

Anti-Money Laundering Policy

for

CLUBHOUSE MEDIA N.V.

VERSION CONTROL

Title	Anti-Money Laundering Policy		
Description	Internal Processes, Program and Compliance Procedures		
Date Created	10 September 2019		
Operative Date	August 2026		
Maintained By	Clubhouse Media		
Version Number	Modifications Made	Date Modified	Status
1.0	Initial Release.	10-Sep-2019	Superseded
2.0	Minor Procedure Improvements.	4-Jun-2021	Superseded
3.0	Update and amendment of policy framework and structure.	22-Dec-2021	Superseded
4.0	Refresh and addition of contents table	20-Dec-2022	Superseded
5.0	Addition of EU Sanctions list, fraud screening and ID provider and blocked countries list.	15-Mar-2024	Superseded
6.0	Draft redraft of policy framework and structure. Never adopted and never in force.	Dec-2025	Superseded
6.1	Compliance review and revision of the draft redraft. Never adopted and never in force.	Jul-2026	Superseded
7.0	Full redraft and restructure: consistent chapter renumbering throughout, alignment to current platform operations and CGA guidance, versioning consolidated to this table.	Aug-2026	Operative

Table of Contents

DEFINITIONS	5
ABBREVIATIONS	6
1. OVERVIEW	7
1.1. INTRODUCTION OF MONEY LAUNDERING	7
1.1.1. <i>Red Flag Typologies & Suspicious Activity Summary</i>	8
1.2. MANAGEMENT	9
1.3. LEGAL FRAMEWORK	9
1.4. RISK-BASED APPROACH	10
1.4.1. <i>Risk Identification and Assessment</i>	10
1.4.2. <i>Risk Mitigation</i>	10
1.4.3. <i>Risk Monitoring and Management Information Systems (MIS)</i>	11
1.4.4. <i>Documentation, Governance, and Accountability</i>	11
1.5. DATA PROCESSING SYSTEM	12
1.6. STAFF TRAINING	13
1.6.1. <i>Frequency and Timing</i>	13
1.6.2. <i>Scope: Who Must Be Trained ("Relevant Staff")</i>	13
2. CUSTOMER ACCEPTANCE AND REGISTRATION POLICY	13
2.1. INTRODUCTION	13
2.2. CUSTOMER ACCEPTANCE	13
2.3. RESTRICTIONS	14
2.4. INFORMATION ENTERED ON REGISTRATION	14
2.5. TERMS ACCEPTANCE	14
2.6. PREVENTION OF UNDERAGE GAMBLING	14
3. CUSTOMER AND BUSINESS RISK ASSESSMENT, RISK SCORING AND PROFILING	15
3.1. INTRODUCTION	15
3.2. BUSINESS RISK ASSESSMENT (BRA)	15
3.3. CUSTOMER RISK ASSESSMENT, CATEGORIZATION AND COMPLIANCE HANDLING	17
3.3.1. <i>Low Risk</i>	17
3.3.2. <i>Normal / Medium Risk</i>	17
3.3.3. <i>High Risk</i>	17
3.4. INDIVIDUAL STATUS	18
3.4.1. <i>PEP</i>	18
3.4.2. <i>Sanctions list</i>	18
3.4.3. <i>Adverse media</i>	18
3.5. GEOGRAPHICAL LOCATION	19
3.6. BEHAVIORAL MONITORING & DUAL-RISK DETECTION POLICY	20
3.6.1. <i>Dual-Scope Behavioral Monitoring</i>	20
3.6.2. <i>Behavioral Risk Aggregation</i>	20
3.6.3. <i>Overt Red Flags & Immediate Escalation</i>	20
3.7. PAYMENT METHODS AND RISK CATEGORIZATION	20
3.7.1. <i>Closed-Loop & Return-to-Source Payment Policy</i>	21
3.7.2. <i>General Rule & Principle</i>	21
3.7.3. <i>Regional & Technical Payout Limitations</i>	21
3.7.4. <i>Identity Matching & Beneficiary Verification</i>	21
3.8. FRAUD RED FLAGS	21
3.9. RISK SCORE CALCULATION	22
3.9.1. <i>Purpose & Objective</i>	22
3.9.2. <i>Scoring Methodology</i>	22
3.9.3. <i>Risk Thresholds & Escalation Triggers</i>	22
3.9.4. <i>Calibration & Confidentiality</i>	22
3.10. CUSTOMER DUE DILIGENCE LEVEL	23
3.11. CUSTOMER WITHDRAWAL PROCESSING & AML CLEARANCE	23
3.11.1. <i>Objective & Core Principles</i>	23
3.11.2. <i>Operational Phases</i>	24
3.11.3. <i>Recordkeeping & Audit Trail</i>	25
4. CUSTOMER DUE DILIGENCE	25

4.1. INTRODUCTION	25
4.1.1. Verification Tiers	25
4.1.2. Mandatory Customer Cooperation	26
4.1.3. Failure to Complete Due Diligence	26
4.1.4. Suspicious Activity Review	26
4.2. STANDARD CUSTOMER DUE DILIGENCE	26
4.2.1. Scope & Core Framework	26
4.2.2. Data Collection & Verification Requirements	26
4.3. DOCUMENTS ACCEPTANCE	27
4.3.1. Proof of Identity (POI) Requirements	27
4.3.2. Proof of Address (POA) Requirements	27
4.3.3. General Document Integrity & Quality Standards	28
4.4. THRESHOLD APPROACH	28
4.4.1. Application of Monetary Thresholds	28
4.4.2. Identification of Linked Transactions	28
4.4.3. Verification Framework	28
4.5. ONGOING MONITORING	29
4.5.1. Scope & Objectives	29
4.5.2. Core Monitoring Activities	29
4.5.3. Review Intervals & Trigger Events	29
4.6. ENHANCED DUE DILIGENCE	29
4.6.1. Purpose & Overview	29
4.6.2. High-Risk Triggers for EDD	29
4.6.3. Governance and Approval Requirements	30
4.6.4. Key Definitions: Source of Funds vs. Source of Wealth	30
4.6.5. Mandatory EDD Measures	30
4.6.6. Acceptable Source of Wealth (SoW) Documentation	31
4.7. POLITICALLY EXPOSED PERSONS AND SANCTIONS SCREENING	31
4.8. PROCEDURE FOR ACCOUNT CLOSURE	32
4.8.1. General Grounds for Closure	32
4.8.2. ML/TF-Related Account Closures	32
5. DEPOSIT AND WITHDRAWAL MANAGEMENT PROCEDURES	33
5.1. PLAYER ACCOUNT BALANCE, PROMO CASH & WAGERING FRAMEWORK	33
5.1.1. Dual-Balance Wallet Structure	33
5.1.2. Fund Deduction Priority (Wagering Mechanics)	33
5.1.3. Wagering Requirements & Cash Conversion	33
5.2. PLAYER DEPOSITS	33
5.2.1. Cryptocurrency Risk Management & Screening Policy	34
5.3. PLAYER WITHDRAWALS	34
6. SUSPICIOUS ACTIVITY REPORTING AND UNUSUAL TRANSACTION REPORTING	34
6.1. INTRODUCTION	34
6.1.1. Objective vs. Subjective Indicators	35
6.2. RED FLAGS INDICATORS AND INTERNAL ESCALATION	36
6.3. FAILURE TO COMPLETE CDD MEASURES	36
6.4. INTERNAL SUSPICIOUS ACTIVITY REPORT	37
6.4.1. Independent Escalation & Non-Interference	37
6.4.2. Contents of an Internal SAR	37
6.4.3. Duties of the Compliance Officer	37
6.5. EXTERNAL REPORT TO FIU	38
6.5.1. Link Analysis & Pattern Identification	38
6.5.2. SAR / UTR Filing Evaluation Checklist	38
6.6. REPORTING PROCEDURE	38
6.7. TIPPING OFF	39
6.7.1. Prohibition of Tipping off	39
7. INTERNAL CONTROL	39
7.1. INTRODUCTION	39
7.2. RECORDKEEPING	39
7.3. MONEY LAUNDERING REPORTING OFFICER	40
7.4. TRAINING	41
7.5. EMPLOYEES BACKGROUND CHECK	42

7.6. INTERNAL AND EXTERNAL REVISION AND STAYING UP TO DATE	43
APPENDIX 1	43

Definitions

“Money laundering” means:

the conversion or transfer of property, knowing or suspecting that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.

the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing or suspecting that such property is derived from criminal activity or from an act of participation in such an activity.

the acquisition, possession, retention or use of property, knowing or suspecting, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity.

participation in, association to commit, attempts to commit and aiding, abetting, facilitating, and counselling the commission of any of the actions referred to in points (a), (b) and (c).

“Senior management” means an officer or employee with sufficient knowledge of a company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, who does not need, in all cases, to be a member of the board of directors.

“Terrorist financing” means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.

“European Economic Area (EEA)” means Member State of the European Union or other contracting state which is a party to the agreement for the European Economic Area signed in Porto on the 2nd of May 1992 and was adjusted by the Protocol signed in Brussels on the 17th of May 1993, as amended.

“EU Directive” means the Directive 2015/849/, EU 847/2015, EC 1781/2006 of the European Parliament and the Council of May 2015 on the prevention of the use of the financial system for Money Laundering and Terrorist Financing.

“Money Laundering and Terrorist Financing” means the money laundering offences and terrorist financing offences defined in the Law.

“Manual” means the Policy on Know Your Customer (KYC) & Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) which has been drafted and adopted according to the EU Directive.

“Occasional Transaction” means any transaction other than a transaction carried out during an established Business Relationship formed by a person acting during financial or other business.

“Clients” means customers utilising Clubhouse Media N.V.'s services

“Politically exposed persons” means natural persons who are or have been entrusted with prominent public functions, other than middle ranking or more junior officials. The definition also covers their immediate family members or persons known to be close associates of such persons.

For the purposes of this definition the term "natural persons who are or have been entrusted with prominent public functions" includes the following:

- Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries.
- Members of Parliament or similar legislative bodies.
- Members of the governing bodies of political parties.
- Members of courts of auditors or of the boards of central banks.
- Ambassadors, chargés d'affaires and high-ranking officers in the armed forces.
- Members of the administrative, management or supervisory boards of State-owned enterprises. Family members include the following:

the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person

the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;

the parents of a politically exposed person; Persons known to be close associates means:

natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person and

natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

"Business Relationships" in accordance with the definition provided in the PMLFT business relationships must comprise three important cumulative elements, which are the following:

the relationship must be of a business, professional or commercial nature between two or more persons;

at least one of the persons involved in the relationship must be a subject person (whether undertaking a relevant financial business or a relevant activity); and

the relationship has, or is expected to have at the time when the contact is established, an element of duration.

Abbreviations

"AML" Anti-Money Laundering

"BRA" Business Risk Assessment

"CDD" Customer Due Diligence

"CRA" Customer Risk Assessment

"CTF" Counter-Terrorist Financing

"EDD" Enhanced Due Diligence

"FIU" Financial Intelligence Unit

"FS" Financial Sanction

“**FT**” Funding of Terrorism

“**KYB**” Know your Business

“**KYC**” Know Your Customer

“**ML**” Money Laundering

“**MLRO**” Money Laundering Reporting Officer

“**SAR**” Suspicious Activity Report

“**SDD**” Simplified Due Diligence

“**STR**” Suspicious Transaction Report

1. Overview

1.1. Introduction of Money Laundering

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:

1. **Placement** – placement of funds generated from crime into the financial system, either directly or indirectly (blending of funds, invoice fraud, smurfing).
2. **Layering** – the process of separating illicit proceeds from their source by creating complex “layers” of financial transactions designed to disguise the audit trail and provide anonymity (multiple bank transfers, investing in “cash” business).
3. **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:

1. For money laundering to occur, the funds involved must be the proceeds of criminal conduct.
2. 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.

Clubhouse Media N.V. (“CHM”) 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.

1.1.1. Red Flag Typologies & Suspicious Activity Summary

1.1.1.1. Account & Identity Anomalies (KYC Red Flags)

- **Multi-Accounting & Shared Data:** Multiple player accounts sharing the same IP address, physical address, device ID, phone number, email domain, or withdrawal endpoint (bank account, e-wallet, or crypto address).
- **Synthetic / False Identity:** Documents showing signs of alteration, fraudulent creation, or belonging to deceased individuals; reluctance or failure to provide valid secondary proof of identity/address.
- **Rapid Account Changes:** Sudden modification of personal data, contact details, or payment credentials immediately prior to submitting a large withdrawal request.
- **Third-Party Operations:** Accounts operated by someone other than the registered individual, including proxy betting, syndicate-controlled profiles, or accounts registered under family members/associates.

1.1.1.2. Transaction & Payment Anomalies (Financial Red Flags)

- **Pass-Through / "Casino as a Bank":** Depositing funds and immediately requesting a withdrawal with little to no wagering activity (using the platform solely as a fund-clearing or mixing tool).
- **Structuring / "Smurfing":** Intentionally splitting deposits or withdrawals into multiple small amounts to stay below verification, CDD, or statutory reporting thresholds (e.g., repeatedly depositing amounts just under NAF 5,000 / EUR 2,000).
- **Third-Party Payment Methods:** Attempting to deposit or withdraw using payment instruments (credit cards, bank accounts, e-wallets) registered under a name that does not match the player's profile.
- **Unusual Payment Methods or Velocity:** Rapid, successive deposits from multiple distinct cards, e-wallets, or crypto addresses within a short timeframe.
- **High-Risk Crypto / Anonymizing Tools:** Deposits coming from privacy coins, mixing/tumbler services, darknet-linked wallets, or exchanges with permissive/non-existent KYC controls.

1.1.1.3. Gameplay & Wagering Anomalies (Operational Red Flags)

- **Equal / Opposite Betting:** Placing opposing bets on the same event or game (e.g., betting on both Red and Black in roulette) to achieve zero-risk turnover and cash out funds clean.
- **Micro-Farming & Bonus Exploitation:** Automated or coordinated low-dollar wagering/deposit patterns designed to extract promotional cash or loyalty rewards systematically across multiple accounts.
- **Abnormal Staking Patterns:** Sudden, uncharacteristic jumps from minimal wagers to extremely high-value bets without an evident change in player profile or economic capacity.

1.1.1.4. Behavioral & Interaction Red Flags

- **Probing Thresholds / KYC Avoidance:** Repeatedly asking customer support staff about exact reporting limits, verification triggers, or how to withdraw without submitting identity documents.
- **Pressure & Coercion:** Attempting to bribe, threaten, or unduly pressure support staff to bypass compliance checks or speed up pending payouts.
- **Incoherent Source of Wealth/Funds:** Inability or refusal to explain the origin of large deposits, or providing financial documents that contradict the customer's known employment or economic standing.

1.2. Management

CHM — Clubhouse Media N.V., a limited liability company incorporated under the laws of Curaçao, with the company number 145680, having registered office at Korporaalweg 10, Willemstad, Curaçao — appointed a Compliance Officer as part of the art. 5g of the NOIS.

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 Compliance officer. Failure to comply with this Policy, or to report knowledge or suspicion as it requires, may result in disciplinary action and, where applicable law provides, personal liability.

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.

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:

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

CHM 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. Please refer to Section 1.6. Staff Training

1.3. Legal framework

CHM's Policy and Procedures were created subject to the relevant applicable legislation, in particular (but not limited to):

- The Penal Code of Curaçao (Wetboek van Strafrecht van Curaçao) — Title XXXI (Criminalization of Money Laundering, Professional Laundering, and Predicate Offenses, replacing the former NOPML framework).
- The National Ordinance on Games of Chance (Landsverordening op de Kansspelen – LOK).
- The National Ordinance on Identification when Rendering Services (NOIS / LID).
- The National Ordinance on the Reporting of Unusual Transactions (NORUT / LMOT).

This AML/CFT Policy is maintained in strict compliance with the laws of Curaçao and regulatory directives of the Curaçao Gaming Authority (CGA), specifically:

- **NOIS:** Landsverordening identificatie bij dienstverlening (P.B. 2017, no. 92, as amended).
- **NORUT:** Landsverordening melding ongebruikelijke transacties (P.B. 2017, no. 93, as amended).
- **LOK:** Landsverordening op de Kansspelen (P.B. 2024).
- **Penal Code:** Wetboek van Strafrecht van Curaçao, Title XXXI, Art. 2:404 (P.B. 2011, no. 48).
- **Sanctions:** Sanctielandsverordening 2014 (P.B. 2014, no. 55).

- EU-Directive 2015/849 of the European Parliament and of the Council of 20 May 2015;(4AMLD)
- EU-Directive 2018/843 of the European Parliament and of the Council of 30 May 2018; (5AMLD)
- EU-Directive 2018/1673 Of the European Parliament And Of The Council Of 23 October 2018;(ÂMLD)
- The FATF Recommendations.

1.4. Risk-based approach

CHM employs a Risk-Based Approach (RBA) to ensure that anti-money laundering (AML) and counter-terrorist financing (CTF) measures are proportionate to the specific risks identified across its operations. This framework allocates compliance resources efficiently by prioritizing higher-risk customers, payment methods, and geographic locations.

1.4.1. Risk Identification and Assessment

CHM conducts two levels of risk assessment: an Enterprise-Wide Risk Assessment (EWRA) to evaluate operational exposure, and individual Customer Risk Scoring at onboarding and throughout the customer lifecycle.

A. Enterprise-Wide Risk Factors

CHM regularly evaluates risks across four key categories:

- **Customer Risk:** Assessing the risk inherent in player demographics, including Politically Exposed Persons (PEPs), high-net-worth individuals, high-volume gamblers, and non-resident accounts.
- **Geographic Risk:** Evaluating risks associated with customer residency, nationality, IP location, and funding origins. Special scrutiny is applied to FATF Black and Grey-listed jurisdictions, tax havens, and regions subject to international sanctions.
- **Product and Service Risk:** Assessing the vulnerability of gaming products, including high-frequency live casino games, promotional bonuses, and unutilized deposit cash-outs.
- **Delivery Channel & Payment Risk:** Mitigating risks associated with non-face-to-face digital onboarding, third-party payment processors, anonymizing payment tools (e.g., prepaid vouchers, virtual cards), and cryptocurrency transfers processed through third-party providers (Naewe and BVNK).

B. Individual Customer Risk Scoring

Customer risk ratings (Low, Medium, or High) are assessed and formally assigned by the Compliance function during Customer Due Diligence (CDD/EDD) and withdrawal reviews. The team evaluates profile details, submitted documentation, geographic exposure, and account activity to determine the player's final risk tier if necessary.

1.4.2. Risk Mitigation

Once risks are identified, CHM applies targeted controls to lower residual risk to an acceptable level, aligned with its board-approved Risk Appetite Statement.

A. Proportional Customer Due Diligence (CDD)

- **Low/Normal Risk:** standard deposit/withdrawal thresholds, and routine monitoring.
- **High Risk:** Triggers mandatory Enhanced Due Diligence (EDD). This includes:

- Verification of Source of Funds (SoF) and Source of Wealth (SoW).
- Verification that payment accounts match the customer's identity.
- Senior management or MLRO sign-off before establishing or continuing the business relationship.

B. Automated Operational Controls

- **PEP & Sanctions Screening:** Screening at identity verification via Shufti Pro, with re-screening on risk triggers, including significant changes to a player's account details. CHM will apply ongoing screening to higher-risk players where the combined risk indicators warrant it, or the Compliance Officer deems it necessary.
- **Crypto Risk Mitigation:** Automatic crypto-to-fiat conversion upon deposit via Naewe and BVNK, with the payment providers' blockchain analytics screening applied to reject wallet transfers tied to darknet markets, mixers, ransomware, or stolen funds.
- **Financial Threshold Controls:** Immediate enforcement of EDD and identity re-verification upon reaching individual or linked transaction thresholds of EUR 2,200 (or local currency equivalent).
- **Payment Restrictions:** Strict prohibition of third-party payment instruments and mandatory enforcement of 1:1 deposit-to-wager turnover rules to prevent pass-through "casino-as-a-bank" activity.

1.4.3. Risk Monitoring and Management Information Systems (MIS)

Risk management is a continuous process. CHM maintains real-time monitoring and reporting infrastructure to track emerging threats and profile shifts.

A. Transaction and Behavioral Monitoring

- **Transaction Risk Data:** CHM's payments platform attaches automated risk analysis to every transaction, which CHM reviews for suspicious patterns, including velocity spikes (rapid successive deposits), multi-accounting, shared device/IP environments, structuring/smurfing below reporting thresholds, and promotional bonus exploitation.
- **Periodic Profile Reviews:** High-risk accounts undergo formal re-reviews by the compliance team at least every six (6) months, or immediately upon a material trigger event (e.g., sudden PEP status change or unexpected deposit escalation).

B. Management Information Systems (MIS) Reporting

The Compliance Officer / MLRO compiles monthly compliance reports for senior management containing key metrics:

- Distribution of player risk categories (Low vs. Medium vs. High).
- Volume of EDD files opened, approved, and rejected.
- Number of accounts frozen, closed, or flagged for multi-accounting/bonus abuse.
- Volume and nature of internal suspicious activity reports, along with external Unusual Transaction Reports (UTRs) / Suspicious Activity Reports (SARs) submitted via goAML or local authorities.

1.4.4. Documentation, Governance, and Accountability

CHM maintains a clear audit trail and corporate governance structure to ensure regulatory accountability at all levels.

A. Record Retention & Audit Trail

- **5-Year Retention Standard:** All KYC verification records, EDD documents, transaction histories, risk scoring logs, internal SAR evaluations, and external UTR filings are retained securely for a minimum of five (5) years post-account closure.
- **Decision Logging:** Compliance decisions—specifically determinations not to file a UTR/SAR following an internal flag—must be fully documented with clear rationale for regulatory inspection.

B. Board & Senior Management Oversight

- **Policy Ownership:** The Board of Directors holds ultimate accountability for CHM's AML/CFT framework and must formally approve the Risk Assessment Policy and Risk Appetite Statement annually.
- **Annual MLRO Report:** The MLRO presents an annual comprehensive report to the Board detailing the effectiveness of AML controls, audit findings, regulatory updates, staff training results, and resource requirements.
- **Resourcing:** Senior management guarantees the Compliance function and MLRO sufficient operational independence, technical tools, budget, and personnel to execute their duties without commercial conflict of interest.

1.5. Data processing system

CHM operates its internal data processing system to detect high-risk scenarios, money laundering, and terrorist financing in day-to-day operations.

The Data processing system consist of the following mechanisms:

- Standard Document Verification (Delayed CDD Framework)
- Low/Normal-Risk Thresholds: Under Curaçao regulations (NOIS/LOK/CGA guidance), delaying full identity document collection (e.g., government ID, proof of address) is legally permissible for low- or normal-risk players until:
- The player submits their first withdrawal (WD) request, OR
- The player reaches the cumulative deposit or wagering threshold of EUR 2,200 (or local equivalent, such as NAf 4,000), whichever occurs first.
- Immediate Verification Exceptions (Immediate CDD/EDD Required)
- High-Risk Override: Delayed document verification cannot be applied as an absolute rule for all users. Verification may be required at any earlier point, including at or shortly after registration—regardless of whether a withdrawal is requested or the EUR 2,200 threshold is met—where any of the following apply:
- Geographic Risk: The customer resides in a high-risk or FATF Black/Grey-listed jurisdiction.
- Payment Risk: The customer utilizes high-risk cryptocurrency transactions, unverified third-party wallets, or non-custodial payment methods.
- Behavioral Risk / Red Flags: The account is flagged for suspicious activity, such as multi-accounting, bonus abuse, or structural deposit patterns.
- Politically exposed person (PEP) and sanction list checks are performed by the relevant software
- Transaction monitoring is managed by trained staff
- Reporting of all suspected money laundering cases to the Compliance Officer and the FIU.

CHM will monitor trends and changes connected to ML/TF and will develop additional internal procedures to keep it up to date.

1.6. Staff Training

Upon joining CHM and thereafter annually, all staff (including outsourcing teams) will get training on AML/CFT procedures and associated policies. The training will be supplied by online and face-to-face training providers or by the appropriate CHM's specialist. The specific employees are to be trained depending on the individual risk analysis.

Minimum Mandatory Training Requirements

1.6.1. Frequency and Timing

New Joiners (Induction Training): Mandatory AML/CFT induction training must be completed by all relevant new employees before or within 30 days of starting their role, and strictly before they are permitted to handle customer accounts, review KYC, or process payouts.

Annual Refresher Training: Refresher training must be conducted at least once every 12 months for all existing relevant staff to cover updated laws, emerging typologies, and policy changes.

Specialized Officer Requirement: The Compliance Officer / MLRO must undergo at least 10 hours of dedicated, advanced AML/CFT training annually (e.g., CAMS, AMLFC, or accredited regulatory updates).

1.6.2. Scope: Who Must Be Trained ("Relevant Staff")

Training cannot be limited to the compliance team alone. "Relevant employees" legally includes:

Customer Support & Operations: Frontline staff who interact directly with players.

Payments & Risk/Fraud Teams: Staff handling deposits, withdrawals, and fraud alerts.

Compliance & Legal Personnel: Staff managing CDD/EDD and SAR/UTR filings.

Senior Management & Board Members: Executives with ultimate supervisory responsibility.

2. Customer Acceptance and Registration Policy

2.1. Introduction

Before gambling, depositing or placing real-money stakes, 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 CHM may or not accept potential customers and describes the registration process.

2.2. Customer Acceptance

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

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 IP address, email address and mobile number. 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.

Checks by IP address, email address and mobile number are done in order to prevent players opening multiple accounts in order to bypass the AML threshold.

Existing customers who have an existing exclusion on the site. Individuals with fraud red flags.

Individuals considered to be PEP, under Sanctions or listed in any blacklists — in particular the international sanctions and watchlist databases maintained by the United Nations, the European Union, the United States (OFAC), the United Kingdom (HMT) and other principal authorities, as screened through CHM's screening provider.

2.4. Information Entered on Registration

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

- First Name and Last Name,
- Date of Birth,
- Country of Residence,
- Email address and verified mobile number,
- 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. Prevention of Underage Gambling

Prevention of Underage Gambling

CHM enforces strict technical and operational controls to prevent underage individuals from registering or accessing its services.

To successfully establish an account, applicants must be at least 18 years of age or the statutory legal gambling age in their jurisdiction of residence, whichever is higher.

The Date of Birth provided during account registration is systematically cross-checked and verified against official government-issued identification documents during the Customer Due Diligence (CDD) and verification process. Any account found to belong to a minor will be terminated immediately, with all deposits returned (where legally permitted) and winnings voided.

3. Customer and Business Risk Assessment, Risk Scoring and Profiling

3.1. Introduction

Within the risk-based framework, CHM 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 CHM's policies and procedures are based on the following:

- Actual regulatory and legal requirements;
- Guidance provided by GCB and FIU;
- CHM's own internal evaluation of its overall business risk assessment, and its knowledge and experience with its customers.

3.2. Business Risk Assessment (BRA)

CHM's activity necessitates the conducting of a Business Risk Assessment (BRA) whereby all products/services / verticals and jurisdictions are given due consideration in terms of risk posed. A qualitative and a quantitative approach has been undertaken and the result of which was scrutinised through the application of a quantitative approach, which assesses the risk posed by the client, products, payment, transaction, interface, employee's and MLRO duties including also internal security.

The BRA is held separately and may be accessed accordingly. For any updates or changes within such assessment a relevant update is provided and for which attendance will be taken, and knowledge of such will be tested accordingly through the following methods:

- Examination/ assessment
- Workshops
- A sampling of work

The policies and procedures are influenced by the BRA, assessing the inherent and residual risk of risk factors and manifestation thereof. As a must, every employee is to be made aware of such policy and the employee's knowledge of the policy is periodically tested.

The BRA is an all-encompassing view of the risks posed to CHM, being: vulnerabilities and threats which may be encountered by CHM through the course of its business, as well as the mitigating factors conducted prior to the seed funding, and continuing on an ongoing basis thereafter, as new or material developments arise.

The residual risk as a result of such assessment will thereby determine whether a particular risk will fall within the risk appetite, or if the risk is too high, so as to outrightly refuse such business. In terms of products, CHM may opt to act so as if the risk falls within a level which is not within the risk appetite, such product's risk mitigators will be increased. If such a product's risk still falls within a level of risk that is not acceptable, the product in question will be discontinued.

A GAP analysis is also conducted to determine any weaknesses to follow through a product offering. The BRA is conducted prior to the launch of any product to identify the risk associated, mitigating factors, and whether such product will fit CHM's risk appetite. The factors which are included in the BRA are as follows:

- Product

- Service
- Transaction
- Geography
- Customer
- Interface
- Employee
- Duties of the MLRO
- Third parties

The manifestation of risk of the factors included above are duly assessed in relation to money laundering and funding of terrorism. In developing the operational AML/CFT procedures set out below, CHM has reviewed its business processes against the criteria set out above with the aim of taking a 'risk-based approach' to the development of AML/CTF controls.

CHM has developed a risk assessment which summarises the areas of low, high and medium risk which it is exposed to, in line with its risk-based approach. CHM has also performed a risk assessment of its operations which are also carried out periodically, depending on the nature of said risk. For example, due to the evolving nature of technology, risk assessments pertaining to technological products used by CHM shall be carried out yearly, or when new risks or products are in place.

The BRA is updated whenever substantial changes to CHM's systems, processes and overall operations are carried out. It is also re-evaluated, depending on the National Risk Assessment (NRA), as well as based on ongoing monitoring and trends.

The Business ML/FT Risk Assessment and related measures, policies, controls and procedures are to be recorded and made readily available for review by interested authorities, including the Curacao Gaming Control Board (GCB) at any time. All aspects of the BRA are covered, including:

- Methodology adapted
- The reasons for considering a risk factor as high/low/medium risk
- The outcome of the BRA
- Any information sources used.

The BRA is an encompassing view of inherent risks, vulnerabilities and threats to CHM, the mitigating factors conducted and the residual risk, and the means and measures employed within which they are mitigated. CHM's policies, internal controls, compliance management and procedural documentation, is influenced by the BRA. Every CHM employee is made aware of BRAs and updates, knowledge of which is tested periodically. The BRA is assessed and approved by the Board of Directors. It is made readily available to the GCB upon request.

The manifestation of risk of the factors above are assessed in relation to ML and FT. In developing the operational AML/CTF policy and procedures, CHM has reviewed its business processes against the criteria set out above to take a 'risk-based approach' to the development of AML/CTF controls. The BRA summarises the factors into low, medium and high risk. Due to the nature and evolving technology, the BRA shall be carried out every year unless material changes are noted.

New or material changes shall warrant a re-evaluation of the BRA; such changes shall also be applicable upon introduction of new products, services, jurisdictions and payment methods. Changes within the regulatory framework shall also be considered as pertinent

elements that shall contribute to a review of the risk. The business risk assessment is also a criminal risk assessment for which perceived data is taken into account to further prevent any risk from possibly happening. The BRA will be carried out at least annually.

3.3. Customer Risk Assessment, Categorization and Compliance handling

Based on the information supplied at registration (e.g. customer home address, customer location, customer age, whether PEP/sanctions), CHM will make an initial risk assessment of each customer. Customers thus start their gambling history with CHM 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.

3.3.1. Low Risk

- Standard retail players from low-risk countries who play occasionally, deposit modest amounts using transparent, traditional payment methods (e.g., standard debit card in their own name), and have clear identity verification.
- **Compliance Handling:** Standard Customer Due Diligence (CDD). standard transaction limits monitoring, and light ongoing monitoring.(sample based)

3.3.2. Normal / Medium Risk

- Active players who deposit or play regularly, near standard verification thresholds, or use payment methods that carry slightly higher inherent risk (e.g., e-wallets like Skrill/Neteller).
- **Compliance Handling:** Regular ongoing monitoring, periodic profile updates (e.g., re-verifying documents every 12 to 24 months), and standard transaction trigger alerts.

3.3.3. High Risk

- Players who meet specific high-risk triggers, such as:
 - **PEP status:** Politically Exposed Persons or their family/close associates (RCAs). A confirmed PEP is rejected or closed outright (see clause 3.4.1).
 - **High Velocity / High Value:** High-volume players depositing/withdrawing large amounts rapidly (e.g., crossing EUR 2,000 / 2,200 threshold).
 - **High-Risk Jurisdictions:** Players residing in or using funding from countries on FATF black/grey lists.
 - **Payment Anomalies:** Heavy cryptocurrency usage, prepaid cards, or third-party payment attempts.
 - **Behavioral Red Flags:** Frequent structural deposits (smurfing), immediate withdrawals without playing, or uncooperative responses during verification.

- **Compliance Handling:** Enhanced Due Diligence (EDD) is legally required. This involves collecting Source of Wealth (SoW) / Source of Funds (SoF), increased account monitoring, bi-annual profile reviews, and senior management (Compliance Officer / MLRO) approval to maintain the relationship.

The Two Contexts of Risk in iGaming

Risk categorization in gaming usually exists across two separate operational tracks:

- **AML / Financial Crime Risk:** Evaluating the likelihood of money laundering, fraud, terrorist financing, or sanctions evasion (as outlined above).
- **Safer Gambling / Responsible Gambling (RG) Risk:** Evaluating the player's risk of gambling harm or addiction (e.g., Low, Moderate, High Risk of Problem Gambling) based on play frequency, night-time play, chasing losses, or rapid deposit escalations.

3.4. Individual status

3.4.1. 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 new or existing customer that is found to be a PEP or relative of such will have their account rejected or closed.

3.4.2. Sanctions list

Governments and international authorities publish sanctions lists to combat persons engaged in illegal activities. Sanction lists include sanctioned people, organisations, or governments. Companies, individuals, organisations, 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.

3.4.3. Adverse media

Adverse Media Screening Policy

3.4.3.1. Definition & Scope

Adverse Media (or "Negative News") refers to any publicly available, credible information—derived from media outlets, regulatory bodies, law enforcement agencies, or legal databases—that links a customer or beneficial owner to financial crime, money laundering, terrorist financing, fraud, corruption, or other predicate offenses.

3.4.3.2. Screening & Identification

Adverse media checks may be conducted on a risk basis through CHM's screening provider (Shufti Pro) and during manual compliance reviews.

3.4.3.3. Procedure for Adverse Media Hits

When negative news is identified in relation to a new applicant or existing customer, the following protocol applies:

Mandatory EDD Classification: Any plausible or confirmed adverse media match automatically elevates the customer's risk profile to High Risk and triggers mandatory Enhanced Due Diligence (EDD).

Plausibility & Severity Assessment: The Compliance function evaluates the credibility, recency, and relevance of the information (e.g., distinguishing between formal financial crime charges versus unverified personal allegations).

Governance & Determination:

Rejection / Account Closure: If the adverse media confirms involvement in financial crime, terrorist financing, severe fraud, or active law enforcement prosecution, the registration must be rejected or the existing account terminated immediately.

MLRO Approval: Retaining or onboarding any customer associated with verified adverse media requires a formal risk assessment and explicit written approval from the Compliance Officer / MLRO.

Regulatory Reporting: If the findings reveal reasonable grounds to suspect that funds are linked to criminal activity, an internal suspicious activity report must be escalated to file an Unusual Transaction Report (UTR) / Suspicious Activity Report (SAR) with the relevant Financial Intelligence Unit (FIU).

3.5. Geographical location

If CHM identifies that the customer resides in a High-risk county, 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. CHM 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 FATF "Black List"

(High-Risk Jurisdictions subject to a Call for Action)

These countries have severe strategic deficiencies in their anti-money laundering and counter-terrorist financing regimes.

The FATF "Grey List"

(Jurisdictions under Increased Monitoring)

These countries are actively working with the FATF to address strategic deficiencies in their AML/CFT regimes and are subject to increased monitoring.

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

3.6. Behavioral Monitoring & Dual-Risk Detection Policy

3.6.1. Dual-Scope Behavioral Monitoring

CHM monitors customer account activity using a combination of automated transaction-risk tooling and manual review. This framework operates a dual-scope detection model designed to concurrently identify:

- **Anti-Money Laundering / Counter-Terrorist Financing (AML/CFT) Red Flags:** Irregular financial flows, velocity anomalies, pass-through turnover, and abnormal wagering patterns.
- **Responsible Gambling (RG) Markers of Harm:** Behavioral indicators pointing to problem gambling, uncharacteristic spending escalation, or potential financial distress.

3.6.2. Behavioral Risk Aggregation

Observed behavioral anomalies generate weighted scores within the Customer Risk Engine. These behavioral indicators aggregate alongside profile and transactional risk factors to maintain an updated, holistic assessment of overall account risk.

3.6.3. Overt Red Flags & Immediate Escalation

In instances where explicit or severe ML/TF behaviors are observed (e.g., severe pass-through withdrawals, active structuring, or unexplainable origin of funds):

- The account bypasses routine cumulative scoring thresholds.
- The file is immediately escalated for mandatory Enhanced Due Diligence (EDD).
- The Compliance function conducts an expedited review to evaluate the account and, where warranted, initiate the formal investigation and Suspicious Activity Report (SAR) / Unusual Transaction Report (UTR) process.

3.7. Payment Methods and risk categorization

CHM assesses the inherent risk of payment instruments based on fund traceability, source-of-funds transparency, and Return-to-Source (closed-loop) compatibility:

Payment methods that allow full auditability, link directly to a regulated financial institution, and support Return-to-Source (RTS) payouts are classified as Low Risk.

Clear traceability of the account holder's identity, verified origin of funds at the financial institution level, and technical capability to return funds directly to the depositing account.

Payment channels that obscure the identity of the sender, rely on cash funding, or prevent Return-to-Source payouts are classified as High Risk.

Payment Method	Risk Rating
Bank-linked transfer methods and debit cards issued by regulated banks	Low
Licensed e-wallets	Medium
Non-refundable prepaid vouchers, cash-backed deposit mechanisms, privacy-focused cryptocurrencies, and unverified third-party e-wallets.	High

3.7.1. Closed-Loop & Return-to-Source Payment Policy

3.7.2. General Rule & Principle

To prevent money laundering, payment manipulation, and unauthorized third-party transfers, CHM prioritizes ownership-verified payouts. Withdrawals may be returned to the depositing payment instrument where the payment provider supports it; in all cases the destination must be verified as belonging to the registered player.

3.7.3. Regional & Technical Payout Limitations

CHM recognizes that certain deposit methods or geographic jurisdictions do not support technical returns, or operate with limited payout channels (e.g., regions where a single local payout method serves as the primary or exclusive withdrawal channel).

In instances where withdrawing via the original deposit method is not technically feasible:

- The customer will be routed to an approved alternative payout method
- The primary operational requirement shifts to Strict Identity & Ownership Matching.

3.7.4. Identity Matching & Beneficiary Verification

Whenever a payout is processed to a channel different from the deposit source due to system or regional availability:

- Payouts will only be executed if the alternative destination account (e.g., the receiving account or bank) is conclusively verified to belong to the exact same individual who registered the gaming account and made the initial deposit.
- Third-party payouts are strictly prohibited under all circumstances.
- CHM reserves the right to request proof of account ownership (e.g., bank statement, screenshot of e-wallet profile, or void cheque) and apply Enhanced Due Diligence (EDD) prior to approving any alternative withdrawal request.

3.8. Fraud red flags

CHM maintains an automated Anti-Fraud Risk Management System designed to identify, mitigate, and prevent sophisticated technical, financial, and behavioral fraud typologies. Controls are configured to detect:

- Account & Identity Risks: Synthetic identity creation, identity theft, Account Takeover (ATO), multi-accounting, and proxy/VPN location obfuscation.
- Payment & Transactional Fraud: Credit card fraud, Card-Not-Present (CNP) fraud, unauthorized chargebacks, and payment instrument manipulation.
- Operational & Game Integrity Risks: Bot attacks, syndicate/fraudulent traffic, and player collusion.

CHM recognizes that fraudulent activities frequently act as predicate offenses or early indicators for money laundering and financial crime.

Consequently, any customer account triggering a high-risk fraud indicator or anomaly is immediately subjected to mandatory escalation:

3.9. Risk Score Calculation

3.9.1. Purpose & Objective

The purpose of the automated risk scoring system is to detect cumulative ML/TF risk indicators—individual behaviors, transaction patterns, or profile attributes that may appear minor in isolation, but collectively represent elevated money laundering or terrorist financing risk.

3.9.2. Scoring Methodology

Customer risk is assessed by the Compliance function using automated transaction-risk data and manual review, against a weighted internal scoring framework.

- **Weighted Factors:** Risk parameters — including player demographics, geographic origin, payment methods, transaction velocity, wagering anomalies, and PEP/Sanctions screening results — carry weightings set and maintained by the Compliance Officer. The heaviest weightings attach to confirmed PEP or sanctions exposure, adverse media, high-risk jurisdictions, and pass-through or structuring behaviour.
- **Cumulative Assessment:** Indicators that appear minor in isolation aggregate into the customer's overall risk assessment; higher aggregate risk corresponds to a higher risk classification.

3.9.3. Risk Thresholds & Escalation Triggers

The assessment places each customer in one of three tiers (Low, Normal/Medium, or High):

- A customer whose combined indicators reach the internally defined high-risk level is escalated to operational controls, including mandatory Enhanced Due Diligence (EDD), increased transaction monitoring, and review by the Compliance function.
- A customer's risk classification is updated whenever new information or observed behaviour warrants it.

3.9.4. Calibration & Confidentiality

- **Confidentiality:** Specific scoring formulas, parameter weightings, and threshold triggers are strictly internal to prevent gaming or circumvention by bad actors.
- **Continuous Calibration:** The Compliance Officer / MLRO periodically reviews and recalibrates the risk scoring model to reflect evolving threats, newly identified typologies, and regulatory changes.

Automated risk indicators

Trigger Category	Specific Indicator	Operational & Compliance Action
Sanctions & Watchlists	Confirmed match against international Sanctions or PEP/Watchlists	Immediate Account Freeze. Block all transactions, freeze remaining funds, and submit a UTR/SAR via goAML.
Underage Gambling	Applicant is under 18 or the legal age in their jurisdiction	Immediate Account Termination. Reject registration, void winnings, and handle deposits per regulatory rules.

Trigger Category	Specific Indicator	Operational & Compliance Action
Syndicate Fraud	Confirmed multi-accounting or automated bonus farming syndicate	Immediate Payout Decline & Account Freeze. Void promotional funds, block associated payment methods/IPs.

Risk Classification & Action

Risk Category	Required Compliance & Operational Action
Low Risk	Standard transaction limits and automated monitoring.
Medium / Normal Risk	Increased transaction monitoring. Full CDD document verification required prior to first withdrawal or reaching EUR 2,200 cumulative deposits. Periodic profile review every 12–24 months.
High Risk	Mandatory Enhanced Due Diligence (EDD). Immediate verification of Source of Funds (SoF) and Source of Wealth (SoW). Bi-annual profile review (every 6 months). Explicit MLRO sign-off required to maintain the account relationship.

3.10. 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 upon WD / DP over the threshold / and indicator for EDD	X	X	X
Collect additional personal details		X	X
Collect Source of Funds/ Wealth info		X	X (with documentation)
Ongoing monitoring	X (sample based)	X	X (Enhanced)
Additional measures to address any other risk identified			X
Report suspected cases of ML/FT	X	X	X

3.11. Customer Withdrawal Processing & AML Clearance

3.11.1. Objective & Core Principles

Withdrawal processing is governed by three fundamental rules:

- **Mandatory 1x Wagering Turnover:** Players must wager deposited funds at least once (1x) prior to withdrawal to prevent the platform from being utilized as a money-pass-through or banking channel.
- **Verified-Ownership Payout:** Withdrawals are processed to a payment method verified to belong to the registered player; where the deposit method supports payouts, they may be returned to it. Refer to Section 3.7 Payment Methods and risk categorization

- **Risk-Based Verification:** Payout approval is contingent upon the player's risk classification and the validity of their Customer Due Diligence (CDD/EDD) documentation.

3.11.2. Operational Phases

Phase 1: Technical & Automated Pre-Checks

Upon submission of a withdrawal request, the system automatically performs pre-processing validation:

- **Wagering Requirement Verification:** The system checks that the deposit turnover requirement (clause 5.1.3.1) has been met.
- **Bonus & Active Wager Check:** Confirms no active bonus conditions or unresolved bets lock the requested funds.
- **Fraud System Scan:** Verifies that the account has no active fraud red flags (e.g., bot activity, account takeover alerts, multi-accounting flags, or chargeback history).

Control Action: If pre-checks fail, the withdrawal is automatically held or cancelled, and the player is notified of the unfulfilled requirement

Phase 2: Risk-Based Routing

The system routes the request based on the player's assigned risk classification:

- **Low-Risk Accounts:** Routed to automated or expedited processing, provided identity documentation on file remains fully verified and unexpired.
- **Medium & High-Risk Accounts:** Suspended from automatic processing and placed into the AML Review Queue for manual clearance.

Phase 3: Manual Verification & AML Clearance

For accounts in the AML Review Queue, the Compliance function performs the following mandatory checks:

A. Document Validity Review

- Verify that Proof of Identity (POI) and Proof of Address (POA) are on file.
- Ensure all documents remain valid and unexpired (POA must be dated within the last 3 to 6 months).
- **If documents are expired or missing:** The withdrawal is placed on Hold, and the player is prompted to submit updated documentation.

B. Closed-Loop & Payment Ownership Verification

- **Ownership Verification:** The analyst verifies that the requested withdrawal destination belongs to the registered player, returning funds to the deposit method where supported.
- **Alternative Routing (Technical / Regional Limitations):**
 - If the deposit method cannot receive payouts, the analyst verifies that the alternative destination account (e.g., a local transfer method or direct bank transfer) is held in the exact same legal name as the registered player.
 - Proof of Account Ownership (e.g., bank statement, bank portal screenshot, or e-wallet profile clearly displaying the player's name and account details) must be reviewed and approved prior to release.

- **Third-Party Payout Prohibition:** Any payout requested to a third-party account is strictly rejected.

C. Enhanced Due Diligence (EDD) & High-Value Triggers

- If the withdrawal causes cumulative deposits/withdrawals to breach statutory thresholds (e.g., EUR 2,200), or if the account is rated High Risk, mandatory Enhanced Due Diligence (EDD) applies.
- The Compliance function must collect and verify Source of Funds (SoF) and/or Source of Wealth (SoW) documentation before approving the release.

Phase 4: Final Approval, Rejection, or SAR Escalation

Once manual review is complete, the reviewing compliance staff member executes one of three actions:

Decision	Criteria	Action
Approve	Docs valid, turnover met, payment ownership confirmed, no suspicious activity.	Release funds for payment processing.
Hold / Reject	Expired documents, unfulfilled 1x turnover, or unverified payout ownership.	Cancel or hold withdrawal; notify player of required documents or play-through requirements.
Escalate (SAR/UTR)	Suspected pass-through money laundering, third-party payout attempt, synthetic identity, or refusal to supply SoF/SoW.	Freeze withdrawal, freeze account balance if necessary, escalate file to MLRO for Suspicious Activity Report (SAR) evaluation via goAML.

3.11.3. Recordkeeping & Audit Trail

Every withdrawal decision—whether approved, rejected, or held for documentation—must be logged in the system with:

- Timestamp of review and identity of the reviewing analyst/MLRO.
- Verification status of documents reviewed.
- Explicit rationale if an alternative payout channel (e.g., a regional payout method) was authorized.
- All associated logs stored for a mandatory statutory period of 5 years post-account closure.

4. Customer Due Diligence

4.1. Introduction

Customer Due Diligence Framework & Cooperation Requirements

4.1.1. Verification Tiers

CHM applies a proportional approach to customer verification, formally distinguishing between standard Customer Due Diligence (CDD) and Enhanced Customer Due Diligence (EDD) based on customer risk categorization, transaction thresholds, and behavioral triggers.

4.1.2. Mandatory Customer Cooperation

Customers are required to cooperate fully with all CHM requests for identification, address verification, and financial documentation (including Source of Funds and Source of Wealth) necessary to fulfill statutory due diligence obligations.

4.1.3. Failure to Complete Due Diligence

Where CHM is unable to apply or complete required CDD or EDD measures—whether due to customer refusal, non-responsiveness, or unresolvable documentation discrepancies—CHM shall strictly enforce the following measures:

- Refuse to establish a new business relationship or register the account.
- Immediately halt all transaction activity and refuse pending withdrawal requests.
- Freeze and terminate any existing customer relationship.

4.1.4. Suspicious Activity Review

In all instances where due diligence cannot be completed, the customer file must be immediately escalated to the Compliance Officer / MLRO to assess whether the circumstances warrant filing a Suspicious Activity Report (SAR) / Unusual Transaction Report (UTR) with the relevant Financial Intelligence Unit (FIU)

4.2. Standard Customer Due Diligence

Standard Customer Due Diligence (CDD)

4.2.1. Scope & Core Framework

CHM enforces Standard Customer Due Diligence (CDD) to mitigate Money Laundering and Terrorist Financing (ML/TF) risks. The CDD framework consists of two mandatory operational pillars:

Identification: Gathering personal identity details directly from the customer during the account registration process.

Verification: Validating the provided identity details against reliable, independent documents, data, or electronic verification sources (such as independent electronic verification through Shufti Pro).

Where CHM uses third-party providers to perform verification or screening, responsibility for compliance with CHM's due-diligence obligations remains with CHM.

4.2.2. Data Collection & Verification Requirements

To establish a customer profile and satisfy statutory compliance standards, CHM collects and verifies the following attributes:

A. Identification Data (Collected at Registration)

Full Legal Name: First name(s) and surname.

Date of Birth: To verify legal gambling age eligibility.

Full Residential Address: Street name, house/building number, postal/ZIP code, city, and country of residence.

Contact Information: Verified email address and/or phone number.

B. Identity & Address Verification Documents (Collected upon Withdrawal / Threshold / High-Risk Trigger)

Proof of Identity (POI): A valid, unexpired, government-issued photo ID (e.g., international passport, national identity card, or driver's license).

Proof of Address (POA): A recent document—issued within the last 3 to 6 months—clearly displaying the customer's full name and residential address (e.g., utility bill, bank statement, or government correspondence).

4.3. Documents acceptance

4.3.1. Proof of Identity (POI) Requirements

To verify a customer's legal name, date of birth, and nationality, CHM requires a clear, unexpired, government-issued photo identification document.

Accepted POI Documents:

- International Passport (must show signature page and full Machine Readable Zone / MRZ).
- National Identity Card (front and back).
- Driver's License (front and back).
- Official Government-Issued Travel Document or Residence Permit (front and back).

POI Validation Criteria:

- Must be fully valid and unexpired at the time of submission.
- Must contain a clear photo of the account holder, full legal name, date of birth, and document expiry date.
- Must match the exact personal details provided during account registration.
- Biometric Match: Where facial biometric verification is enabled as part of automated verification, the document photo is validated against a real-time facial liveness check / selfie.

4.3.2. Proof of Address (POA) Requirements

To verify residential address, the customer must provide an official document displaying their full legal name and current home address.

4.3.2.1. Accepted POA Documents:

- Utility Bill: Water, electricity, gas, sanitation, or fixed landline internet bill (issued within the last 3 months).
- Financial Statement: Bank statement, credit card statement, or e-money account statement from a licensed institution (issued within the last 3 months).
- Government Correspondence: Official tax assessments, municipal letters, or local authority correspondence (issued within the last 6 months).
- Formal Lease / Tenancy Agreement: Currently active lease agreement (must show signatures of both tenant and landlord, and remain within the active tenancy period).

4.3.2.2. Unacceptable POA Documents:

- Mobile phone (cellular) bills.
- Commercial or business address correspondence.
- Medical bills or insurance invoices.

- Unofficial, handwritten, or P.O. Box receipts.

4.3.3. General Document Integrity & Quality Standards

All submitted documents must meet strict physical and digital formatting criteria prior to approval:

- **Full Document View:** The complete document must be captured, showing all four corners. Cropped images or truncated documents will be rejected.
- **Image Quality:** Documents must be captured in high-resolution, full-color format. Images that are blurry, distorted, overexposed (flash glare), or underexposed will be declined.
- **Digital vs. Physical Documents:** Original PDF statements directly downloaded from bank or utility portals are accepted. For physical documents, photos must be taken directly from the original paper—black-and-white photocopies, scans of scans, or photos taken off a computer monitor screen are strictly prohibited.
- **Language & Translation:** Documents issued in non-Latin alphabets (e.g., Cyrillic, Arabic, Chinese) must be accompanied by a certified translation into English if automated OCR systems (Shufti Pro) cannot parse the data.

4.4. Threshold approach

Threshold Checks & Linked Transactions Policy

4.4.1. Application of Monetary Thresholds

CHM applies Enhanced Due Diligence (EDD) measures to any customer transaction—or series of linked transactions—that reaches or exceeds EUR 2,200 [or local currency equivalent].

For the purposes of this policy, a "Transaction" includes:

Deposits: Any deposit or funding operation required to participate in remote gambling activities.

Winnings & Withdrawals: The collection, payout, or withdrawal of winnings, as well as the withdrawal of deposited funds or profits derived from placed wagers.

4.4.2. Identification of Linked Transactions

Transactions are deemed linked if they form part of the cumulative activity undertaken by a customer during a single logged-in session on CHM's gambling platform.

This definition is non-exhaustive. Applying a Risk-Based Approach (RBA), CHM continuously monitors for other circumstances indicating linked activity—specifically where a customer intentionally fragments or spreads wagers, deposits, or withdrawals across multiple smaller transactions to evade CDD or EDD thresholds (structuring).

4.4.3. Verification Framework

Upon reaching or anticipating the EUR 2,200 threshold through single or cumulative transactions, CHM immediately enforces risk-based verification procedures in line with its overall AML/CFT framework.

4.5. Ongoing monitoring

4.5.1. Scope & Objectives

Ongoing monitoring is a core component of CHM's Customer Due Diligence (CDD) framework. The objective is to ensure that customer activity remains consistent with CHM's knowledge of the player, their risk profile, and their source of funds.

4.5.2. Core Monitoring Activities

Ongoing monitoring consists of the following key controls:

- **Transaction & Behavior Monitoring:** Continuously evaluating transaction activity (deposits, wagering, and withdrawals) to ensure it aligns with the customer's known financial profile, assets, and source of funds/wealth.
- **Document Maintenance:** Re-verifying identity when previously submitted identification documents expire, prioritized according to customer risk levels.
- **Inconsistency Resolution:** Investigating and resolving any discrepancies or sudden changes identified in customer information, payment methods, or account activity.
- **Risk-Sensitive Profile Updates:** Reviewing and updating Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) profiles at intervals determined by the customer's assigned risk category.

4.5.3. Review Intervals & Trigger Events

Customer profiles are updated based on a combination of periodic intervals and event-driven triggers:

- **Periodic Reviews:** High-risk customer profiles and associated CDD/EDD documentation are reviewed at least every 6 months, while standard-risk profiles are reviewed on a periodic, risk-weighted schedule.
- **Trigger Event Reviews:** An immediate CDD update is conducted regardless of schedule if:
 - An existing identification or verification document expires.
 - Unusual, complex, or suspicious transaction patterns emerge.
 - Information surfaces indicating a change in PEP or Sanctions status.
 - Discrepancies are flagged during automated or manual account reviews.

4.6. Enhanced Due Diligence

4.6.1. Purpose & Overview

To mitigate elevated Money Laundering and Terrorist Financing (ML/TF) risks, CHM applies Enhanced Customer Due Diligence (EDD) measures and enhanced ongoing monitoring in addition to standard Customer Due Diligence (CDD) procedures.

4.6.2. High-Risk Triggers for EDD

EDD measures must be applied in any of the following circumstances:

- **High-Risk Classification:** Cases identified as high risk by CHM's internal risk assessment or based on guidance/typologies issued by relevant regulatory authorities.

- **Data Inconsistency or Doubt:** Situations where CHM has doubts regarding the veracity, accuracy, or currency of previously collected customer identification data.
- **PEP Involvement:** Where a customer or potential customer is identified as a Politically Exposed Person (PEP), or a Family Member or Close Associate (RCA) of a PEP. EDD in such cases serves to confirm status; a confirmed PEP is rejected or closed outright (see clauses 3.4.1 and 4.7).
- **False or Fraudulent Information:** Cases where a customer has provided false, misleading, or stolen identification documents or information, and CHM exceptionally considers continuing the business relationship following risk evaluation.
- **Unusual or Complex Activity:** Any transaction that is complex, unusually large, exhibits an abnormal pattern, or lacks an apparent economic or lawful purpose.
- **Payment Mismatches:** Circumstances where a customer requests the payout of winnings to a payment account different from the account used to make deposits/wagers., please refer to Section 3.7.1
- **General Elevated Risk:** Any other scenario that, by its nature or context, presents a heightened ML/TF risk.

4.6.3. Governance and Approval Requirements

Establishing or continuing a business relationship with a customer categorized as high-risk—whether at onboarding or due to a subsequent status change—requires prior formal approval from the Compliance Officer / MLRO.

4.6.4. Key Definitions: Source of Funds vs. Source of Wealth

To ensure full transparency of payment flows, the origin and destination of money used in all transactions must be traceable to a verified account.

- **Source of Funds (SoF):** Refers to the origin of the specific funds being used to deposit or transact on CHM's platform. SoF verification goes beyond identifying the remitting financial institution; it must establish the substantive origin and circumstances under which those specific funds were acquired.
- **Source of Wealth (SoW):** Refers to the origin of the customer's entire body of wealth (i.e., total net worth/assets). Verification must provide a complete picture of how the customer accumulated their overall wealth over time.

4.6.5. Mandatory EDD Measures

When an account is subjected to EDD, CHM performs tailored risk-mitigation measures, which may include:

- **Re-Verification of Identity:** Re-performing CDD checks to ensure all personal data and documentation are current.
- **SoF & SoW Verification:** Obtaining independent, reliable documentation to confirm that the customer's funds and wealth originate from legitimate sources.
- **Non-Anonymous Payment Controls:** Verifying that all deposits originate from traceable payment methods owned by the customer (e.g., via bank statements or official account statements) to eliminate payment anonymity.
- **Enhanced Ongoing Monitoring:** Increasing the frequency, depth, and scrutiny of ongoing account monitoring and transaction reviews.
- **Transaction Investigation:** Formal examination of suspicious or unusual transaction patterns to determine underlying risk and evaluate whether a Suspicious Activity Report (SAR) must be filed.

4.6.6. Acceptable Source of Wealth (SoW) Documentation

Wealth Category	Acceptable Verification Documents
Salary / Employment Income	Certified payslips, certified employer letter, or audited financial accounts (if self-employed).
Financial Investments	Certified share/investment sale contracts, official investment statements, or a formal letter from a certified accountant.
Property Sale	Certified copy of the contract of sale, or an official letter from a solicitor/estate agent confirming transaction details.
Inheritance	Certified copy of the grant of probate/will showing the distribution value, alongside proof of receipt.
Sale of Company	Certified sale agreement, public registry filings, media articles, or a certified letter from an accountant/solicitor.

4.7. Politically Exposed Persons and Sanctions Screening

CHM utilizes automated KYC software tools to screen customers against global Sanctions, PEP, and Watchlist databases. Screening is systematically executed upon the occurrence of specific operational triggers:

- **Withdrawal Requests:** Prior to the approval and execution of any payout request.
- **Cumulative Deposit Thresholds:** Upon a customer reaching or exceeding regulatory deposit thresholds (e.g., EUR 2,200 cumulative deposits).
- **Enhanced Due Diligence (EDD) Triggers:** Whenever an account is escalated for EDD due to high-risk behavioral anomalies, fraud alerts, or adverse media hits.

In case of identifying a PEP, responsible staff will send a report to the CO.

The Compliance Officer will investigate each case to identify positive or false-positive PEP alerts. CHM has the right to request additional documents from the customer for this purpose within the investigation.

If the PEP alert is true-positive, the Compliance Officer will reject registration or close the account and inform 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 organisation.

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.

4.8. Procedure for Account Closure

4.8.1. General Grounds for Closure

CHM may terminate a customer's account for various operational, regulatory, or risk-related reasons, including but not limited to:

- Fraud or cheating
- Bonus abuse
- Allowing third-party access to the account
- Underage gambling
- Safer gambling concerns / Problem gambling
- Abusive behavior toward staff
- Commercial considerations
- Failure to complete Customer Due Diligence (CDD)
- General breaches of the Terms and Conditions

4.8.2. ML/TF-Related Account Closures

This section specifically governs account closures resulting from suspected or confirmed Money Laundering or Terrorist Financing (ML/TF).

Mandatory Relationship Termination: By law, CHM must end the business relationship with any customer suspected or known to be involved in ML/TF, unless formal consent (e.g., Defence Against Money Laundering / DAML) is granted by relevant law enforcement authorities. Even if consent is granted, account closure remains the default precautionary measure.

Strict Prevention of Tipping-Off: Anti-money laundering legislation strictly prohibits informing a customer that they are under suspicion or that a Suspicious Activity Report (SAR) has been submitted. All closure communications must be handled with extreme discretion using standardized, generic phrasing (such as a standard Terms & Conditions breach) to prevent tipping off.

SAR and Consent Considerations: Prior to closing an account subject to ML/TF concerns, the Compliance Officer / MLRO must evaluate whether an SAR must be submitted and if "Appropriate Consent" (DAML) must be formally requested from authorities before taking action on remaining funds or account status.

CDD Failure Mandate: Where CHM is unable to apply or complete mandatory CDD measures when a customer reaches required transaction thresholds, CHM is legally required to immediately halt all transaction activity and terminate the business relationship.

5. Deposit and Withdrawal Management Procedures

5.1. Player Account Balance, Promo Cash & Wagering Framework

5.1.1. Dual-Balance Wallet Structure

Each registered player account maintains a unified cashier interface comprising two distinct balance types:

- **Real Money Balance:** Contains unencumbered player deposits and settled cash winnings. Real money funds are available for withdrawal at any time, subject to standard anti-money laundering controls.
- **Promo Cash (Bonus Balance):** Contains non-cashable promotional funds, bonus matches, or free credits granted by CHM as part of promotional campaigns.

5.1.2. Fund Deduction Priority (Wagering Mechanics)

When a player places a bet, the platform automatically draws from available balances according to a fixed priority hierarchy:

1. **Real Money First:** Wagers are debited from the Real Money Balance prior to utilizing any promotional funds.
2. **Promo Cash Second:** Once real money funds are exhausted, wagers are debited from the Promo Cash Balance.
3. **Winnings Treatment:** Winnings generated from wagers placed with Real Money are credited directly to the Real Money Balance. Winnings from wagers placed using Promo Cash are treated in accordance with the applicable promotional terms, which determine whether and how value derived from promotional funds becomes withdrawable.

5.1.3. Wagering Requirements & Cash Conversion

5.1.3.1. Standard Deposit Turnover (AML Requirement)

To mitigate money laundering and pass-through schemes, all cash deposits carry a mandatory 1x minimum wagering requirement. Deposited funds must be wagered at least once in full across eligible games before a withdrawal can be requested.

5.1.3.2. Promo Cash Wagering Requirements

Promo Cash cannot be withdrawn directly. Value derived from promotional funds becomes withdrawable only in accordance with the wagering requirements attached to the promotion; the specific requirements are published in the applicable promotional terms and the CHM Terms and Conditions.

5.2. Player Deposits

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

Deposits are processed through a centralised, PCI DSS-compliant payments platform through which third-party payment providers are connected. CHM does not hold any credit card data itself.

The transaction is submitted through the platform to the relevant payment provider; on approval, the deposit status is updated and the funds added to the player's balance. Please refer to Section 3.7

5.2.1. Cryptocurrency Risk Management & Screening Policy

5.2.1.1. Payment Processing & Auto-Conversion

CHM processes all cryptocurrency transactions through authorized third-party payment service providers, specifically Naewe and BVNK.

Conversion & Settlement: Incoming customer cryptocurrency deposits are handled and automatically converted into supported fiat or base currencies directly by the payment providers upon transaction processing.

Provider Screening: Prior to conversion and settlement, all cryptocurrency transfers are subject to the compliance and wallet-analytics screening operated by the payment providers.

5.2.1.2. Monitored Risk Categories

Transactions are continuously evaluated and screened against high-risk categories, including but not limited to:

- **Darknet Services & Marketplaces:** Platforms operating on darknet networks to offer or trade illegal goods and services.
- **Illegal Services:** Entities, websites, or resources directly engaged in unlawful commercial operations.
- **Stolen Coins & Tainted Funds:** Assets marked as fraudulent or originating from known protocol hacks, wallet breaches, or thefts.
- **Ransomware & Extortion:** Wallet addresses linked to extortion schemes, malware, ransomware, or blackmail payments.
- **Scams & Fraudulent Operations:** Entities with verified involvement in cryptocurrency scams, phishing, or financial fraud.
- **Mixing & Anonymizing Services:** Obfuscation services (mixers/tumblers) designed to break transaction trails and obscure source of funds.
- **Fraudulent Exchanges:** Virtual asset service providers (VASPs) confirmed to be operating illegally or facilitating money laundering.
- **High-Risk / Low-KYC Exchanges:** Cryptocurrency exchanges operating with non-existent, permissive, or insufficient Customer Due Diligence controls.

5.3. Player Withdrawals

Please refer to Section 3.11.

6. Suspicious Activity Reporting and Unusual Transaction Reporting

6.1. Introduction

Every employee of CHM is obligated to report to the Compliance Officer any knowledge or suspicion of money laundering, terrorist financing, or funds derived from criminal activity used on CHM's platform.

The Compliance Officer will evaluate each internal report to determine whether sufficient grounds for knowledge or suspicion exist. Where such grounds are established, a report must be submitted to the Financial Intelligence Unit – Financiële Inlichtingen Eenheid (hereinafter "FIU" or "FIU Curaçao").

For the purposes of this policy:

- Knowledge means having direct, factual certainty of an event or origin of funds.
- Suspicion means observing unusual or unexpected activity that, upon further review, lacks a clear, logical, or legitimate commercial/financial purpose.

The obligation to report is ongoing. An activity may not seem suspicious initially, but if concern arises or escalates following subsequent inquiries or player interactions, the activity must be treated as reportable.

When assessing a case, the Compliance Officer considers all surrounding circumstances and may request further information from the customer or third parties. The decision to conduct additional inquiries depends on existing player profile data, transaction history, and the feasibility of making such inquiries without compromising confidentiality.

Under Curaçao law, the reporting baseline focuses on an Unusual Transaction (UTR). Statutorily, a reportable transaction is defined as:

Any completed or attempted transaction (or series of connected transactions) conducted by or on behalf of a player, where established objective thresholds are met, or where CHM knows, suspects, or has reasonable grounds to suspect that the funds are linked to money laundering, predicate offenses (such as fraud or identity theft), or terrorist financing.

1. "Unusual" vs. "Suspicious" Distinction

CHM's Duty: Under CGA / NORUT guidance, CHM does not need absolute proof or certainty of crime to file a report; reasonable grounds for suspicion or an indicator match are sufficient.

The FIU's Duty: CHM submits an Unusual Transaction Report (UTR) to FIU Curaçao via the goAML system. It becomes a formal Suspicious Transaction Report (STR) once the FIU analyzes the data and escalates it to law enforcement.

6.1.1. Objective vs. Subjective Indicators

Reports fall into two statutory trigger categories:

Objective Indicators (Mandatory Reporting):

- Any monetary transaction (deposit, payout, or wager) reaching or exceeding the legal reporting threshold (e.g., NAf 5,000 / ~\$2,800 USD).
- Any transaction tied to individuals under active police investigation or international sanction lists.

Subjective Indicators (Discretionary / Pattern-Based):

Transactions where the behaviour, structure, or origin raises a red flag, regardless of the dollar amount.

Key triggers include multi-accounting, shared withdrawal endpoints (proxy emails/bank details), syndicate bonus farming, synthetic identity usage, or depositing/withdrawing without minimal game play.

Attempted Transactions are Included

Under CGA/LOK compliance rules, CHM's Compliance Officer / MLRO is required to document this finding, freeze the accounts/withdrawals concerned, and log a UTR with FIU Curaçao via goAML.

6.2. Red Flags Indicators and Internal Escalation

Red flags do not automatically result in an external report to the FIU; rather, they are indicators that warrant further inquiry into a customer's behavior. If an investigation fails to yield a reasonable commercial or legal explanation for a red flag, an internal report must be submitted to the Compliance Officer.

The following non-exhaustive list of red flags should be monitored and evaluated:

- **CDD/EDD Non-Cooperation:** Customer refuses or fails to provide required documentation during Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) procedures.
- **Multi-Accounting:** Customer attempts to register or operate multiple accounts across the platform.
- **Pass-Through / Minimal Play:** Customer deposits significant funds, engages in minimal or zero wagering, and immediately requests a withdrawal of un-wagered balances.
- **Unexplained Transaction Velocity:** Customer engages in frequent, high-volume deposit and withdrawal requests without a clear gaming rationale.
- **Abnormal Pattern Shifts:** Noticeable, sudden changes in gaming patterns—such as a player executing transaction volumes significantly higher than their established historical baseline.
- **Inter-Account Transfers:** Customer inquires about or attempts to move funds between different accounts within the gaming group.
- **Affordability Discrepancies:** Customer executes transaction volumes that appear disproportionate to their known financial profile, source of wealth, or income.
- **Third-Party Payment Routing:** Customer attempts to withdraw or transfer funds to a bank account or payment method registered under a third party's name.
- **Unverified Payout Endpoints:** Customer requests a withdrawal to a payment method that has not been previously verified or used for deposits.
- **Multiple Payment Method Cycling:** Customer registers multiple credit/debit cards or e-wallets under a single profile and attempts circular funding or rapid switching between them.
- **Irrational Loss Behavior:** Customer repeatedly deposits and loses unusually large sums of money without demonstrating expected player behavior or concern regarding losses.

6.3. Failure to Complete CDD Measures

Where a customer refuses or fails to provide the requested Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) documentation within the specified timeframe, CHM is obligated to restrict the gaming account and suspend or terminate the business relationship.

However, a customer's reluctance or failure to provide CDD/EDD documentation shall not, on its own, be automatically equated to a suspicion of Money Laundering, Terrorist Financing, or Proliferation Financing (ML/TF/PF).

The Compliance Officer will perform a holistic case review using all available data, including:

- Payment methods and funding channels used;
- Gaming behavior, wagering levels, and playing patterns;
- Geographic risk profile and country of residence; and
- Open-source intelligence (OSINT), media searches, and adverse screening results.

If, after evaluating all relevant factors, the Compliance Officer determines that reasonable grounds for suspicion exist, an Unusual Transaction Report (UTR) must be submitted to FIU Curaçao. If no grounds for suspicion exist, the account will remain closed/blocked, and eligible funds will be returned to the player using the original deposit channel where legally permitted.

6.4. Internal Suspicious Activity Report

Every employee has a mandatory duty to immediately report any knowledge, suspicion, or reasonable grounds to suspect money laundering, terrorist financing, or predicate illegal activity. If an employee observes unusual customer behavior or transaction patterns, they must report it to the Compliance Officer without delay using the approved Internal Suspicious Activity Report (iSAR) Form.

6.4.1. Independent Escalation & Non-Interference

An employee is obligated to submit an internal report directly to the Compliance Officer whenever suspicion arises, regardless of whether their supervisor or manager agrees. Line managers, team leads, and department heads do not have the legal authority to suppress, alter, or block an internal disclosure. The ultimate decision to escalate a report externally rests solely with the Compliance Officer.

6.4.2. Contents of an Internal SAR

An Internal SAR must include the following details:

- **Customer Details:** Full name, user/account ID, residency details, and contact information.
- **Reporting Employee Statement:** A clear, factual summary detailing the exact observations, behaviors, or transactions that caused suspicion.
- **Supporting Documentation:** All relevant supporting evidence, including transaction logs, game logs, communication histories, or payment records.

6.4.3. Duties of the Compliance Officer

Upon receiving an Internal SAR, the Compliance Officer will:

1. **Acknowledge Receipt:** Promptly acknowledge receipt of the disclosure to the reporting employee.
2. **Investigate & Evaluate:** Review the report against existing account history, playing patterns, and open-source intelligence to determine if reasonable grounds for suspicion exist.
3. **File External Report (If Warranted):** Submit an official report to FIU Curaçao via the goAML portal if suspicion is substantiated.
4. **Document & Notify:** Record the final decision and rationale in the internal compliance log (whether reported externally or retained internally) and inform Senior Management as required.

6.5. External report to FIU

Upon receipt of an Internal SAR, the Compliance Officer is responsible for determining whether the matter warrants an external disclosure to FIU Curaçao.

In evaluating the case, the Compliance Officer applies a Risk-Based Approach (RBA), recognizing that AML/CFT legislation targets serious financial crime involving material financial exposure or intentional attempts to circumvent regulatory safeguards. Isolated, low-value events (such as individual chargebacks or single promo violations) generally do not trigger external reporting duties unless they result in illicit proceeds being deposited or held on the platform. However, the Compliance Officer must evaluate whether such individual instances form part of a broader, systematic scheme or syndicate pattern.

6.5.1. Link Analysis & Pattern Identification

To assess whether reasonable grounds for suspicion exist, the Compliance Officer evaluates all available data to identify common denominators across multiple accounts or transactions. Indicators of organized or systematic activity include, but are not limited to:

- Shared or overlapping IP addresses and device fingerprints;
- Identical bank accounts, e-wallet emails, or withdrawal endpoints;
- Related personal credentials, physical addresses, or contact details; and
- Repeated, synchronized transaction behaviors across multiple profiles.

6.5.2. SAR / UTR Filing Evaluation Checklist

To complete the external reporting evaluation, the Compliance Officer must document the following key facts:

- **Who:** Full identity details of all involved parties and their relationships to the accounts.
- **How:** The specific mechanism, payment channels, and gameplay used to carry out the activity.
- **What:** The exact nature, location, and estimated value of the suspected criminal or terrorist property.
- **When:** The precise timeframe of past occurrences and any indicator of upcoming or planned activity.

6.6. Reporting Procedure

CHM is obliged to submit a suspicious activity report or Unusual Transaction Report to the FIU, through the user interfaces (goAML) on the FIU's website, without due delay if there are indications that:

- CHM 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 CHM 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.

CHM 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, CHM submits SAR immediately.

6.7. Tipping off

6.7.1. Prohibition of Tipping off

It is a serious criminal offence to disclose to a customer or any unauthorized third party that an Internal SAR or external report to FIU Curaçao has been filed, is being prepared, or is under active consideration, where such disclosure is likely to prejudice an investigation. This principle is strictly known as the Prohibition of Tipping Off.

While internal discussions among relevant personnel (such as Operations, Risk, and Compliance) are permitted on a strict need-to-know basis, no employee may—directly or indirectly—alert the customer or their associates that they are under review or law enforcement scrutiny.

To prevent tipping off, no CHM employee shall:

- **Attribute Delays to Regulatory Authorities:** Inform a customer that a deposit, withdrawal, or account review is delayed because CHM is awaiting FIU consent, instructions, or clearance.
- **Disclose Active Investigations:** Inform a customer that law enforcement, FIU Curaçao, or regulatory authorities are conducting an investigation into their account or funds.
- **Use Compliance Terminology:** Mention internal compliance forms, SARs/UTRs, goAML, or money laundering inquiries during customer interactions.

All customer communications regarding delayed withdrawals or account blocks must utilize standardized, neutral operational phrasing.

7. Internal Control

7.1. Introduction

CHM 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

CHM 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.)

CHM 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 money laundering 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.

CHM destroys all the documents and data collected after retention period expiration unless other recordkeeping or retention obligations apply, but not later than after 10 years.

7.3. Money Laundering Reporting Officer

CHM has appointed a 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 Compliance Officer is the main contact point for the FIU.

In order to ensure that the Compliance Officer is able to fulfill their role effectively, CHM guarantee that:

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

The Compliance Officer carries 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 CHM'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 Compliance Officer activities on the risk situation of CHM and the measures taken and intended to implement the obligations under money laundering regulations.

The Compliance Officer is authorized, within the scope of the 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.

Questions regarding this Policy, and all internal reports under it, are directed to the Compliance Officer.

7.4. Training

CHM will give training to all staff directly or indirectly through a service provider upon joining CHM and after that annually. Please refer to Section 1.6.

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

Training will be conducted as follows:

- Training material based on the finalised and approved policies CHM 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 CHM find that some issues are not clear, CHM 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,
- CHM's policies and procedures to prevent money laundering and the financing of terrorism,
- CHM'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 CHM'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 CHM
- Data protection regulations.

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 CHM's policies and procedures and any changes or improvements made.

The Money laundering 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 CHM's policies and procedures or applicable legislation, all staff will get the relevant training.

7.5. Employees background check

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

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

- a valid original identity document,
- CV,
- any other documents as CHM deems necessary to request.

Once a person is employed, screening shall still be carried out on an ongoing basis as required. All CHM'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 CHM feels the need to perform such inspections. In particular, such inspections shall be carried out when suspicion arises concerning the behaviour of specific employees. CHM 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.

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

7.6. Internal and external revision and staying up to date

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

- Key personnel have subscribed to mailing lists offered by the FIU, GCB and FATF and joined relevant forums
- CHM periodically takes legal advice from gambling consultants for AML best practices
- In the case of an update, CHM will take the following steps, as necessary:
 - Update CHM'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.

CHM may engage a third-party service provider with expertise in AML compliance to conduct independent external reviews of CHM's AML policies and procedures. The results of these reviews will be reported to the senior management and used to enhance CHM's AML/CTF measures and documents as needed. The frequency of external reviews is determined by senior management. It may be conducted annually or more frequently, depending on the need for an updated assessment of CHM's AML program's effectiveness.

This Policy is reviewed within one year of its effective date or of any major revision, and at least once every three years thereafter, or sooner where regulatory change requires it.

Appendix 1

- Afghanistan
- Aland Islands
- American Samoa
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Barbados
- Belize
- Benin
- Bhutan
- Bonaire (including Sint Eustatius and Saba)

- Bouvet Island
- British Indian Ocean Territory
- Burundi
- Cape Verde
- Central African Republic
- Chad
- Cocos (Keeling) Islands
- Cook Islands
- Comoros
- Congo, Democratic Republic of
- Congo, Republic of
- Crimea
- Cuba
- Curacao
- Djibouti
- Donbas
- Equatorial Guinea
- Eritrea
- Fiji
- French Guyana
- French Polynesia
- French Southern Territories
- Gabon
- Gambia
- Grenada
- Guadeloupe
- Guam
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Holy See (Vatican City State)
- Iran
- Iraq
- Ivory Coast (Côte d'Ivoire)
- Kherson
- Kiribati
- Kosovo
- Kyrgyzstan
- Lao People's Democratic Republic
- Lebanon
- Liberia
- Libya
- Macao
- Malawi
- Mali

- Marshall Islands
- Martinique
- Mauritania
- Mayotte
- Micronesia, Federated States of
- Montserrat
- Myanmar
- Nauru
- New Caledonia
- Niger
- Niue
- Norfolk Island
- North Korea
- Northern Mariana Islands
- Palau
- Palestinian Territory
- Papua New Guinea
- Pitcairn
- Puerto Rico
- Rwanda
- Saint Barthelemy
- Saint Helena
- Saint Kitts and Nevis
- Saint Lucia
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Sao Tome E Principe
- Seychelles
- Sint Maarten
- Sierra Leone
- Solomon Islands
- Somalia
- South Georgia and the South Sandwich Islands
- Sudan (North and South)
- Suriname
- Svalbard and Jan Mayen
- Syria
- Tajikistan
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- United States of America

- United States Minor Outlying Islands
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Venezuela
- Wallis and Futuna
- Western Sahara
- Western Samoa
- Yemen
- Zaporizhzhia
- Zimbabwe