6 CYRPTOCURRENCY TRANSACTIONS

Cryptocurrency transactions are only possible if the initial deposit was made with a crypto currency. Following this transaction all transactions (deposits, wagers and withdrawals) with the Player must be conducted using the same crypto currency as with the first deposit.

The Company will at no time sell/buy/exchange crypto currency with and/or to FIAT currency.

The Company is bound by the following requirements as set by the Master License Holder:

- Collect and verify proof of identity and proof of address as described above in the 'Client Due Diligence' paragraph and to make sure that a Player is over 18 years of age.
- Collection and storage of hardware KYC in all pathways from signup, login, deposits and withdrawals, including but not limited to IP address, mac address and browser information to ensure that all wagering, deposits and withdrawals are to/from the same Player (IP and computer).
- The Company will make available to the Master License holder on demand and provide proof of balance as acceptable by the Master License Holder, to ensure Player's funds have been deposited.
- Provide proof of Solvency to the Master License Holder on a periodic basis (weekly, monthly) to ensure that operator has all funds to cover all bets and jackpots and that the crypto currency is kept in a separate account.
- The Company will display the rate of exchange from crypto currencies to FIAT currency on the home page of the Website. In no way shall the Company make exchanges between any crypto currency and any FIAT currency.
- The Company must include in their Terms and Conditions and highlights that crypto currency values can change dramatically depending on the market value.

It is important to note that due to the current anti-money-laundering regulations, the Player may deposit money into the Player Account only to play and to use the Services. Likewise, the Player may only withdraw winnings and not the funds deposited into the Player Account.

Players who deposit and withdraw without gaming activities will have their funds blocked until further notice. The Company is not a financial institution and does not grant interest on deposits. In

any case, the Company reserves the unlimited right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

Notification of new payment methods will be made on the homepage of the Website and sent by e-mail to the Account Holders as they are added. For each new depositing method, this Manual and the Terms and Conditions on the Website will be updated accordingly.

8.7 SECURITY REVIEW

The Company reserves the right to conduct a review at any time to validate the identity, age and/or registration data provided by the Account Holder to verify the use by the Customer of the provided services for any breach of the Terms and Conditions and any applicable laws. At the moment of registration the applicant provides the Company with authorization to make any relevant inquiries pertaining to his person and to use and disclose information to any third party considered necessary in order to conduct its verification checks.

Third party agencies may be engaged to confirm the provided age, identity, address and payment details, the ordering of a credit report and/ or the verification of the provided information by checking it against certain public or private databases. All applicant/ Account holders are made aware that by accepting the Terms and Conditions of the Company, they agree that the provided information may be used, recorded and disclosed and that the data may be recorded by the Company or third party engaged.

The review may be performed from time to time at the discretion of the Company and/or due to regulatory, security or other business reasons, During the review the Customer may be restricted from withdrawing funds from the account and/ or prevented from accessing certain Services offered on the website.

8.8 FINANCIAL INSTITUTIONS

We prohibit the opening and keeping of accounts with financial institutions operating without the required authorisation or licence. This policy applies to financial institutions who are involved in financial transactions on our behalf.

We consider unauthorised financial institutions to be those that have not obtained the necessary authorisation or licence from the relevant regulatory authorities to operate as a financial institution. This includes entities that are not registered, licensed, or authorised by the relevant financial regulatory body in the jurisdiction where they are operating.

We require all employees, contractors, and agents to verify the authorisation or licence status of any financial institution with which they are considering opening or keeping an account. If the financial institution is found to be operating without the required authorisation or licence, the employee, contractor, or agent must not proceed with opening or keeping an account with that institution.

We take the prohibition of opening and keeping accounts with unauthorised financial institutions seriously and any violation of this policy may result in disciplinary action, up to and including termination of employment or engagement.

This policy is designed to protect our organization and our stakeholders from the risks associated with unauthorised financial institutions, including the potential for fraud, money laundering, and other financial crimes. By adhering to this policy, we demonstrate our commitment to responsible financial practices and ethical behaviour.

We will regularly review and update this policy as necessary to ensure that it remains relevant and effective in addressing the risks associated with unauthorised financial institutions.

8.9 SHELL BANKS

We prohibit the maintenance of accounts and/or relationships with shell banks. This policy applies to all financial institutions of our organization who are involved in financial transactions on our behalf.

We consider shell banks to be financial institutions that have no physical presence in any country and are not affiliated with a regulated financial group. These institutions are typically used for illegal activities such as money laundering, terrorist financing, and other financial crimes.

We require all financial institutions to verify the presence of a physical office and regulatory authorization of any financial institution with which they are considering maintaining an account or relationship. If the financial institution is found to be a shell bank, the employee, contractor, or agent must not proceed with maintaining an account or relationship with that institution.

We take the prohibition of maintaining accounts and/or relationships with shell banks seriously and any violation of this policy may result in disciplinary action, up to and including termination of employment or engagement.

This policy is designed to protect our organization and our stakeholders from the risks associated with shell banks, including the potential for fraud, money laundering, and other financial crimes. By adhering to this policy, we demonstrate our commitment to responsible financial practices and ethical behavior.

We will regularly review and update this policy as necessary to ensure that it remains relevant and effective in addressing the risks associated with shell banks.

8.10 INTERNAL FRAUD

To prevent and detect internal fraud, we have:

- Established and communicated clear expectations for ethical conduct and integrity among all employees, contractors, and agents.
- Conducted thorough background checks and reference checks on all new hires and contractors.
- Segregated duties and responsibilities to prevent any one person from having too much control or access to sensitive information or assets.
- Implemented and enforced a system of internal controls to detect and prevent fraud, including regular monitoring and analysis of financial transactions and records.

- Provided regular training and education to all employees, contractors, and agents on fraud prevention, detection, and reporting.
- Encouraged and provide channels for reporting any suspected or actual fraud, including a confidential reporting mechanism.
- Investigated all reported incidents of fraud promptly and thoroughly, taking appropriate disciplinary action and, if necessary, reporting to the relevant authorities.

We take the prevention and detection of internal fraud seriously, and any violation of this policy may result in disciplinary action, up to and including termination of employment or engagement, and may also lead to civil or criminal liability.

This policy is designed to protect our organization and our stakeholders from the risks associated with internal fraud, including the potential for financial loss, reputational damage, and legal and regulatory sanctions. By adhering to this policy, we demonstrate our commitment to responsible financial practices and ethical behavior.

8.11 TESTING

To ensure the effectiveness of our AML policies, we will conduct independent testing on a regular basis. The independent testing will be conducted by a qualified third-party, who is not involved in the design or implementation of our AML policies.

The independent testing will assess the adequacy and effectiveness of our AML policies, procedures, and controls, and will identify any deficiencies or weaknesses. The testing will cover all relevant areas of our operations, including customer due diligence, transaction monitoring, reporting, and record-keeping.

The independent testing will be conducted on a regular basis, at least annually, or as otherwise required by applicable laws and regulations. The results of the independent testing will be reported to senior management and the board of directors, and any necessary corrective actions will be taken promptly.

We will ensure that the third-party conducting the independent testing has the necessary expertise, independence, and resources to conduct a thorough and objective assessment of our AML policies. We will also ensure that the third-party is provided with access to all relevant documents, records, and personnel.

Problem gambling can lead to financial difficulties and debt, which may increase the risk of individuals engaging in criminal activity to fund their gambling habits. This can make them vulnerable to exploitation by money launderers who offer to pay off their debts in exchange for using their bank accounts to move illicit funds.

To prevent and detect problem gambling, we:

- Provided training and education to all employees, contractors, and agents on the signs of problem gambling and the risks associated with it.
- Implemented and enforced a system of internal controls to identify and mitigate the risks associated with problem gambling, including customer due diligence, responsible gambling policies, and procedures for reporting and addressing suspected problem gambling.
- Monitor customer behaviour and transactions for signs of problem gambling, including unusual patterns of play, frequent or large deposits, and use of credit cards or other high-risk payment methods.
- Provide resources and referrals to customers who may be experiencing problem gambling, including self-exclusion programs and problem gambling helplines.
- Maintain strict confidentiality of all information related to problem gambling and ensure that all employees, contractors, and agents are aware of their responsibilities in protecting customer privacy.

9 MONEY LAUNDERING REPORTING AND TRAINING

9.1 THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

The Company has designated an MLRO who oversees the review of KYC information and the monitoring of Player Account activities. Specifically, the MLRO oversees the following:

Ensure a proper review of the Player Accounts by the personnel in relation to identification and verification of an Account Owner,

- Keep a list of registered Account Holders
- Monitor the reviews and investigations conducted by the designated personnel performed on the Player Account activities.
- Provide initial and ongoing training to all relevant staff ensuring awareness of their personal responsibilities and the procedures in respect of identifying Players monitoring Player activity, record-keeping and reporting any unusual/suspicious transactions.
- Cooperate with all relevant administrative, enforcement and judicial authorities in their endeavour to prevent and detect criminal activity.
- Ensure that this policy is adhered to, reviewed and maintained regularly.

9.2 REPORTING OF SUSPICIOUS TRANSACTIONS

Any transactions or circumstances for which the Company has not received sufficient verifying information for and/or of which the Company knows, suspects or has reason to suspect that any of the transaction(s), among other actions, (i) involve funds derived from illegal activities, (ii) are intended to conceal funds from illegal activities, or (iii) involve the use of the Company system to facilitate criminal activity, may give rise to its report to the FIU in Curaçao.

The Money Laundering Reporting Officer (MLRO) is in charge of the reporting with the relevant authority and will hold a list of all instances in which it did not consider it necessary to report. The decision not to report will be sufficiently supported.

9.3 RECORD KEEPING

The Company maintains a record of all relevant documentation on a separate database for at least five years after ending a business relationship. The Company is obliged to retain files in a way that enables investigating authorities to identify a satisfactory audit trail for individual transactions including the amounts, currencies and type of transactions. In specific circumstances, if ordered by rule of law and permitted by national law and the relevant authorities, the Company may provide copies of the records maintained.

9.4 STAFF DUE DILIGENCE

It is imperative that the Company's employees are of undisputed integrity. To ensure this objective, the Company follows a procedure whereby all applicants must produce a curriculum vitae, at least two references and relevant educational qualification certificates, and/or professional certificates, which are checked and verified by the Company's Human Resources Department.

9.5 STAFF AML TRAINING

Each Employee must complete a yearly AML Training course so that they are aware and updated of all the internal procedures and policies of the company and with the changes in the regulatory environment.

They are also trained on different forms of AML/CFT and any violations which may occur relevant to the products and services we offer.

9.6 PROCEDURES AND POLICY REVIEW

All AML/CFT procedures and policies are review yearly and are always approved by the MLRO and the Board of Directors.

9.7 MLRO CONTACT

The current Money Laundering reporting officer is Neil Caruana and can be contacted on neil.c@mtmgroup.io

10 COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

The Company is committed to upholding the highest standards of compliance with all applicable AML/CFT laws and regulations. This section outlines the obligations of stakeholders under this policy and the consequences of failing to comply.

10.1 COMPLIANCE OBLIGATIONS

All employees, contractors, consultants, and third-party providers involved in any aspect of the Company's operations are required to adhere to this AML/CFT policy and its supporting procedures. It is the responsibility of each individual to understand their role in detecting and preventing money laundering and terrorist financing.

Compliance includes, but is not limited to:

- Conducting appropriate customer due diligence (CDD)
- Following internal escalation procedures
- Reporting suspicious activity without delay
- Ensuring no breaches of AML/CFT controls or regulatory obligations

Any uncertainties or concerns about compliance should be promptly raised with the MLRO or Compliance Department.

10.2 BREACHES OF POLICY

A breach of this policy occurs when an individual:

- Fails to comply with the required due diligence measures
- Does not follow reporting or escalation procedures
- Knowingly overlooks suspicious transactions or behavior
- Engages in activity that undermines the Company's AML/CFT framework

Both acts of commission (intentional wrongdoing) and omission (negligence or inaction) are considered breaches and will be taken seriously.

10.3 DISCIPLINARY MEASURES

Internal disciplinary action may be taken depending on the nature and severity of the breach. These measures may include:

- Verbal or written warnings
- Suspension of duties
- Demotion
- Termination of employment or contractual relationship

Each case will be reviewed on its merits, taking into account the intent, potential harm, and history of the individual's conduct.

10.4 LEGAL AND REGULATORY CONSEQUENCES

In addition to internal disciplinary action, breaches of AML/CFT obligations may result in:

- Regulatory penalties, including fines, license suspension or revocation
- Criminal prosecution where misconduct is deliberate or reckless
- Personal liability for employees or officers who are found negligent or complicit

The Company has an obligation to cooperate with regulators and law enforcement, and will not shield individuals from investigation or prosecution.

10.5 REPORTING CONCERNS

Any employee who becomes aware of a breach, or potential breach, of this policy is encouraged to report it without delay to the MLRO. Reports will be handled confidentially and without retaliation.

11 RELATED INFORMATION

This AML/CFT Policy should be read in conjunction with the following internal policies, regulatory frameworks, and guidelines:

11.1 INTERNAL POLICIES AND PROCEDURES

As covered in this document

- KYC and Customer Due Diligence Procedures
- Enhanced Due Diligence Guidelines
- Transaction Monitoring Procedures
- Suspicious Transaction Reporting Protocol
- AML Risk Assessment Methodology

11.2 LEGAL AND REGULATORY FRAMEWORKS

- Curaçao National Ordinance on Identification of Clients (NOIS)
- Curaçao National Ordinance on the Reporting of Unusual Transactions (NORUT)
- FATF Recommendations (www.fatf-gafi.org)
- EU Directives on AML (where applicable)
- CFATF Guidelines (www.cfatf-gafic.org)

11.3 EXTERNAL GUIDANCE AND TOOLS

- Financial Intelligence Unit Curaçao (FIU-Nederlandse Antillen): www.fiu-curacao.cw
- OFAC Sanctions List: www.treasury.gov
- EU Sanctions Map: www.sanctionsmap.eu
- AML Screening (Hooyu)



Signature

20/01/2025

Date