

Apollo Sync B.V.

AML Policy

Version 2.1

Table of Contents

1. Overview
 - 1.1. Introduction
 - 1.2. Management
 - 1.3. Legal framework
 - 1.4. Risk-based approach
 - 1.5. Business Risk Assessment
 - 1.6. Data processing system
 - 1.7. Staff Training
2. Customer Acceptance and Registration Policy
 - 2.1. Introduction
 - 2.2. Customer Acceptance
 - 2.3. Restrictions
 - 2.4. Information Entered on Registration
 - 2.5. Terms Acceptance
 - 2.6. Underage Customers
 - 2.7. Customer Due Diligence
3. Customer Risk Scoring and Profiling
 - 3.1. Introduction
 - 3.2. Customer Risk Assessment
 - 3.3. Risk Score Calculation
 - 3.4. Customer Due Diligence level
 - 3.5. Additional Details & Source of Funds/Wealth
 - 3.6. On-Going Monitoring
 - 3.7. Withdrawals
 - 3.8. Automated Transaction Monitoring
4. Customer Due Diligence
 - 4.1. Introduction
 - 4.2. Standard Customer Due Diligence
 - 4.3. Documents acceptance
 - 4.4. Threshold approach
 - 4.5. Ongoing monitoring
 - 4.6. Enhanced Due Diligence
 - 4.7. Politically Exposed Persons and Sanctions Screening

- 4.8. Procedure for Account Closure
- 5. Deposit and Withdrawal Management Procedures
 - 5.1. Player Account Balance
 - 5.2. Payment Methods
 - 5.3. Player Deposits
 - 5.4. Player Withdrawals
 - 5.5. Withdrawal Payouts
 - 5.6. Virtual Assets and Cryptocurrency Policy
- 6. Suspicious Activity Reporting
 - 6.1. Introduction
 - 6.2. Red Flags Indicators
 - 6.3. Inability to Complete CDD Measures
 - 6.4. Internal Suspicious Activity Report
 - 6.5. External report to FIU
 - 6.6. Reporting Procedure
 - 6.7. Tipping-off
- 7. Internal Control
 - 7.1. Introduction
 - 7.2. Recordkeeping
 - 7.3. AML/CFT Compliance Officer
 - 7.4. Training
 - 7.5. Employees background check
 - 7.6. Internal and external revision and staying up to date
 - 7.7. Version Control
 - 7.8. Contact Information

Appendix 1 — Prohibited Countries

Signatures

1. Overview

1.1. Introduction

Money laundering is the process of concealing, disguising, converting, transferring, or removing criminal property. In other words, it is the process of converting the proceeds of crime into assets with legal origin.

There are three stages of money laundering:

- Placement – placement of funds generated from crime into financial system, either directly or indirectly (blending of funds, invoice fraud, smurfing).
- Layering – the process of separating illicit proceeds from their source by creating complex "layers" of financial transaction designed to disguise the audit trail and provide anonymity (multiple bank transfers, investing in "cash" business).
- Integration – the provision of apparent legitimacy to criminal derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system and appear to be legitimately earned or acquired funds (property dealing).

Terrorist financing is the provision or collection of funds with the intention that they should be used (or in the knowledge that they are to be used) to carry out acts that support terrorists or terrorist organizations or to commit acts on terrorism.

The key differences between ML and TF are:

- For money laundering to occur, the funds involved must be the proceeds of criminal conduct.
- For terrorist financing to occur, the source of funds is irrelevant, i.e., the funds can be from a legitimate or illegitimate source.

However, they both involve money or other forms of value. They both involve the movement of money or value, for example, from one person to another, one account to another, one institution to another, one country to another, one asset class to another. They are both keen to disguise the source and destination of funds.

Apollo Sync B.V. developed internal security measures to prevent money laundering and terrorist financing. The key features of these measures aim to stay aware of high-risk customers and detect suspicious activity, including the predicate offenses to money laundering and terrorist financing.

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

1.2. Management

The Company has appointed a designated AML/CFT Compliance Officer in accordance with the applicable Curaçao AML/CFT framework and CGA requirements.

This policy applies to all employees and outsource staff undertaking anti-money laundering, responsible gambling and anti-fraud procedures to the extent connected to their direct responsibilities, including senior management and AML/CFT Compliance Officer.

AML/CFT Compliance Officer, the key individual responsible for the prevention of money laundering and the financing of terrorism, has overall responsibility for ongoing regulatory compliance and anti-money laundering procedures.

AML/CFT Compliance Officer will be fully engaged in defining and managing the processes needed to prevent money laundering and other fraudulent activity based on the following principles:

- The Company assumes that most customers are not money launderers. However, it identifies players since it requires the applicable regulations, using a risk-based approach.
- The Company monitors all transactions and activity.
- The Company continuously monitors its customers as well as risks and processes.

The Company will ensure that all relevant employees are trained on AML and CTF policies and procedures and emphasize alerting these risks. Relevant employees will be required to pass competency tests on this topic.

The AML/CFT Compliance Officer is the designated office responsible for the maintenance, periodic review and updating of this AML Policy. Any questions or proposals regarding this Policy should be addressed to the AML/CFT Compliance Officer at the contact details specified in Section 7.8 of this Policy.

1.3. Legal framework

The Company's AML/CFT framework is based on, among other things:

- (a) the National Ordinance on Identification when Rendering Services (Landsverordening identificatie bij dienstverlening – LID);
- (b) the National Ordinance on the Reporting of Unusual Transactions (Landsverordening melding ongebruikelijke transacties – LMOT);
- (c) the National Ordinance on Games of Chance (LOK);
- (d) the National Sanctions Ordinance of Curaçao;
- (e) applicable national decrees, ministerial regulations, FIU reporting rules, and CGA guidance; and
- (f) FATF standards, to the extent relevant.

1.4. Risk-based approach

The Company undertakes to prevent and combat money laundering and terrorist financing following a risk-based approach. The Company's risk-based approach covers the following areas:

- Risk identification and assessment – identifying the money laundering risks facing the Company, given its customer, product, and services profile and having regard to available information, and assessing the potential scale and impact of the risks
- Risk mitigation – identifying and applying adequate measures to mitigate the material risks facing the Company
- Risk monitoring – putting in place management information systems (MIS) and keeping up to date with changes to the risk profile through changes to the business or to the threats, and
- Documentation – documenting the risk assessment and strategy and having policies and procedures covering the above and achieving effective accountability from the board and senior management.

1.5. Business Risk Assessment (BRA)

In accordance with the requirements of the CGA and FATF Recommendations, Apollo Sync B.V. has conducted a comprehensive Business Risk Assessment (BRA) to identify and evaluate the money laundering, terrorist financing and proliferation financing (ML/TF/PF) risks to which the Company is exposed.

1.5.1. Scope of the BRA

The BRA covers the following risk dimensions:

The Company offers online casino games (slots, live casino, table games), sports betting and lottery services. The primary ML/TF risks associated with online gambling include: high transaction velocity, cross-border fund flows, use of anonymous payment methods, and the potential to launder funds through deposits and withdrawals with minimal actual play. Risk rating: HIGH.

The Company serves individual retail customers globally. Risk factors include: anonymous online registration, customers from high-risk jurisdictions, PEPs and their associates, customers using high-risk payment methods (cryptocurrency, prepaid cards). The Company applies a risk-based customer profiling system (see Section 3). Risk rating: MEDIUM to HIGH depending on customer profile.

All services are delivered exclusively online via the website (apolosync.vip). There are no face-to-face interactions. Online-only delivery increases the risk of identity fraud and use of third-party accounts. Geo-blocking controls are applied to restrict access from prohibited jurisdictions. Risk rating: MEDIUM.

The Company operates globally with geo-blocking applied to restricted territories (see Appendix 1). FATF blacklisted jurisdictions are blocked. Customers from FATF grey-listed jurisdictions are subject to Enhanced Due Diligence; where a grey-listed jurisdiction is also included in the Company's Prohibited Countries List (Appendix 1), access is blocked at registration and geo-blocking level. Players from high-risk countries are subject to EDD. Risk rating: MEDIUM to HIGH depending on player location.

The Company accepts bank transfers, debit/credit cards, e-wallets and cryptocurrency. Cryptocurrency and prepaid cards present the highest ML/TF risk due to potential anonymity. The Company applies enhanced scrutiny to all high-risk payment methods (see Section 3.2.4). Risk rating: LOW (bank transfers) to HIGH (cryptocurrency).

The BRA methodology includes qualitative and quantitative risk assessments using sources such as FATF, CFATF, CGA, Transparency International, OFAC, and U.S. INCSR. The Company's business risk assessment also takes into consideration and includes the outcomes and recommendations of the National Risk Assessment (NRA) of the jurisdictions where it operates, including Curaçao.

1.5.2. Risk Appetite

The Company maintains a LOW risk appetite for ML/TF/PF. The Company does not knowingly accept customers who pose a high ML/TF risk unless appropriate EDD measures have been applied and approved by the AML/CFT Compliance Officer. The Company does not accept customers from FATF blacklisted jurisdictions or those subject to international sanctions. Customers from FATF grey-listed or otherwise high-risk jurisdictions are subject to Enhanced Due Diligence and may be rejected where the resulting risk cannot be adequately mitigated. Where a grey-listed jurisdiction is included in the Company's Prohibited Countries List (Appendix 1), customers from that jurisdiction are blocked at the registration and geo-blocking level.

1.5.3. Monitoring Effectiveness

The effectiveness of ML/TF risk mitigation measures is monitored through:

- Monthly review of AML alerts and SAR statistics by the AML/CFT Compliance Officer;
- Quarterly reporting to senior management;
- Annual internal audit of AML controls;
- Annual (or more frequent) third-party external AML review.

1.5.4. Technological Risk Assessment

Prior to the launch of any new product, business practice, delivery mechanism or technology, the Company shall conduct a dedicated technological risk assessment to identify and mitigate any new ML/TF risks introduced by such changes. The results of this assessment shall be approved by the AML/CFT Compliance Officer and Managing Director before launch.

1.5.5. BRA Revision

The BRA shall be reviewed and updated:

- At least once per calendar year;
- Whenever there is a material change to the Company's operating environment, products, services or customer base.

The BRA is a confidential internal document. It shall be formally documented, approved by senior management, reviewed at least annually, and made available to the CGA and other competent authorities upon lawful request.

1.6. Data processing system

The Company operates a combination of automated and manual controls for customer identification, verification, sanctions/PEP screening, transaction monitoring, and suspicious activity escalation, applied on a risk-based basis in accordance with law and the Company's internal procedures.

1.7. Staff Training

All staff (including outsourcing teams) shall complete initial AML/CFT training within 30 days of joining the Company, and thereafter on an annual basis. The training will be supplied by online and face-to-face training providers or by the appropriate Company's specialist. The specific employees are to be trained depending on the individual risk analysis.

1.7.1. Annual Mandatory Training Programme

In accordance with Article 5.9(4) of the National Ordinance on Games of Chance (LOK), the Company provides permanent, annual training to all persons working in the field of Games of Chance with the Company. This training is role-appropriate and covers, as a minimum, the following mandatory topics:

- (a) Mental Well-Being: Awareness of mental health in a gambling environment, recognition of stress and burnout, and support resources available to staff;
- (b) Anti-Bribery and Corruption: The Company's zero-tolerance approach to bribery, applicable legal obligations, reporting obligations, and practical scenarios specific to the gaming sector;
- (c) Crime Prevention: Recognition of fraud, match-fixing, chip-dumping, and other gaming-related criminal behaviours, and the procedures for escalation;
- (d) Responsible Gaming: Signs of problem gambling, intervention techniques, available player protection tools, and the Company's obligations under Article 5.4 of the LOK;
- (e) Anti-Money Laundering and Counter-Terrorist Financing: As detailed in Section 1.7 of this Policy;
- (f) Communication with Players: Best practices for sensitive and effective player communication, including responsible gaming interventions, complaint handling, and interactions with potentially vulnerable players;
- (g) Responsible Advertising: The Company's obligations under Article 5.6 of the LOK, including the prohibition on misleading content, targeting vulnerable persons, and encouraging excessive gaming.

Training is provided annually and within the first 30 days of employment for new hires. Completion is mandatory. Records of training (participants, dates, content, test scores) are maintained by the AML/CFT Compliance Officer and are available for inspection by the CGA upon request.

2. Customer Acceptance and Registration Policy

2.1. Introduction

Before gambling, making a deposit, or placing a real-money stake, the customer must register an account. Customers who do not register an account will not be able to gamble.

The Customer Acceptance and Registration Policy defines the criteria by which the Company may or not accept potential customers and describes the registration process.

2.2. Customer Acceptance

In order to deposit and play on a company's site, a customer must first register on the site.

The Company is strictly prohibited from keeping anonymous accounts or accounts in obviously fictitious names. During registration, the Company ensures that customers are registering an account to play and transact on their own behalf. This is achieved by including specific wording in the Terms and Conditions and requiring a mandatory declaration in the form of a tick box stating that the player is registering to play on his/her own behalf.

Registration is limited to individuals who are over eighteen years of age.

Customers may only open one account in their name per site. Additional checks are run to block multiple accounts by email address, mobile number, device and certain other combinations of customer data. These checks are done in order to prevent customers opening multiple accounts in order to bypass the AML threshold.

2.3. Restrictions

Individuals under 18 years of age are not permitted to register on the site.

Individuals considered to be under Sanctions or listed in any blacklists, in particular:

- Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s.
- Australian Sanctions (AU)
- Bureau of Industry and Security - Entity List (US)
- Bureau of Industry and Security - Unverified List (US)
- Bureau of Industry and Security (US)
- Canada, Office of the Superintendent of Financial Institutions, OSFI Consolidated
- CIA Leader list
- Consolidated Canadian Autonomous Sanctions List
- Department of State, AECA Debarred List (US)
- Department of State, Non-proliferation Sanctions (US)
- EU Financial Sanctions (EU)
- European Union, Consolidated list of persons, groups and entities subject to EU financial sanctions
- Foreign Financial Institutions Subject to Part 561 (the Part 561 List)
- Foreign Sanctions Evaders List (FSE)
- INTERPOL Wanted List
- Islamic Republic of Iran

- Libya Sanctions
- Non-SDN Iranian Sanctions Act List (NS-ISA)
- OFAC Consolidated Sanctions List
- Office of the Superintendent of Financial Institutions (Canada)
- Palestinian Legislative Council (PLC) List
- Sectoral Sanctions Identifications (SSI) List
- Specially Designated Nationals (OFAC)
- Specially Designated Nationals List (SDN)
- Switzerland Sanction List (SECO)
- U.S. Department of Commerce, Bureau of Industry and Security - Denied Persons List
- U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC)
- UK Financial Sanctions (UK)
- UK, Consolidated Financial Sanctions list (HMT)
- United Nations Sanctions (UN)
- United Nations Security Council (UN), Consolidated Sanctions list
- US Consolidated Sanctions (US)
- US State Dept. WMD Non-Proliferation List
- Existing customers who have an existing exclusion on the site.
- Individuals with fraud red flags.

The Company shall not accept customers who are subject to applicable sanctions or otherwise prohibited by law. Customers identified as PEPs, their family members, or close associates shall be subject to Enhanced Due Diligence and may only be accepted or retained where the resulting risk is assessed as manageable and senior approval has been obtained.

2.4. Information Entered on Registration

During the registration process and later on, the Company will request the following identifying information and contact details:

- First Name and Last Name,
- Date of Birth,
- Place of birth,
- Nationality,
- Identity document number,
- Gender,
- Address and country of Residence,
- Email address and mobile number,
- Username and Password.

2.5. Terms Acceptance

During the registration process, the customer must also confirm acceptance of the website's general terms and conditions and its privacy policy.

2.6. Underage Customers

The system does not allow registration of customers who are underage: In order for the registration process to be successful, customers must be at least 18 years old or

of legal age in their territory. Date of Birth will be cross checked with the provided ID upon customer Due Diligence.

2.7. Customer Due Diligence

To complete registration the customer must pass Customer Due Diligence. If the CDD is failed, the registration will be declined.

3. Customer Risk Scoring and Profiling

3.1. Introduction

Within the risk-based framework, The Company will undertake risk profiling of all customers from the time they are registered for the potential money laundering/terrorism financing risks.

It is important to note that the Company's policies and procedures are based on the following:

- Actual regulatory and legal requirements;
- Guidance provided by CGA and FIU;
- Our own internal evaluation of our overall business risk assessment, and our knowledge and experience with our customers.

3.2. Customer Risk Assessment

Based on the information supplied at registration (e.g. customer home address, customer location, customer age, whether PEP/sanctions), the Company will make an initial risk assessment of each customer. Customers thus start their gambling history with the Company categorised as either Low, Medium or High risk for ML/FT, which will determine decisions made at later points in how they are dealt with. Customer risk assessments are made regularly and when new information comes to light.

The customer risk assessment is based on:

- individual status (PEP, under sanctions, adverse media, etc.)
- geographical location
- gambling and transactional behaviour
- payment methods the player is using
- fraud red flags a customer triggered

Customers who are considered High Risk will need to undergo EDD.

3.2.1. Individual status

PEP

Politically Exposed Person means any person who has been entrusted with a high-ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level.

Any customer identified as a PEP, or a family member or close associate of a PEP, shall be subject to Enhanced Due Diligence, source-of-funds/source-of-wealth review, and senior management approval. The business relationship may only be established or continued where the risk is assessed as manageable. If the risk is unacceptable and cannot be mitigated, the account shall be rejected or closed.

Sanctions list

Governments and international authorities publish sanctions lists to combat persons engaged in illegal activities. Sanction lists include sanctioned people, organizations,

or governments. Companies, individuals, organizations, or governments are on these lists as they may pose a high risk.

Individuals and entities on this list are subject to financial restrictions prohibiting counterterrorism regimes and money laundering worldwide.

Any new or existing customer that is found on the Sanctions database will have their account rejected or closed.

A confirmed sanctions match is not subject to discretion or risk assessment. The account shall be immediately frozen without delay, no deposits, withdrawals or gameplay are permitted, the AML/CFT Compliance Officer shall be notified immediately, and the matter shall be reported to the competent authorities in Curaçao (including the FIU and, where required, the Ministry of Finance) within the timeframe prescribed by applicable sanctions law. All actions shall be documented and records retained for a minimum of 5 years.

Adverse media

Adverse Media or negative news is any bad and negative information about the customer or business discovered in various sources. This information can also expose someone to being involved in a crime.

Any new or existing customer mentioned in adverse media will be a subject for EDD. The Company may close the account or reject the registration depending on EDD results.

3.2.2. Geographical location

If the Company finds that the customer resides in a High-risk country, this fact may be a subject for EDD.

High-risk countries are jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and proliferation financing. The Company defines the High-risk countries based on the FATF regulations, which can be found on the following website:

<https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>

The Company has implemented a geo-blocking tool to limit access to our services from players located in certain geographic locations. A list of prohibited countries can be found in Appendix 1.

3.2.3. Gambling and transactional behaviour

Each player's behaviour is constantly monitored. The Company both looks for behaviours that are considered markers of harm for problem gambling and behaviours that indicate money laundering.

Behaviours, if noticed, are allocated scores that combines with other scored ML/FT red flags.

If any examples of overt ML/FT behaviour are observed, then an EDD must be undertaken immediately of the customer and, if necessary, the SAR process implemented.

Furthermore, the Company shall set and document a baseline value which represents the upper limit of a typical player's transactions. A player having a single source of regular income will pose a lesser risk of ML/TF than a player who has

multiple sources of income or irregular income streams. Transactions exceeding this established upper value will trigger an automatic review.

3.2.4. Payment Methods

Payment methods that allow us to trace the origin of the funds (such as the bank account) and to pay back to the source of the funds are considered low risk.

Payment methods that are funded by cash, and don't allow us to trace the source of the funds or to back to source are considered high risk.

Payment Method	Risk Rating
Bank transfers (Klarna, Trustly, Rapid, ApplePay), debit cards issued by banks	Low
EEA licensed e-wallets (Skrill, Neteller, paysafecard)	Medium
Prepaid cards, Vouchers and Cryptocurrency	High

Manipulation of payment methods — for example, making deposits using one method and withdrawals using another — is also considered high-risk by the Company.

3.2.5. Fraud red flags

The Company has anti-fraud risk management system to prevent bot attacks, fraudulent traffic, synthetic identities, account takeovers, identity thefts, credit card and CNP fraud, proxy users, multi-accounting, collusion etc. Some of the fraud red flags may also be connected to money laundering.

If the Company becomes aware a player triggered a fraud red flag, it will automatically be a subject for EDD.

3.3. Risk Score Calculation

The purpose of this procedure is to pick up minor incidents of ML/FT behaviour that by themselves may not warrant suspicion but, if combined with other behaviours, can do so.

A player will be scored by the internal CMS system according to part of the factors above, and a risk score will be assigned.

Each factor will generate a score, and the overall risk score will be a sum of the individual scores. The higher the score, the higher the risk.

Note that these factors, the scores and the thresholds are internal, and will be adjusted as we improve and update the RS Calculation.

Indicator	Description	Score
INDIVIDUAL STATUS		
PEP	A customer considered to be PEP	100

Adverse media	A customer was mentioned in negative news or information the company discovered from various sources	50
Sanctions/blacklist	A customer is under international sanctions/blacklists	100
GEOGRAPHICAL LOCATION		
Not at home	A customer whose IP location is different from their registered address	20
High-risk country resident	A customer resides in a High-risk country	30
GAMBLING BEHAVIOUR		
Large sums no play	A customer depositing large sums, then places minimal stake bets, then withdrawing all their funds	50
Large sums big losses	A customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence (EUR 5000 per week)	50
Low odds betting	A customer repeatedly placing short odds (such as red/black on roulette or repetitive betting on favourites) bets	25
Big changes in money	Dramatic changes in terms of volume and size of player deposits or staking activity	20
Several gaming accounts	A customer is trying to register several gaming accounts	30
TRANSACTIONAL BEHAVIOUR		
Smurfing	A customer making multiple deposits or withdrawals of small amounts without any objective reason	30
Spending above wages	A customers spend is outside of their affordability	20
No withdrawals	Player has never requested a withdrawal. Note: This indicator may reduce the overall risk score only where the player's deposit source, transaction volume, gameplay activity, and overall profile are otherwise consistent with legitimate recreational gambling and no other risk indicators are present. Applied at AML manager discretion.	-20 (conditional)
Withdrawal without	Money is deposited by a customer or held	30

playing	over a period and withdrawn by the customer without being used for gambling	
PAYMENT METHODS		
Card switching	A customer opening an account and registering several different cards and making transfers between them	20
High risk payment methods	A customer uses high-risk payment methods	30
FRAUD RED FLAGS		
VPN	Customer used a VPN	30

A confirmed sanctions match is not subject to risk scoring. It triggers automatic account rejection/freezing, immediate escalation to the AML/CFT Compliance Officer, and mandatory reporting in accordance with Section 4.5.2 and applicable sanctions law. No business relationship may be established or continued with a confirmed sanctions match regardless of any other risk factors.

Once the score is calculated, a risk level is assigned:

CMM Score	Risk Category
0-20	Low
21 - 40	Medium
41 - and higher	High

Not all factors can be automatically included in the CRA calculation due to technical or practical reasons, but we do monitor for these risks in other ways. For example, we check for VPN usage or multi-accounting at the point of registration, we have a separate alert for players who use cards under a different name, and all withdrawals are checked before approval and payment.

3.4. Customer Due Diligence level

The level of customer due diligence (CDD) conducted on a player will depend on the risk score assigned to the player as follows:

	Low	Med	High
Verify ID and address with docs	X	X	X
Collect additional personal details		X	X
Collect Source of Funds/ Wealth info		X	X (with documentation)
Ongoing monitoring	X	X	X (Enhanced)
Additional measures to address			X

any other risk identified			
Report suspected cases of ML/FT	X	X	X

3.5. Additional Details & Source of Funds/Wealth

A daily report will be sent to the AML/CFT Compliance Officer. The report will include any player who is newly classified as medium or high risk, or who has moved from medium to high.

The responsible AML manager will then:

- Review all accounts in the report, including:
 - Checking what information the Company already have on them
 - Open source internet checks
 - Checking if they are in any way suspicious
- The AML manager will then take appropriate action:
 - Block account if needed
 - Apply appropriate Due Diligence measures
 - Review the responses and the information provided by the player
 - Take appropriate action
 - If the player does not reply within 14 days, or the response is unsatisfactory, the account will be blocked. If docs are provided later, the AML manager should consider if the delay itself was suspicious, and act accordingly.

Accounts that have been assigned as medium or high risk will require AML approval before any withdrawal request can be processed.

All decisions taken by the AML manager must be documented.

3.6. On-Going Monitoring

The AML team will conduct on-going monitoring on accounts, on a risk sensitive basis. This includes:

- Obtain fresh identification when existing documents have expired.
- Question the data and information about a player whenever inconsistencies are noticed.
- And in general review and update from time to time, on a risk sensitive basis.

3.7. Withdrawals

When the AML Team review a withdrawal request, they will also look at the player's risk level:

- If the player has been classified as medium or high risk, the Verification Team will review the players documentation, and ensure that all the documents are still valid.
- If any documents have expired, new documents will be requested.

Therefore, any withdrawal request by a player who is flagged as medium or high risk, or any withdrawal request that has been otherwise flagged as high risk, will require approval by the AML team before being approved and processed.

3.8. Automated Transaction Monitoring

3.8.1. System Overview

The Company operates an automated transaction monitoring system (TMS) that analyses all customer transactions in real time to detect suspicious patterns consistent with ML/TF activity.

3.8.2. Automated Triggers

The TMS generates an automated alert when any of the following triggers are activated:

- TRIGGER 1: Single deposit or withdrawal exceeding ANG 4,000 (or equivalent);
- TRIGGER 2: Cumulative deposits reaching ANG 4,000 (or equivalent) since the establishment of the business relationship (date of registration);
- TRIGGER 3: Multiple deposits below ANG 500 within 24 hours from the same customer (structuring indicator);
- TRIGGER 4: Deposit followed by withdrawal of 90% or more of funds with minimal gambling activity (< 10% of deposited amount wagered);
- TRIGGER 5: Repeated low-odds betting (betting on outcomes with odds < 1.1) exceeding 80% of total stakes in any 7-day period;
- TRIGGER 6: More than 3 different payment methods used within 30 days;
- TRIGGER 7: Withdrawal requested to a payment method not previously used for deposit;
- TRIGGER 8: Customer IP address differs from registered address country;
- TRIGGER 9: Detection of VPN or proxy usage;
- TRIGGER 10: Transactions matching patterns associated with known fraud or ML typologies.

3.8.3. Analysis of Patterns

When an alert is generated, the AML Team shall:

- (a) Review the full transaction history of the customer;
- (b) Assess whether the activity is consistent with known structuring, layering or integration typologies;
- (c) Review open-source information about the customer;
- (d) Consider the customer's stated source of funds and income;
- (e) Document the findings and determination in the customer's file.

3.8.4. Escalation

If analysis confirms suspicious activity, the matter shall be escalated to the AML/CFT Compliance Officer within 24 hours of the alert being generated. The AML/CFT Compliance Officer shall determine whether a SAR should be submitted to the FIU Curaçao.

3.8.5. False Positive Management

The AML Team shall document all alerts, including those determined to be false positives, together with the rationale for the determination. This documentation shall be retained for 5 years and used to refine trigger thresholds and rules over time.

4. Customer Due Diligence

4.1. Introduction

The Company distinguishes between Customer Due Diligence (hereinafter – CDD) and Enhanced Customer Due Diligence (hereinafter – EDD)

The customer is obliged to cooperate concerning the fulfillment of the due diligence obligations. If the Company cannot undertake the due diligence, the business relationship won't be established or continued, and no transaction will be carried out. In addition, the Company examines whether it is necessary to submit SAR.

4.2. Standard Customer Due Diligence

The Company applies general (standard) customer due diligence (hereinafter – CDD) measures to the customers at the registration stage. The CDD process consists of:

- identification – establishing identity by collecting information from the customer.
- verification – proving a customer is who they claim to be by obtaining and validating documents or information which supports this claim of identity, which come from a reliable and independent source.

According to the above requirements, The Company collects the following information for identification and verification to prevent money laundering and terrorist financing:

- First and Last Name
- Date of birth
- Place of birth
- Nationality
- address (street, no., ZIP code, city)
- ID
- Proof of Address (POA)

4.3. Documents acceptance

For ID, the Company require a government-issued document containing photographic evidence of the customer's identity. The following documents may be accepted for the verification purpose:

- current signed passport
- driving license
- identity card
- travel document or passport;
- another document to be designated by the Minister

For POA verification the Company accepts:

- Utility bill for a service installed at the residence issued in the last 6 months.
- Correspondence or any other government-issued document from a central or local government authority, department or agency issued in the last 6 months.
- Lease agreement (Does not have to be issued in the last 6 months but must be currently valid.)

The main requirements to the documents provided by the customer are:

- the document must be valid and not expired.
- documents must be clear, legible and of good quality.
- Mobile phone bills may not be accepted.

4.4. Threshold approach and CDD Initiation

Deposit Threshold

The Company applies CDD measures in relation to any transaction (or series of linked transactions) that amounts to ANG 4,000 (four thousand Netherlands Antillean Guilder) or more, in accordance with the National Ordinance Identification when Rendering Services (Landsverordening identificatie bij dienstverlening, LID). For the avoidance of doubt, EUR 2,000 is used as an equivalent threshold where applicable, calculated at the prevailing exchange rate at the time of the transaction.

Calculation of the Threshold

The threshold is calculated as the cumulative total of all deposits made by a customer since the establishment of the business relationship. The following transactions are included in the threshold calculation:

- All deposits of funds to take part in remote gambling;
- Collection of winnings, including withdrawal of deposited funds;
- Winnings arising from the staking of deposited funds.

Transactions are considered 'linked' where they are part of the overall activity of a customer during a single login session, or where the Company has reasonable grounds to suspect that the transactions are being deliberately spread to circumvent the CDD threshold (structuring).

CDD Process upon Reaching the Threshold

Upon a customer reaching the ANG 4,000 threshold, the Verification Team shall immediately:

- (a) Notify the customer that identity verification is required;
- (b) Request the submission of required CDD documents (see Section 4.3);
- (c) Place restrictions on the account based on how the threshold was reached: Upon a customer reaching the ANG 4,000 threshold, the account shall be placed under verification restriction. No further deposits, withdrawals, or gameplay shall be permitted until the required CDD has been completed to the Company's satisfaction, unless a narrower restriction is expressly approved by the AML/CFT Compliance Officer and permitted under applicable law and internal controls.

Where the customer has a pending withdrawal request at the time the CDD threshold is reached or at the time a verification request is issued, and the customer fails to submit the required documentation within 3 (three) calendar days of the verification request being made, the pending withdrawal request shall be suspended and the funds returned to the customer's account balance. The withdrawal shall remain suspended until CDD has been successfully completed or the business relationship terminated.

The customer has 30 (thirty) calendar days from the date on which the threshold is reached to provide all required CDD/KYC documentation.

Failure to Complete CDD within 30 Days

If a customer fails to provide all required CDD documentation within 30 (thirty) calendar days of being notified:

- (a) The customer's account shall be blocked and no further deposits or gameplay shall be permitted;
- (b) All pending withdrawals shall be suspended;
- (c) The AML/CFT Compliance Officer shall be notified and shall assess whether the circumstances give rise to a suspicion of ML/TF warranting a SAR;
- (d) If the AML/CFT Compliance Officer determines that no SAR is warranted, the customer's funds (net of applicable deductions) shall be returned to the account from which they originated, and the business relationship shall be terminated.

Termination of Business Relationship

Where the Company is required to terminate the business relationship due to inability to complete CDD (including upon expiry of the 30-day period), the following steps shall be taken:

- (a) The AML/CFT Compliance Officer formally documents the decision to terminate;
- (b) The account is permanently closed;
- (c) Remaining funds are returned to the originating payment source, subject to the Company's right to withhold funds where required by law or where a SAR has been filed and consent is pending from the FIU;
- (d) All records are retained for the mandatory retention period (5 years);
- (e) Where applicable, a SAR is submitted to the FIU Curaçao.

4.5. Ongoing monitoring

The general due diligence duties include the ongoing monitoring of the business relationship. This includes:

- Obtaining fresh identification when existing documents have expired. (This can be done on a risk-sensitive basis.)
- Questioning the data and information the Company have whenever inconsistencies are noticed.
- general review and update from time to time, on a risk sensitive basis.
- checking if transactions match with the documents and information available at the Company about the customer and the origin, customer's assets
- updating the respective documents, data, or information at appropriate intervals.

To keep all customer information up to date, the Company applies ongoing CDD procedures strictly on a risk-sensitive basis, as determined by the customer's risk profile: at minimum every 6 months for HIGH risk customers, every 12 months for MEDIUM risk customers, and every 24 months for LOW risk customers.

4.5.1. Ongoing Sanctions Screening

The Company conducts ongoing sanctions screening against the UN Consolidated Sanctions List and EU Consolidated Financial Sanctions List as follows:

- At the point of registration (initial screening of all new customers);
- Upon reaching the deposit threshold of ANG 4,000;
- Every six (6) months for all existing active customers;
- Prior to the processing and approval of any withdrawal request;
- Immediately upon receipt of any updated sanctions list or instruction from the competent authorities.

4.5.2. Procedure for Sanctions Matches

Where a customer is identified as a match on a sanctions list, the following procedure shall be applied immediately:

- (a) The customer's account is frozen without delay — no deposits, withdrawals or gameplay are permitted;
- (b) All funds held in the account are frozen in accordance with the applicable Sanctions Ordinance;
- (c) The AML/CFT Compliance Officer is notified immediately;
- (d) The AML/CFT Compliance Officer reports the match to the competent authorities in Curaçao (including the FIU and, where required, the Ministry of Finance) within the timeframe prescribed by law;
- (e) The Company does not lift the account freeze until authorised to do so by the competent authorities.
- (f) All actions taken are documented and records are retained for a minimum of 5 years.

4.6. Enhanced Due Diligence

The Company applies enhanced customer due diligence measures (hereinafter – EDD) and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks.

EDD is applied in the following cases:

- in any case, identified by the Company or in the information provided by the authorities to the Company as one where there is a high risk of money laundering or terrorist financing;
- If the Company has doubts as to whether the information collected regarding the identity of the customer is correct or not (or no longer) accurate;
- if the Company has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP;
- in any case where the Company discovers that a customer has provided false or stolen identification documentation or information and the Company proposes to continue to deal with the customer;
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose,
- if the payment of a customer's winnings is made to a different payment account of the customer than to the account from which the customer makes the wagers,

- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.

In cases where there is a higher risk, establishment of the business relationship or continuation of the business relationship (if the higher risk only arose later or was only recognised later) only with the consent of the AML/CFT Compliance Officer.

If a customer has been deemed to be a high-risk or becomes one at any stage, the Company undertakes the EDD, comprising of (depending on the case):

- undertaking Re-verification of identity (repeated CDD).
- Establishing how the customer acquired his wealth to be satisfied that it is legitimate:
 - salary income or company profit (Certified Payslip / Certified employer letter / audited accounts if self-employed)
 - sale or liquidation of financial instruments (Certified shares/investments sale contracts or statements/ accountant letter)
 - sale of property (Certified copy of the contract of sale or letter from a solicitor or estate agent)
 - inheritance (Certified copy of will including the value of heritage)
 - sale of the company (Certified contracts, media articles, certified letter from accountant or solicitor).
- Establishing the source of the customer's funds to be satisfied that they do not constitute the proceeds from crime.
- Ensure that deposits originate from payment methods and do not allow anonymity by requesting copies of bank statements or account statements.
- Undertaking increased continuous monitoring of the business relationship.
- The suspicious transaction must be investigated, and the business relationship underlying the transaction shall be monitored to assess the risk of money laundering and terrorist financing.

Undertaking the EDD on transactions, the Company's fundamental aim is to ensure the transparency of payment flows. Accordingly, the origin and destination of the money used in a transaction shall be traceable back in each case to an account.

Meaning of Source of Funds

The Source of Funds refers to the origin of the particular funds being used to deposit on the Company's website. This is not simply verifying which bank or financial institution the customer may have received the funds from. The information obtained should be substantive, relevant and establish the fund's origin and the method/circumstances under which the funds were acquired.

Meaning of Source of Wealth

The Source of Wealth refers to the origin of the entire body of wealth (i.e. total assets) of the client. The information that the Company obtains should indicate the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired.

4.7. Politically Exposed Persons and Sanctions Screening

The Company uses KYC software tool to check all new customers at the registration stage against the PEP and Sanctions databases. The Company also regularly check the whole customer database every six months to ensure existing customers have not changed status.

Any customer identified as a PEP or a relative of a PEP shall be subject to the EDD process described below. The Compliance Officer shall assess each case individually. The account shall be rejected or closed only where EDD determines the risk to be unacceptable. Any customer confirmed as matching a sanctions list shall have their account rejected, restricted, or frozen immediately in accordance with applicable sanctions law.

In case of identifying a PEP, responsible staff will send a report to AML/CFT Compliance Officer who in turn will send a report to the senior management.

The AML/CFT Compliance Officer will investigate each case to identify positive or false-positive PEP alert. The Company has a right to request additional documents from the customer for this purpose within the investigation.

If the PEP alert is true-positive, the AML/CFT Compliance Officer will reject registration or close the account and informed the senior management about the decision taken.

Politically Exposed Person means any person who has been entrusted with a high-ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level. In particular, politically exposed persons are:

- heads of state, heads of government, ministers, members of the European Commission, deputy ministers and assistant ministers,
- members of parliament and members of similar legislative organs,
- members of the governing bodies of political parties,
- members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are usually not subject to further appeal,
- members of the boards of courts of audit,
- members of the boards of central banks,
- ambassadors, chargés d'affaires and defence attachés,
- members of the administrative, management or supervisory bodies of state-owned enterprises,
- directors, deputy directors, members of the board or other managers with a comparable function in an international or European intergovernmental organization.

Family member of PEP means a close relative, in particular

- the spouse or civil partner,
- a child and the child's spouse or civil partner and
- both parents.

FATF blacklisted countries are blocked on the Company's sites. Customers from FATF grey-listed jurisdictions are subject to Enhanced Due Diligence. Where a grey-listed jurisdiction is also included in the Company's Prohibited Countries List (Appendix 1), individuals from those countries are not able to register or access the

Services. The operative list of prohibited jurisdictions is maintained in Appendix 1 and the Company's internal Restricted Territories Register.

The list of FATF blacklist/grey-listed countries may be found here - <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>

4.8. Procedure for Account Closure

There are numerous reasons for why the Company will want to close a customer's account:

- Fraud
- Cheating
- Bonus Abuse
- Allowing a third person to use their account
- Under-aged gambling
- Problem gambler
- Being abusive to staff
- Commercial concerns
- CDD failure
- Terms and Conditions breach

The concern of this Company Policy is the reason that there is a suspicion or knowledge that the customer is involved in ML/FT.

By law the Company must end the business relationship with the customer unless we have obtained appropriate consent for it to continue and even then it is precautionary to close the account.

Due to the laws on Tipping Off the Company cannot inform the customer that we have concerns regarding ML/FT, thus account closure must be done sensitively.

The AML/CFT Compliance Officer will need to consider whether if an SAR was submitted as part of the concern about the player's behaviour whether appropriate consent should have been requested.

Where the Company is unable to complete or apply the required CDD measures in relation to a particular customer at the point the CDD threshold for transactions is reached, and is accordingly required to cease transactions and terminate the business relationship with the customer.

4.9. UBO Identification

For corporate accounts, the Company establishes the chain of control and identifies the Ultimate Beneficial Owner (UBO). A UBO is any natural person holding 25% or more of the shares or voting rights, or a person who otherwise exercises ultimate effective control of the customer. Where no natural person is identified under these criteria, the natural person who holds the position of senior managing official must be identified and verified as the UBO.

4.10. Simplified Due Diligence (SDD)

SDD may be applied in low-risk scenarios (e.g., CMM Score 0-20, no ML/TF suspicion, non-PEP, no sanctions, standard payment methods). SDD allows

identification via three basic fields (name, address, DOB), verification via alternative reliable sources, and reduced monitoring frequency. SDD is immediately terminated and upgraded to standard CDD/EDD if the risk profile changes, red flags appear, or the ANG 4,000 threshold is reached.

4.11. Reliance on third parties

The Company may rely on third parties (e.g., regulated payment providers, KYC providers) for CDD elements, provided they are supervised, apply comparable CDD/record-keeping standards, and have a formal agreement in place to provide copies of identification data or other relevant documentation immediately upon request. The Company must test this arrangement from time to time to ensure that it actually functions as set out in the agreement and that the third party responds effectively. The Company retains ultimate responsibility for CDD and cannot outsource the final decision on accepting a client, customer risk assessments, or ongoing monitoring.

5. Deposit and Withdrawal Management Procedures

5.1. Player Account Balance

Each player has a wallet with funds from which bets are deducted, and winnings added. All funds deposited by the player or owed by the Company are credited to the player's corresponding account. The player can top up the funds in his account by depositing through the cashier on the site and then use these funds to place bets. Bets are deducted from his account balance, and winnings are added to the account balance.

The player can withdraw available funds from their account balance. The Company does not offer credit to players. A player may not transfer funds to another player.

5.2. Payment Methods

Payments shall only be accepted and made from accounts held with licenced financial institutions or through licenced payment providers.

No cash deposits/withdrawals will be effected between the Company and its players.

5.3. Player Deposits

After registering, a player may then deposit funds into their account through the cashier on the site.

In order to facilitate these deposits, the company has integrated with a number of gateways. All gateways are PCI DSS compliant, and the company does not hold any credit card data itself.

The company submits the transaction to the PSP and then waits for approval from the card acquirer/e-wallet. On approval, the deposit status is updated and the funds added to the player's balance.

5.4. Player Withdrawals

A player with an available balance will be able to request a withdrawal of the funds via the cashier on the site.

The player will enter the amount they wish to withdraw and select their preferred payout method. The withdrawal amount is then deducted from the player's balance.

5.5. Withdrawal Payouts

In remitting funds to the player, we will, where possible, remit the funds directly into the account where the funds originated from.

Provided that where this is not possible, we will remit the funds to the player in line with the requirements under AML legislation.

5.6. Virtual Assets and Cryptocurrency Policy

5.6.1. Scope

This section governs the acceptance and handling of virtual assets (VA) and cryptocurrency (collectively 'crypto') by Apollo Sync B.V.

5.6.2. Accepted Cryptocurrencies

The Company may accept the following cryptocurrencies as a payment method, subject to the risk controls described in this section:

- Bitcoin (BTC)
- Ethereum (ETH)
- Other cryptocurrencies as approved by the AML/CFT Compliance Officer.

5.6.3. Risk Classification

Cryptocurrency is classified as a HIGH-RISK payment method due to:

- Potential for anonymity and difficulty in tracing fund origins;
- Volatility in value;
- Increased risk of use for ML/TF purposes.

5.6.4. Risk Controls for Crypto Transactions

The following controls apply to all crypto deposits and withdrawals:

- (a) KYC/CDD: Full CDD (identity and proof of address verification) must be completed BEFORE any crypto deposit or withdrawal is processed, regardless of the amount;
- (b) Wallet Screening: All customer crypto wallet addresses shall be screened against blockchain analytics tools to assess wallet risk (e.g., checking for association with darknet markets, sanctions, or high-risk activity);
- (c) Source of Funds: As cryptocurrency is classified as a HIGH-RISK payment method, for any crypto deposit exceeding **ANG 1,000** (cumulative), the customer must provide documentation evidencing the legitimate source of the crypto funds (e.g., purchase receipts from regulated exchanges, bank statements showing fiat-to-crypto conversion) to align with our high-risk customer due diligence thresholds;
- (d) Withdrawal to same wallet: Crypto withdrawals shall only be processed to the same wallet address from which the deposit was made;
- (e) Prohibition on cash-in/cash-out: The Company will not accept direct cash-to-crypto conversions or facilitate peer-to-peer crypto transfers;
- (f) Enhanced monitoring: All customers using crypto are subject to enhanced ongoing transaction monitoring;
- (g) SAR filing: Any crypto transaction that cannot be adequately explained or where the wallet risk score is unacceptable shall be reported to the AML/CFT Compliance Officer for assessment and potential SAR filing.

5.6.5. Prohibited Crypto Arrangements

The Company shall not:

- Accept crypto from mixing services, tumblers or privacy coins (e.g., Monero, Zcash) that obfuscate transaction trails;
- Process crypto transactions on behalf of third parties;
- Accept crypto from wallets flagged by screening tools as high-risk.

5.6.6. Technological Risk Assessment

Before introducing any new cryptocurrency or virtual asset payment method, the Company shall conduct a technological risk assessment as required by Section 1.5.4 of this Policy.

6. Suspicious Activity Reporting

6.1. Introduction

Every employee of the Company must report to the AML/CFT Compliance Officer if there is suspicion or knowledge of money laundering, funding of terrorism or if the funds being used on the Company's website are the proceeds of criminal activity.

The AML/CFT Compliance Officer will consider each report and determine whether it gives grounds for knowledge or suspicion. If they do, then a SAR should be submitted to the Financial Intelligence Unit – Financiële Inlichtingen Eenheid (hereinafter – FIU or FIU Curaçao).

Knowledge means that the person reporting knows the event to be a fact. Suspicion implies that the person reporting the incident may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial or financial sense.

A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report the activity then arises. Likewise, if concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and will need to be reported to the FIU.

The AML/CFT Compliance Officer assesses all the circumstances and may ask the customer or others further questions if needed. The choice depends on what is already known about the customer and the transaction and how easy it is to make further enquiries.

6.2. Red Flags Indicators

Red flags are not intended to automatically result in filing a SAR with the FIU, however are merely indicators that should lead the Company to question the customer's behaviour. If there is no reasonable explanation for the red flags, then an internal report must be made to the AML/CFT Compliance Officer.

The following is a list of possible red flags which should be considered:

- Customer does not cooperate in the carrying out of CDD/EDD.
- Customer attempts to register more than one account on a site.
- Customer makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquires about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the Customer's wealth, income or financial situation.
- Customer seeks to transfer funds to a bank account held in the name of a third party.
- Customer requests a withdrawal to an account he never deposited with.

- Customer opening an account and registering several different cards and making transfers between them,
- Customer depositing large sums, then places minimal bets, then withdrawing all their funds,
- Customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence.

6.3. Inability to Complete CDD Measures

If a customer refuses to provide CDD/EDD documentation, the Company won't immediately equate this on its own to suspicion of ML/FT.

The Company will consider all factors and information, including the payment method used, games played, playing trends and patterns, residence jurisdiction, and open-source information.

If there are grounds to suspect ML/FT after considering all of these factors, then an SAR must be submitted.

6.3.1. Exemption to Avoid Tipping-Off If the Company has a suspicion that transactions relate to money laundering or terrorist financing, it must take into account the risk of tipping-off the customer when performing the CDD process. If the AML/CFT Compliance Officer reasonably believes that performing the CDD or EDD process will tip-off the player, the Company may choose not to pursue the CDD process. In such circumstances, the CDD process shall be halted immediately, and the AML/CFT Compliance Officer shall file a Suspicious Activity Report (SAR) to the FIU Curaçao.

6.4. Internal Suspicious Activity Report

All employees have a duty to report suspicious transactions. If an employee has any suspicion about a customer's behaviour or transaction, it must be reported to the AML/CFT Compliance Officer immediately. All employees are expected to report suspicious transactions to the AML/CFT Compliance Officer. For this purpose employees use approved Internal Suspicious Activity Report Form.

The employee should still submit the report, even if their superiors are not in agreement. It will then be up to the AML/CFT Compliance Officer to determine if the information available can be considered as sufficient for a SAR to be made to the FIU.

The following information is included to an Internal SAR:

- The customers details
- The member of staff's statement about what gave them cause to make the report
- All relevant documentation and information

The AML/CFT Compliance Officer will:

- acknowledge receipt of the report and review and investigate further as required
- make an assessment based upon all the information and decide whether the matter needs to be reported to law enforcement
- if it does, submit a SAR to the FIU

- make a record and inform senior management about the decision taken.

6.5. External report to FIU

6.5.1. Reporting Threshold

In accordance with the National Ordinance on Reporting Unusual Transactions (LMOT), the Company is obliged to report unusual transactions to the FIU Curaçao (Financiële Inlichtingen Eenheid) when the transaction meets or exceeds ANG 5,000 (five thousand Netherlands Antillean Guilder) in value, or where the Company has reasonable grounds to suspect that the transaction involves ML/TF regardless of the amount.

For the avoidance of doubt, the ANG 5,000 reporting threshold applies separately from the ANG 4,000 CDD threshold. Both thresholds may apply simultaneously.

6.5.2. Prohibition on Disclosure (Tipping-Off)

Upon filing a SAR with the FIU Curaçao, or while considering whether to do so, no employee, officer or agent of the Company shall:

- Disclose to the customer or any third party that a report has been or may be submitted;
- Take any action that might prejudice an investigation by the FIU or law enforcement authorities.

This prohibition applies regardless of whether the customer directly asks about the status of their account or the reason for any restrictions. Violation of this prohibition may constitute a criminal offence.

6.5.3. Record-Keeping for CDD Information and Transactions

The Company shall retain the following records for a minimum of 5 (five) years from the date on which the business relationship ends:

- (a) All CDD/EDD documentation collected (copies of identity documents, proof of address, source of funds/wealth documentation);
- (b) All transaction records, including dates, amounts, currencies, payment methods and counterparty details;
- (c) All internal SARs and the outcome of the AML/CFT Compliance Officer's assessment;
- (d) All SARs submitted to the FIU and any correspondence received from the FIU;
- (e) Records of all AML alerts generated by the TMS and the outcome of their investigation.

After the retention period, records shall be securely destroyed unless applicable law requires longer retention (maximum 10 years).

Once the AML/CFT Compliance Officer has received an Internal SAR, she/he will decide if a SAR should be submitted to the FIU.

When making this decision, the AML/CFT Compliance Officer should consider that AML legislation is intended to address and attack serious crime which usually either

involves amounts that are not minimal or circumstances that show an intent to circumvent and abuse the safeguards in place to deter the use of the financial system for criminal purposes.

For example, identity fraud and chargebacks may give rise to ML, but a licensee will only be subject to reporting obligations if they result in funds derived from these activities being deposited with or held by the licensee.

However, the Company won't report single instances involving small amounts but should consider whether it can detect a more significant pattern or scheme.

The AML/CFT Compliance Officer considers whether an internal report gives rise to a suspicion of ML by taking into account all relevant information, including assessing whether there are common denominators between e.g., repeated suspicious behaviour, instances of chargebacks or identity fraud. For example, these may consist of common or related persons, common IP addresses etc.

The AML/CFT Compliance Officer, in deciding to submit the SAR or not, should answer the following questions:

- Who is involved?
- How are they involved?
- What is the criminal/terrorist property?
- What is the value of the criminal/terrorist property (estimated as necessary)?
- Where is the criminal/terrorist property?
- When did the circumstances arise?
- When are the circumstances planned to happen?
- How did the circumstances arise?
- Why you are suspicious or have knowledge.

6.6. Reporting Procedure

The Company is obliged to submit a suspicious activity report to the FIU, through the user interfaces on the FIU's website, without due delay if there are indications that:

- the Company know, suspect, or has reasonable grounds for knowing or suspecting money laundering and/or terrorist financing,
- an asset related to a business relationship or transaction originates from a criminal offence that could constitute a predicate offence to money laundering,
- a business case, transaction, or asset is related to terrorist financing.

When the Company decides whether it is necessary to submit SAR, it takes the following factors into account, including but not limited to:

- the purpose and nature of the transaction,
- peculiarities in the customer,
- the financial and business background of the customer,
- the origin of the assets contributed or to be contributed.

The Company doesn't execute suspicious transactions, except in cases where it cannot postpone the transaction or if the postponement could hinder the prosecution of an alleged criminal offense. In this case, the Company submits SAR immediately.

6.7. Tipping-off

It is an offence to tell anyone that a SAR has been submitted or is being considered to be submitted and that this is likely to prejudice the investigation. This means it is possible to have an internal discussion about the customer, but in no way can the customer or their associates be given any indication that the customer may be under investigation.

This means that no one working for the Company:

- can, at the time, tell a customer that a transaction is being delayed because a report is awaiting a defence (consent) from the FIU
- can tell the customer that law enforcement is conducting an investigation.

7. Internal Control

7.1. Introduction

The Company has a number of internal controls and general procedures which will be used on a day-to-day basis in respect of managing and running the daily operations of the business for the purpose of money laundering and terrorist financing prevention.

7.2. Recordkeeping

The Company keeps all the documents and data collected or obtained within the scope of the due diligence, including:

- all data and information used to identify and verify customers (including type and number of the document, issuing authority, etc.)
- all records (receipts) relating to transactions, i.e., winnings paid out or refunds to customer accounts,
- all documents and records used for the preparation of the risk analysis, the risk analysis itself, including the results of the risk assessment, as well as the documentation on the appropriateness of the measures taken based on these results,
- the results of internal investigations, communication with FIU and regulators,
- documents collected within the scope of business partners due diligence
- documents collected from the employees within the scope of the due diligence
- documents regarding AML trainings (training materials, examination results, etc.)

The Company also keeps all documents created and processed in connection with a suspicion of money laundering or terrorist financing, including:

- all related internal and external correspondence,
- file and interview notes,
- the results of internal investigations and the measures taken, that can explain why the AML/CFT Compliance Officer concluded and initiated the actions taken.

The retention period is five years and starts with the end of the calendar year in which the business relationship ends and in all other cases with the end of the calendar year in which the respective information was ascertained. Applicable legislation may provide for a more extended retention period.

The Company destroys all the documents and data collected after the expiration of the 5-year retention period, unless other statutory recordkeeping or ongoing legal/regulatory obligations require a longer retention period.

7.3. AML/CFT Compliance Officer

The Company has appointed a designated AML/CFT Compliance Officer in accordance with the applicable Curaçao AML/CFT framework and CGA requirements. The AML/CFT Compliance Officer possesses the necessary qualifications, experience and knowledge of AML/CFT requirements to effectively fulfil their responsibilities. The AML/CFT Compliance Officer acts independently and

does not hold any position within the Company that gives rise to a conflict of interest with their AML/CFT duties. The appointment of the AML/CFT Compliance Officer and any change thereto shall be notified to the CGA without undue delay.

The Company has appointed a AML/CFT Compliance Officer whose main responsibility is to review any internal suspicious transaction reports of unusual or suspicious transactions, and where necessary to submit an SAR with the FIU. The AML/CFT Compliance Officer is the main contact point for the FIU.

In order to ensure that the AML/CFT Compliance Officer is able to fulfill their role effectively, the Company guarantee that:

- AML/CFT Compliance Officer acts independently, has been provided the necessary knowledge of the Company's activities and is able to decide independently as to whether internal reports are to be escalated to the FIU.
- AML/CFT Compliance Officer has no conflicting responsibility which may pose a conflict of interest.
- AML/CFT Compliance Officer has sufficient time, resources and information to fulfill their responsibilities.
- AML/CFT Compliance Officer has a right to create work assignments to relevant employees and take decisions regarding ML/TF prevention.

The AML/CFT Compliance Officer and their deputy carry out the following functions (including but not limited to):

- Creation (in writing) and further development of internal risk analysis, including a complete scope of risks connected to money laundering and terrorist financing.
- Developing and updating internal policies and procedures to prevent money laundering and terrorist financing.
- Creation of uniform reporting channels.
- Involvement in other internal organizational and work instructions creation and their further development, related to implementing the regulations on the prevention of money laundering or terrorist financing.
- Ensuring compliance with current AML regulations, and other relevant legislation.
- Ongoing monitoring of the Company's business activity to comply with the money laundering regulations.
- Ensuring CDD/EDD is undertaken.
- Suspicious activity risk assessment.
- The submission of SARs in appropriate cases.
- Contributing to the content of staff AML training.
- Maintaining a list of all inquiries received from law enforcement agencies and records relating to internal and external disclosures.
- Submitting a report to the management on AML/CFT Compliance Officer activities on the risk situation of the Company and the measures taken and intended to implement the obligations under money laundering regulations.

The AML/CFT Compliance Officer and their deputy are authorized, within the scope of their performance of their work:

- To perform their tasks independently and effectively

- To submit the necessary legally binding declarations for the undertaking and represent it externally in relevant situations.
- To provide undertaking-specific instructions for all matters relating to the prevention of money laundering and terrorist financing.
- To carry out random checks without restriction.

The AML/CFT Compliance Officer acts independently, is strictly independent from the games operations, and does not hold any position within the Company that gives rise to a conflict of interest. The responsibilities are formalized in a Job Description, which must be signed and dated by the AML/CFT Compliance Officer.

7.4. Training

The Company will give training to all staff directly or indirectly through a service provider upon joining the Company and after that annually.

Relevant training materials will be prepared for all teams based on the company policies which have been compiled according to the applicable legislation requirements and guidelines.

Training will be conducted as follows:

- Training material based on the finalized and approved policies the Company has, in the form of documents and presentations.
- Training will be provided to existing management and staff in a class setting or online.
- Training will also be included in the induction of all new staff.
- Training will be followed up with a questionnaire to test everyone's understanding.
- Should the Company find that some issues are not clear we will repeat the training focusing on the issues that were not understood.
- Regular refresher training will be given, which will include any updates and will focus on any shortfalls that arose during the previous period.
- Any update in policy will be communicated in a group email and through ad-hoc training, and added to periodic training updates and material.

Staff training will focus on ensuring awareness of:

- all applicable legislation,
- the provisions of the money laundering and terrorist financing requirements,
- staff personal obligations under the money laundering and terrorist financing requirements,
- applicable internal reporting procedures,
- Company's policies and procedures to prevent money laundering and the financing of terrorism,
- Company's identification and verification procedures, record-keeping, and other procedures to prevent money laundering and the financing of terrorism,
- recognition and handling of suspicious transactions,
- Staff personal liability for failure to report information or suspicions under the money laundering and terrorist financing requirements and the Company's internal procedures; and
- New developments, including information on current techniques, methods, and trends in money laundering and the financing of terrorism.

- The money laundering and terrorist financing risks faced by the Company
- Data protection regulations.

The training program is tailored to different employee segments:

- New employees: General AML/CFT/CFP awareness and reporting indicators;
- Customer-facing staff: Front-line detection of ML methods and ID verification;
- Audit staff: Changes in regulation, testing methods;
- AML Compliance staff: Specialized training on new trends;
- Supervisors, Managers, Board of Directors: High-level instruction on reputational risk, policies, and enforcement.

The AML/CFT Compliance Officer maintains a Training Log containing: program description, attendee names, dates, test results, and ongoing training plans.

Induction training sessions will be conducted for all employees and will include fraud prevention, detection and ancillary matters, as required by their role. Refresher training will also be provided, both on a regular basis and as needed, so as to keep employees up to date and informed of the Company's policies and procedures and any changes or improvements made.

The AML/CFT Compliance Officer keeps records of training delivered, showing what training has been provided, when and by whom, and the next training date. In case of any changes to the Company's policies and procedures or applicable legislation, all staff will get the relevant training.

7.5. Employees background check

Prior to engaging employees, the Company will carry out relevant integrity checks, in-line with their position, responsibilities and access levels. The Company will not employ any persons who are not deemed to be fit and proper.

For this purpose, the Company may request the following documents (in each case with due regard to data protection):

- a valid original identity document,
- CV,
- a certificate of good conduct or police clearance certificate to screen for criminal records,
- any other documents as the Company deems necessary to request.

Once a person is employed, screening shall still be carried out on an ongoing basis as required. All Company's employees must guarantee that they observe the provisions of applicable legislation and the associated due diligence obligations, report facts relevant to money laundering, and do not themselves participate actively or passively in dubious transactions.

For this purpose, senior management will regularly carry out checks on employees or whenever the Company feels the need to perform such inspections. In particular, such inspections shall be carried out when suspicion arises concerning the behaviour of specific employees. The Company may carry out these checks through surprise spot checks or other procedures that will enable such personnel to verify whether employees comply with the policies and procedures.

The frequency and extent of screening that shall be carried out shall be proportionate to the risk level posed by the employee. The risk level will be determined case by case depending on employee's position (e.g., head of dept, senior, mid), the scope of duties and obligations, etc.

The Company will check all the employees at least once a year. The Company will use an employee performance sheet for this purpose.

7.6. Internal and external revision and staying up to date

This AML Policy shall be reviewed at a minimum once per calendar year, or more frequently whenever:

- there are material changes to the applicable regulatory framework;
- the Company's products, services or delivery channels change significantly;
- the Company's risk profile changes materially; or
- the CGA, FIU Curaçao, or any other competent authority issues relevant guidance, instructions, or legal updates.

The date of each review, the name of the reviewer and any amendments made shall be recorded in the Version Control table (Section 7.7). The Policy must be formally approved by the Managing Director after each review.

The Company has compiled its policies and procedures according to the requirements of the applicable legislation and guidance of the FATF, CGA and FIU. However, the requirements and guidance, as well as external fraud trends, can and will change. Therefore, the Company has implemented the following measures to ensure the relevance of the Company's internal AML documentation:

- Key personnel have subscribed to mailing lists offered by the FIU, CGA and FATF and joined relevant forums
- The Company periodically obtains legal advice from gambling law and AML consultants to ensure ongoing compliance with best practices
- In the case of an update, the Company will take the following steps, as necessary:
 - Update Company's policy documentation and training material
 - Inform all relevant staff by email regarding the updates, meet with relevant team managers, and ensure they update their teams appropriately
 - Update email communication templates and chat canned responses.
 - Update website policies, maintaining a version number and 'last update' date.
 - Update the Terms and Conditions, maintaining a version number and 'last update' date.

Any consequential update to the Terms and Conditions will trigger a pop-up notification to players on their next login where they will need to accept and agree to the new version before proceeding.

The AML compliance program must be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party not involved with the organization's AML compliance staff. The auditors performing this review must be sufficiently qualified, having at least two years of experience in

AML/CFT compliance along with a bachelor's degree and a recognized AML certification (e.g., CAMS, CAMS-Audit, or AMLFC). The scope of the testing and the results must be documented, with any deficiencies reported to senior management and the Board of Directors for prompt corrective actions.

7.7. Version Control

Policy Status

This is Version 2.1 of the AML Policy of Apollo Sync B.V. This Policy supersedes Version 2.0 dated Feb-01-2026.

Version History:

Version	Date	Changes Made	Approved By
1.0	Nov-13-2024	Initial version	KRADONOV IHOR
2.0	Feb-01-2026	Updated comply with LOK Article 5.9 & LOK Article 5.10 & Article 5.11	KRADONOV IHOR
2.1	May-06-2026	Updated per CGA comments; added BRA, Crypto Policy, Transaction Monitoring, amended thresholds to ANG	KRADONOV IHOR

All versions of this Policy are retained by the AML/CFT Compliance Officer. The current version is available to all relevant staff.

The Company is constantly improving its policies to actively combat Money Laundering and the Financing of Terrorism and therefore requires Version control to keep track of Changes and Approval by the Director.

7.8. Contact Information

For any questions regarding this AML Policy, please contact the designated responsible person:

AML/CFT Compliance Officer

Apollo Sync B.V.

Chuchubiweg 17, Willemstad, Curaçao

Email: AMLO@apolosync.vip

All AML-related communications from the FIU, CGA or other regulatory authorities should be addressed to the AML/CFT Compliance Officer at the above contact details.

7.9. Interaction with the Curaçao Gaming Authority (CGA)

The Company shall promptly provide the CGA, upon lawful request, with the AML/CFT compliance programme, BRA records, AML/CFT Compliance Officer role documentation, unusual transaction reporting records, frozen-account records, training logs, independent review reports, and CDD/EDD records, subject to legal confidentiality restrictions.

Appendix 1 — Prohibited Countries

The Company maintains a Restricted Territories Register approved by Compliance and reviewed periodically. The register reflects legal prohibitions, sanctions, licensing limitations, fraud risk, AML/CFT risk, and commercial risk. The operative list used by registration, geolocation, payments, and website controls shall be the current internal Restricted Territories Register and the public-facing restricted-jurisdictions notice published on the Website.

Signatures

This AML Policy (Version 2.1) has been reviewed, approved and signed by the authorised representatives of Apollo Sync B.V.

AML/CFT Compliance Officer

Name: KRADONOV IHOR MYKHAYLOVYCH

Signature: _____

Date: MAY-06-2026

Managing Director

Name: LOOK JUN CHERN

Signature: _____

Date: MAY-07-2026