

Thot Management N.V.

Anti-Money Laundering, Counter-Terrorism
Financing and Counter-Proliferation Financing
Policy

Version 3.1

1.	<i>Policy Statement</i>	5
2.	<i>Purpose</i>	5
3.	<i>Audience</i>	6
4.	<i>Definitions</i>	6
5.	<i>Policy Implementation</i>	8
5.1.	Business Risk Assessment	8
5.2.	Customer Risk Assessment.....	9
5.3.	Customer Acceptance Policy	11
5.3.1.	Step 1: Customer Registration	11
5.3.2.	Step 2: Submission of Documents & Verification	12
5.3.3.	Step 3: Age Verification.....	13
5.3.4.	Step 4: Geolocation Check	13
5.3.5.	Step 5: Approval or Rejection of verification.....	14
5.4.	Customer Due Diligence	15
5.4.1.	Sanctions Screening Obligations and Process.....	15
5.4.2.	Enhanced Due Diligence	16
5.4.3.	Timeline for Submitting CDD Documents and Consequences of Non-Compliance	16
5.5.	Ongoing Monitoring	17
5.5.1.	Fraud Mitigation.....	17
5.5.2.	NearLine Triggers.....	18
5.5.3.	High to low value split ticket monitoring	18
5.5.4.	Low value to high split ticket monitoring.....	18
5.5.5.	Monitoring of Expired Card Response	18
5.5.6.	Variance Checks	19
5.5.7.	Velocity Controls	19
5.5.7.1.	IP Address Checks	19
5.5.7.2.	Transactions Coming from Proxy IPs	19
5.5.7.3.	Transactional Checks	19
5.5.7.4.	Physical Address Check	20
5.5.7.5.	E-mail Address Check	20
5.5.8.	Offline Triggers	20
5.5.8.1.	Decline Reason Codes Monitoring	20

5.5.8.2.	Chargebacks Reason codes	20
5.5.8.3.	BIN Analysis.....	20
5.5.8.4.	Activity on Dormant Client Accounts	21
5.5.8.5.	SAFE and TC40	21
5.5.9.	Review and Auditing	21
5.6.	Reliance on third parties to perform customer due diligence.....	21
5.7.	Reporting of unusual transactions	22
5.7.1.	Recognizing Unusual Transactions.....	22
5.7.2.	UTR filing process:.....	23
5.7.3.	Record Keeping and Retention	23
	Termination of Business Relationship	23
5.8.....		23
5.8.1.	Termination of Player Accounts.....	23
5.8.2.	Termination of Providers and Third Parties.....	24
5.9.	Anti-Money Laundering Compliance program	24
5.9.1.	Appointment of a Compliance Officer	24
5.9.2.	Employee Screening	25
5.9.3.	Employee Training.....	25
5.9.4.	Independent Audit Function	26
5.9.5.	Examination by the Curaçao Gaming Authority	26
6.	Compliance and Consequences of Non-Compliance	26
	Contact Information.....	27
7.....		27
8.	Policy History.....	27

Key Information

Approving Official(s)	e-Management N.V.
Responsible Office	Compliance & Risk Management Teams
Effective Date	Revision Effective since January 6, 2025
Next Review Date	Next Scheduled review January 4, 2028

Approval

Date: October 29, 2025

Name: e-Management N.V.

Signature:



1. Policy Statement

Thot Management N.V. (hereinafter the “Company”), is licensed and regulated by Curaçao Gaming Authority (CGA) to offer remote (online) games of chance, under License No. OGL/2024/1132/0522. In accordance with applicable legislation and its license conditions, the Company has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (hereinafter “AML, CTF and CPF”) policy.

This document outlines current internal practices related to our KYC policies and their alignment with the regulations as well as providing a summary on our practices for protecting our gambling platform from fraudulent activity and general risk, money laundering and problem gambling. This is achieved using a number of automated systems as well as having operational teams that evaluate and monitor all transactional data and Customer registrations to ensure our platform only provides services to verified and eligible individuals.

2. Purpose

The information provided below applies to all Customers who register / participate in gambling activity that is offered by our platform. The document covers the collection, verification and storage of identification data as well as outlining internal processes and reporting that allows the monitoring and actioning of suspicious or malicious activity.

The objectives of this document:

- Ensuring compliance with applicable laws and regulations related to customer verification.
- Mitigating risks associated with fraud, money laundering, and gambling addiction.
- Providing a secure and transparent environment for customers.
- Ensuring that the gambling platform only offers services to verified and eligible individuals.

The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

3. Audience

The policies and processes outlined are intended and applicable to all employees, associates, contractors, subcontractors and 3rd party vendors and suppliers.

4. Definitions

- I. **Money Laundering:** generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the 'placement' stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions. At the 'layering' stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the 'integration' stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.
- II. **Terrorism Financing:** refers to the provision of funds or financial support for terrorist acts, individuals, or organizations, and is characterized by the intent to intimidate populations or compel governments and international bodies to act or refrain from acting. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.
- III. **Proliferation Financing:** the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.
- IV. **KYC:** The process by which a business verifies the identity of its customers. This process is critical for ensuring compliance with legal and regulatory standards, particularly with respect to anti-money laundering (AML) regulations.
- V. **AML:** A set of laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income. These regulations are designed to detect and report suspicious financial activities, ensuring that businesses and financial institutions do not inadvertently facilitate money laundering or terrorist financing.
- VI. **ID Verification:** The process of confirming a customer's identity using official documents, such as a government-issued ID, passport, or driver's license. ID verification is a key component of KYC and helps ensure the individual is who they claim to be.

- VII. **POI:** A document or combination of documents used to verify a customer's identity. This typically includes government-issued photo IDs such as a passport, national ID card, or driver's license. POI is required as part of the KYC process.
- VIII. **POA:** A document or combination of documents that verify a customer's residential address. Common examples include utility bills, bank statements, or official government correspondence. POA is required in the KYC process to ensure the customer's address matches the information provided.
- IX. **CDD:** A standard process of verifying the identity of customers and assessing the potential risk they may pose. CDD typically involves collecting basic personal information, such as name, address, and date of birth, along with documentation to confirm their identity (POI) and address (POA). CDD is a mandatory step in the KYC process for all customers.
- X. **EDD:** A deeper investigation that is conducted for customers considered to be higher risk, such as politically exposed persons (PEPs), those from high-risk jurisdictions, or those with complex financial backgrounds. EDD involves additional steps such as obtaining more documentation, conducting thorough background checks, and monitoring transactions for suspicious activity.
- XI. **PEP (Politically Exposed Person):** Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, and the direct family members or close associates of such persons. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions, and the direct family members or close associates of such persons.
- XII. **PAN:** The Primary Account Number (PAN) is the full account number used in payment card transactions (credit, debit, prepaid cards, etc). It consists of up to 16 digits and is divided into several parts that contains different information about the card and the cardholder.
- XIII. **TC40 File:** Contains data on fraud-related chargebacks, including chargeback reason codes, fraud detection, and transaction details.
- XIV. **SAFE File:** Contains data regarding transactions, chargebacks, and compliance information specifically tied to **VISA** and **MasterCard** standards
- XV. **UTR:** Unusual Transaction Report is a report submitted to the Financial Intelligence Unit of Curaçao based on a transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.

- XVI. **UBO (Ultimate Beneficial Owner):** Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

5. Policy Implementation

Policy implementation is done company-wide through individual and departmental training, ongoing quality review and operational level scorecard evaluation – this done on a monthly, quarterly and annual basis focused on individual and line of business adherence to policies.

5.1. Business Risk Assessment

The company acknowledges the inherent risks associated with its line of business, particularly in the context of online gambling. Recognizing these risks is vital to ensuring the platform operates within the required regulatory framework and provides a secure, compliant, and fair environment for its users. The identification of these risks and the implementation of effective mitigation measures and processes are essential to minimize exposure to various threats.

5.1.1. Financial Risks

Risk: Fraud and Financial Crimes (Money Laundering, Terrorist Financing) Mitigation

Measures:

- We have in place robust KYC processes and procedures as well as quality control to ensure all Customers are verified
- Financial transactions are monitored in real time, allowing us to detect and take action on unusual activity or patterns that are outside of normal or usual Customer behavior
- All registrations are screened for AML databases, including PEP, sanctions lists and other high risk entities
- Enhanced due diligence is completed on Customers who display high risk or suspicious activity
- We have in place a number of anti-fraud technologies, machine learning tools as well as people resources to help prevent, review and take action on unauthorized, high risk and suspected fraud in real time to help protect our Customer and platform.

5.1.2. Compliance and Regulatory Risks

Risk: Non-compliance with Regulatory Requirements

- **Mitigation Measures:**
 - We have stringent data protection policies and systems in place to ensure Customer and overall platform security
 - Our internal compliance team remains up to date and updates, as needed, internal policies and processes as well as communicate change as appropriate to the affected teams within the organization.
 - Internal compliance group complete mandatory audits and ensure required training of staff on the legal and regulations as needed

- Regularly audit internal processes to ensure compliance with all relevant **gambling licenses** and regulatory standards.

5.1.3. Fraud Risks

Risk: Identity Fraud or Account Takeover

- **Mitigation Measures:**
 - 2FA is a process that is completed at different stages of an account, at log in, withdrawal as well as notification when an unknown device is identified at the login
 - Usual behavior, at sign in and transaction stage are reviewed and monitored, including reporting and reviews of account changes to mitigate account takeover fraud
 - Regularly update and strengthen the **identity verification** process to reduce the possibility of fraudulent account creation or account takeover.

5.2. Customer Risk Assessment

To ensure that customers are properly identified and comply with regulatory requirements, the platform requires the submission of an appropriate photo ID during the KYC (Know Your Customer) process. Below are the guidelines and procedures for submitting valid identification documents, as well as the steps taken to verify their authenticity.

1. Accepted Identification Documents

For the identification of person, customers must provide one or more of the following government-issued documents:

- **Passport**
 - A valid passport that clearly displays the customer's photo, full name, and date of birth.
- **National Identity Card**
 - A national identity card issued by the customer's home country, containing the customer's name, photo, and date of birth.
- **Driver's License**
 - A driver's license issued by a recognized authority, which must display the customer's photo, name, address, and date of birth.
- **Residence Card**
 - A residence card for foreign nationals or residents issued by the government, which includes the customer's name, photo, and date of birth.

The document must follow the below guidelines:

For the identification documents to be accepted and processed, they must meet the following criteria:

- **Clear, Legible, and Durable**
 - The document must be **clear**, legible, and durable in nature. It should be scanned or photographed in full colour to ensure that all details are visible.
- **Full Image Submission** ○ A photo or scan of the entire document is required.
For documents that have two sides (e.g., driver's licenses or ID cards), both sides must be submitted.
 - The image must not be cropped, and all information, including edges, must be visible.
- **Date of Birth**
 - The date of birth must be clearly visible on the document, as it is crucial for verifying the customer's eligibility (e.g., to ensure they are of legal gambling age).
- **Valid Document**
 - The document must be valid and in-date. Expired identification documents will not be accepted.
- **Temporary Work Permits and Paper ID Cards** ○ Temporary work permits or paper ID cards are generally not accepted as valid forms of photo identification. These types of documents are often seen as less secure or prone to manipulation.

Temporary work permits or paper ID cards are generally not accepted as forms of photo identification.

Identity documents are fed to a 3rd party provider (Acuitytec) which will verify the validity and legitimacy of such documents against known templates using optical character recognition software and checks for security features and evidence of tampering.

In cases where the software solution cannot make an appropriate assessment or identifies issues with the submitted documents, the document will be escalated for manual review by a team of trained human agents. This process ensures that the verification remains accurate, thorough, and compliant with regulatory standards.

- Bank/Credit Card Statement
- Utility Bill
- Correspondence by central or local Government authorities, departments or agencies

To ensure the document is valid for residential address verification, it must meet the following criteria:

- **Clear and Legible**
 - The document must be clear, readable, and free from any blurriness or distortions.
 - Ideally, the document should be in colour, although black-and-white copies may be acceptable as long as the details are legible.
- **Full Document/Scan Submission**

- Customers must submit a photo or scan of the entire document, ensuring that all details (name, address, and date) are visible.
- Sensitive information, such as account numbers, should be covered or blacked out for security and privacy purposes. However, the name and address should remain visible and clear.
- **Document Date**
 - The document must be dated within the last 3 months (90 days) from the day it is submitted. This ensures the address is current and accurate.
- **Full Name and Address**
 - The document must clearly state the customer's full name and residential address. These details should match the information provided by the customer during registration.

In cases where the residential address provided by the customer differs from the address listed on their photo ID (if applicable), additional documentation may be required. Customers will be asked to provide supporting documentation to clarify the discrepancy.

Possible supporting documents include:

- **Residency Card**
 - A residency card showing the customer's legal residence in the country of the address.
- **Work Permit**
 - A work permit or other official government-issued document that confirms the customer's legal residency in the country specified on the address.
- **Additional Proof of Address**
 - Another utility bill or official correspondence showing the customer's name and new residential address, if the original documents do not align.

5.3. Customer Acceptance Policy

The following section outlines the step-by-step procedure a user must follow during onboarding in order to be eligible to make a deposit.

5.3.1. Step 1: Customer Registration

Upon registering for an account on the platform, customers will be required to provide the following basic information. This information is essential to verify the customer's identity and ensure compliance with legal and regulatory requirements such as age restrictions, anti-money laundering (AML) rules, and responsible gambling policies.

1. Required Customer Information

Full Name

- The customer must provide their legal full name as it appears on official documentation (e.g., passport, national ID, or driver's license). This will be used to verify their identity against submitted documents during the KYC process.

Date of Birth

- The customer must enter their date of birth to confirm they are of legal gambling age (typically 18 or 21 years of age, depending on the jurisdiction). This information is critical to comply with age restrictions and prevent underage gambling.

Residential Address

- The customer will need to provide a residential address. This will be used for Proof of Address (POA) during the KYC verification. The address must be valid, and the customer may be required to submit documentation (e.g., a utility bill, bank statement) to verify this address.

Email Address

- A valid email address is required to facilitate account communication, including verification emails, system notifications, and promotional offers. It will also be used for password recovery and security alerts.

Phone Number

- A valid phone number is required to enhance communication and support. It may be used for multi-factor authentication (MFA), account recovery, or to send notifications and updates about account activity.

5.3.2. Step 2: Submission of Documents & Verification

The KYC team plays a crucial role in ensuring the authenticity and validity of documents provided by customers. To prevent fraud and ensure compliance with regulatory standards, a thorough verification process is implemented. Below is the detailed process for handling and verifying the documents submitted by the customer:

1. Document Submission by Customer

- The customer submits the necessary documents, such as Proof of Identity (POI) and Proof of Address (POA), as part of the KYC process.
- Documents may include government-issued IDs, utility bills, bank statements, or other official documents that verify the customer's identity and address.

2. Document Authenticity Verification by KYC Team

1: Initial Document Review

- I. The KYC team begins by reviewing the documents to ensure they are legitimate, clear, and meet the platform's verification requirements.
- II. They will check for standard indicators of authenticity, such as security features on ID cards or government-issued documents (e.g., watermarks, holograms).

2: Document Inspection for Completeness

- I. The KYC team ensures that all necessary fields in the documents are clearly visible and complete (e.g., name, date of birth, address, and expiration dates).
- II. Missing or incomplete details may result in a request for additional documentation.

3: Document Validation

- I. The KYC team will verify that the documents match the information provided by the customer during the registration process (e.g., comparing the name, address, and date of birth).
- II. If the document type is not in the expected format or contains unusual details, the team may ask the customer to resubmit the document.

5.3.3. Step 3: Age Verification

To ensure compliance with age restrictions and prevent underage gambling, the platform will implement a robust **age verification process**. This is critical to adhere to legal requirements and to provide a responsible gambling environment.

- *Step 1: Date of Birth Submission*
 - During the registration process, customers will be required to provide their date of birth. This will be used to verify that they meet the legal age requirement for online gambling, which typically ranges between 18 and 21 years of age, depending on the jurisdiction.
- *Step 2: Age Validation*
 - The platform will validate the provided date of birth using automated checks to ensure that the customer is of legal gambling age. The system will compare the date of birth against the platform's minimum age requirement, which will be set according to the relevant jurisdiction in which the customer resides.
 - If the customer's age is verified and meets the legal gambling age, they will be allowed to continue the registration process and access gambling activities.

5.3.4. Step 4: Geolocation Check

To ensure the platform adheres to the legal requirements of various jurisdictions, a geolocation check will be performed on customers before they can access gambling services. This process is critical for ensuring that users are located in regions where online gambling is permitted, in line with local laws and regulations.

- Upon registration or login, customers will be required to allow the platform to detect their IP address.
- The system will automatically cross-check the IP address against a database of allowed regions where online gambling is legal.
- If the IP address is from a region where online gambling is prohibited, the customer will be unable to proceed with registration or gambling activities.

5.3.5. Step 5: Approval or Rejection of verification

Approval Process

- *Step 1: Successful Verification*
 - Once all required documents (e.g., proof of identification, proof of address) have been successfully verified and the information matches the registration details, the account will be marked as fully verified.
- *Step 2: Customer Notification*
 - The customer will be notified of the successful verification via email and/or SMS.
 - The notification will include a confirmation that their account is now fully verified and they are cleared to proceed with gambling activities, including deposits, withdrawals, and placing bets.

Rejection Process

- *Step 1: Verification Failure*
 - If any of the submitted documents or information are found to be incomplete, invalid, or fraudulent, the customer's account will be temporarily suspended.
 - Suspended accounts will not be able to engage in gambling activities (e.g., no deposits, withdrawals, or placing bets) until the issues are resolved.
- *Step 2: Customer Notification*
 - The customer will be notified via email that their account has been suspended due to issues with the verification process.
 - The email will clearly explain the reason for the suspension (e.g., missing or invalid documents, fraudulent information).
 - The customer will be provided with instructions to correct or submit additional documentation to resolve the issue.
 - The email will also include a deadline or timeframe within which the customer should provide the required documentation to lift the suspension.
- *Step 3: Opportunity for Resolution*
 - The customer will be given an opportunity to upload additional or corrected documentation via their account dashboard or by responding to the support team.
 - If the customer fails to provide the required documents or resolve the issue within the stipulated timeframe, further actions may be taken, including permanent account closure.
- *Step 4: On going Monitoring*
 - After initial verification, the platform may periodically monitor or recheck customer accounts for continued compliance with the platform's KYC policies.
 - In high-risk scenarios, accounts may undergo Enhanced Due Diligence (EDD) to ensure ongoing compliance.

5.4. Customer Due Diligence

The company uses the service offered by Acuitytec & Compliance Advance to search and monitor for PEPs and sanctioned applicants

Once the system has obtained at least one reliable identification document, a number of fields will be fed to the Acuitytec software. Onboarding will proceed if the software does not return any match, otherwise the client will not be allowed to access the account and the platform until further verification is completed, which requires a manual review. In such cases, the results by Acuitytec will be analysed to verify if the match is a true match or a false positive.

In case of a false positive, onboarding will proceed as normal. If the match is a true, the customer will be asked to complete EDD or will be denied onboarding, depending on which category has triggered the true match, and to which extent. Depending on the result of the Acuitytec software check, there may be additional restriction applied to the account.

Any true matches for PEPs or users who are adjudged to be High Risk will require the user to complete Enhanced Due Diligence in addition to the above-mentioned requirements for Identity and Address verification. EDD measures are detailed appropriately in a forthcoming section.

5.4.1. Sanctions Screening Obligations and Process

All customers, counterparties, and payment service providers are screened against relevant sanctions lists, including but not limited to:

- United Nations Security Council Sanctions Lists;
- European Union Consolidated Sanctions List;
- OFAC Sanctions List; and
- Lists issued under Curaçao's Sanctions National Ordinance and Kingdom Sanction Law.

Screening occurs:

- During initial onboarding and registration;
- Prior to each withdrawal or payment transaction;
- Whenever customer details are updated; and
- As part of periodic ongoing monitoring.

If a sanctions match or potential match is detected, the customer's account must be **immediately frozen**. The Compliance Officer must be informed without delay. The Compliance Officer will verify the match using secondary sources and, if confirmed, will submit a report to the FIU Curaçao within forty-eight (48) hours and notify the relevant authorities under the Sanctions National Ordinance.

5.4.2. Enhanced Due Diligence

Enhanced Due Diligence is carried out when appropriate and requires further verification of and typically additional information, to help corroborate the provided data / documents with additional proof. This process allows for additional collection and verification of Customer data and is triggered for a number of different and unique events, including but not limited to:

- Users identified as PEPs
- Users identified as High-Risk after a review of their documentation
- Users exhibiting suspicious activity patterns
- User with high value transactions (Payout/Deposit)
- Users asking for account updates (Data changes, limit updates)
- Users exceeding \$5,000 in payouts / deposits exceeding \$25,000

The ongoing monitoring at the sign up stage, transactional stage and behavior stage may identify and trigger the required EDD process, requiring a Customer to provide additional information regarding:

- Employment Status
- Source of Funds & Wealth
- Targeted probing related to gambling activities

Additional documentation is required to confirm residential address, government issued ID with “Selfie” to prove liveness or other documentation as needed. An account pending further verification is temporarily restricted pending submission of requested information and full verification is completed.

Addition checks may be completed using third party services to further enhance the verification of a Customer and to conclude the investigation.

5.4.3. Timeline for Submitting CDD Documents and Consequences of Non-Compliance

Under the National Ordinance on Identification when Rendering Services (NOIS), the Company must identify and verify customers before or during the establishment of the business relationship.

When a customer reaches a cumulative transaction threshold of Cg. 4,000 or requests a withdrawal, full Customer Due Diligence (CDD) verification must be completed within thirty (30) calendar days.

Procedures and Deadlines:

- The customer is notified immediately upon reaching the Cg. 4,000 threshold and requested to submit verification documents.
- Pending verification, the customer may continue gameplay but cannot deposit or withdraw additional funds.
- If the documents are not provided or are deemed invalid within thirty (30) days:
 - The account will be suspended;
 - Remaining balances may be held pending review; and
 - The case will be escalated to the Compliance Officer to assess whether a UTR must be filed with the FIU Curaçao.

5.5. Ongoing Monitoring

After the initial KYC verification, the platform will implement a continuous monitoring system to ensure that all customer activities remain compliant with relevant laws and regulations. This section outlines the procedures for monitoring customer accounts and the need for periodic re-verification. This is an essential component of the platform's Anti-Money Laundering (AML) and fraud prevention strategies.

The platform will establish a comprehensive monitoring process to track customer transactions and activities. This will include, but not be limited to, the following:

- **Transaction Monitoring:** All customer transactions will be monitored for unusual or suspicious activity. Automated systems will analyze transaction patterns to identify red flags such as:
 - Large or frequent transactions inconsistent with the customer's usual behavior.
 - Transactions involving high-risk jurisdictions or entities.
 - Any actions that trigger alerts under AML guidelines.
- **Behavioral Monitoring:** In addition to transactions, the platform will monitor customer behavior across the system. This may include account access patterns, login locations, and usage of specific platform features.
- **Real-time Alerts:** The platform will implement a real-time alert system that flags transactions or activities requiring further investigation. Alerts will be based on predefined risk parameters and thresholds.
- **Risk Scoring:** Each customer will be assigned a risk score based on various factors, including transaction history, geographic location, and account activity. Higher risk scores will trigger more frequent or in-depth reviews.

5.5.1. Fraud Mitigation

This type of risk primarily, though not exclusively, pertains to the processing of transactions that may lead to fraud, chargebacks, or refunds. The platform is committed to mitigating these risks by implementing a series of real-time rules and velocity checks designed to provide greater assurance regarding cardholder activity. These measures aim to reduce potential losses and enhance the platform's ability to identify and respond to suspicious transactions, particularly over the long term.

Below are a set of rules that have been implemented or are still in the process of being implemented:

- Count of credit/debit cards used to transact within specific periods
- High frequency and out of pattern transaction monitoring
- Failed/declined transaction review
- BIN and credit card velocity flags
- Maximum Per transaction and account cumulative amounts, with preset account and card limits – optional customer support available to adjust, with additional due diligence requirements
- Maximum transactions per day, week and month
- Dormant account activity alerts (90 days)
- Geo location fencing with geo variance review

- Linked / duplicate account algorithms using IP and device data, registration information and other parameters
- Transactional scrubbing, comparing provided information with card country, registration information and geo location

5.5.2. NearLine Triggers

Nearline triggers are a set of automated monitoring actions designed to detect and respond to suspicious or anomalous behavior on the platform that may not immediately qualify as high-risk but requires further attention. These triggers are typically based on patterns or events that could indicate potential fraud, chargeback, or other financial risks over time. Nearline triggers function as an additional layer of monitoring, operating between real-time checks and deep-dive investigations, providing an effective means of early detection and intervention.

Nearline triggers are specifically implemented to provide proactive insights into the system and act as a preventative measure before risks evolve into more serious issues. These triggers generally help to reduce false positives and maintain a balance between user experience and fraud detection.

5.5.3. High to low value split ticket monitoring

This monitoring strategy is designed to identify and mitigate potential fraudulent activities related to "splitticket" fraud, where a fraudster attempts to circumvent transaction limits by making multiple small-value transactions rather than a single large one. In this scenario, a trend is observed where multiple declined transactions (typically greater than 3) are made using the same card, name, email, or telephone number, each declining in value, followed by a successful approval of a final transaction within the same hour or day.

This pattern could indicate an attempt to "test" the card or account, often to find a threshold where a transaction will be approved after several smaller failed attempts. These types of fraudulent activities aim to avoid detection and maximize the success of the final fraudulent transaction.

5.5.4. Low value to high split ticket monitoring

Designed to detect and mitigate potential fraud associated with "low-to-high split ticket fraud". This type of fraud occurs when a fraudster attempts multiple transactions that progressively increase in value, starting with small amounts and eventually culminating in a higher-value approved transaction. This pattern often appears as a strategy to bypass transaction limits or fraud detection systems by using an incremental approach, testing the card or account for successively larger amounts until a successful transaction is approved. The pattern typically occurs within a short time frame (e.g., within the same hour).

By identifying these trends, the platform can take action before the fraudster is able to complete their fraudulent transaction or cause financial losses.

5.5.5. Monitoring of Expired Card Response

To detect and respond to patterns where a significant percentage of declined transactions, within a specific time frame, are due to expired cards, "Do Not Honour" response or invalid card verification codes. The types of decline/rejected transactions could indicate invalid card usage or organized attempted fraud on compromised cards on our site.

This monitored utilizing risk modeling specifically related to high risk card behavior, systemically alerting our team which requires a manual review by our risk investigation team. The team will confirm the risk associated with the transactions and if needed, take preventative measures to ensure the fraud activity is mitigated.

5.5.6. Variance Checks

Customer activity is monitored to flag excessive variances in transactions based on historical patterns, this ensures we can identify potential compromised accounts as well as risk based behavior by our Customers, reducing the risk of excessive spending helping to manage our exposure and over extension by the Customer.

5.5.7. Velocity Controls

5.5.7.1. IP Address Checks

IP address is used to monitor both registration activity to help ensure geo variance is identified and flagged based on the information provided by the Customer as well as monitoring location using IP to confirm account information and location matching. The IP also allows us to put regional restrictions as well as identify high risk locations and suspicious activity based on variances/mismatched data.

1. Blacklist IP

- Flagged IP addresses are placed in our “Negative” database, allowing us to monitor the activity, triggering an alert and if needed used to restrict access from specific IP’s that we have determined to be high risk due to confirmed/suspicious activity.

2. Country IP Geo-Location

- Country specific monitoring through IP data and geo locating services are provided by a 3rd party (TrueValidate), allowing us to monitor activity that may pose a risk due to mismatched geographical information, triggering an alert and based on different rules in place, potentially requiring further verification

5.5.7.2. Transactions Coming from Proxy IPs

- Proxy IP’s generally mask location data, making it difficult to complete geographical and some identity checks, potentially attempting to bypass regional restrictions.
- We use a third party service (TrueValidate) to identify IP information, including device and location services, flagging proxy or VPN services, alerting the team.

5.5.7.3. Transactional Checks

We have further enhanced fraud prevention tools to monitor transactions, helping to reduce chargeback risk and potential Customer related abuse who may attempt to exploit unknown vulnerabilities or promotions, which is achieved with additional checks and pre-set limits:

- Limiting transaction amount per payment instrument
 - The maximum can not exceed \$2,000
- Limiting transaction amounts on a daily, weekly and monthly basis

- o The maximum allowed transaction amount per account on a daily, weekly and monthly basis is dependent on the account history and EDD status (Require to increase transaction limits)
- Limiting the number of active credit/debit cards on an account
- Escalation process in order to review accounts reach their limits
 - o Escalation process to review requests for limit changes / frequent requests giving oversight and ensuring proper limit control and Customer risk assessment

5.5.7.4. Physical Address Check

The physical address is verified using a third party service (Acuitytec, IDV-USA), comparing phone data, geolocation and personal data. Verification of address is completed with all new card registrations, comparing provided information with card issuer, allowing for mismatched information to be flagged and actioned.

5.5.7.5. E-mail Address Check

Third party services provide verification of the validity and risk associated with the email address provided – this allows us to determine risk based on age of email, compromised emails and the ability to receive emails, identifying invalid emails that may be associated with fraudulent registrations.

5.5.8. Offline Triggers

5.5.8.1. Decline Reason Codes Monitoring

Decline reasons are an identifier of potential abuse, which we report on regularly and receive alerts specific to high risk and potential issuer fraud blocks. This allows for identification of potential testing, BIN attacks and card running, we have a number of rules that trigger based off of this activity and take action to prevent further attacks if identified by placing additional restrictions on specific data that is identified related to an attack.

Both of these parameters may signal account abuse or fraudulent activity, as they represent a significant change in behavior. Below, we define how to monitor and analyze each parameter and set up alerting mechanisms.

5.5.8.2. Chargebacks Reason codes

Chargeback reason codes are provided by the acquirer and allow us to identify true fraud and potential Customer service issues. These are reviewed as needed and when necessary escalated to the provider to ensure accuracy in reporting.

5.5.8.3. BIN Analysis

BIN monitoring and analysis is completed on a regular basis and as needed based on variances in BIN activity within specific periods, significant increases may indicate a specific BIN and series is compromised and being tested, excessive declines either on a specific BIN or a unusually high number of attempts may also indicate testing or carding/running, resulting in a review and further mitigation methods.

5.5.8.4. Activity on Dormant Client Accounts

We trigger alerts on accounts that have any activity following a dormancy/inactivity period of 90+ days – these accounts are reviewed and actioned as needed.

5.5.8.5. SAFE and TC40

TC40 and SAFE are reported on through our provider daily and as needed, ensuring we are monitoring and maintaining the data as required by the card associations

- Monitoring our fraud to sales ratio and ensuring we remain at acceptable levels according to card association requirement
- Monitoring our dispute to sale ratio and ensuring we remain at acceptable levels according to card association requirement
- Monitoring TC40 and SAFE reporting to ensure accuracy

5.5.9. Review and Auditing

Internal KYC reviews are conducted periodically to ensure systems, processes and procedures are aligned and compliant with legal requirements. These reviews are completed as mandated by the regulatory body and is dependent on user KYC status, tenure, document age and other account information to ensure accuracy. In cases where KYC requires an update or additional documents are needed, the Customer is notified via email and telephone and account notification.

Internal audits are conducted at a minimum of once a year and as required to assess the effectiveness of current policies and processes and effectiveness of the system – detailed audit results are compiled and reported to senior management, providing full details of and all findings, requiring an action plan on identified opportunities. This process is in place to validate the platform adheres to regulatory standards and ensures a secure environment for all users.

This process is designed to ensure the platform adheres to regulatory standards and provides a secure environment for all users.

5.6. Reliance on third parties to perform customer due diligence.

All payment sources are verified using third party services (Acuitytec, Assurance Pay, Bank Account Verification, IP Stack) to ensure profile information matches with the financial institution, cross checking name, address, banking details, personal details including location as well as transactional history. These verification parameters are completed at the payout and deposit stage and may require further verification based on the provided results (Refusal to accept payment or transaction)

- Address Verification Services
 - Verifies registered information with payment issuer data, confirming payment instrument ownership
- Name Verification Services
 - Verifies registered information with payment issuer data, confirming payment instrument ownership
- Bank Account Verification
 - Verifies banking information matches registered information and account ownership

- Personal Detail Verification ○ Verifies DOB, Address and high risk factors related to geo location relative to transaction location and bank location

In house reporting and transaction rules allow for proper oversight and additional verification as needed and based on risk based data modelling.

5.7. Reporting of unusual transactions

5.7.1. Recognizing Unusual Transactions

UTRs are filed as needed and are based on account deposit/withdrawal/wagering activity within our platform. The intention of this process is to ensure activity that may be perceived as suspicious of money laundering, fraud or abnormal activity or dollar amounts exceeding the below threshold are properly reported to proper authorities as required.

The following transactions or intended transactions are deemed unusual:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Cg. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 - A cashless transaction in the amount of Cg. 5,000.00 or more.
 - Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 - Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 - A cash out in the amount of Cg. 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as “objective indicators”, while (d) is referred to as “subjective indicator”. While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behaviour of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

Additionally, linked transactions that cumulatively reach or exceed Cg. 5,000 within a 24-hour period are considered for unusual transaction reporting in accordance with the Ministerial Decree on Indicators for Unusual Transactions (2015, no. 73).

5.7.2. UTR filing process:

Internal Reporting:

- Any employee who suspects that a transaction may be unusual or related to money laundering, terrorism, or proliferation financing must immediately notify the Compliance Officer using the Internal Unusual Activity Report Form.
- The report must be submitted within twenty-four (24) hours of detecting the activity.
- The Compliance Officer must review the report, assess supporting information, and determine whether it meets the criteria for filing an external UTR.

Compliance Officer Review:

- The Compliance Officer has ten (10) business days to complete the internal review, obtain additional information if necessary, and document the rationale for the decision.
- If the transaction meets objective or subjective indicators, the Compliance Officer shall prepare and submit a UTR to the FIU Curaçao via the goAML platform.

External Reporting:

- Reports filed under the objective indicators (e.g., transactions $\geq$ Cg. 5,000) must be submitted to the FIU within forty-eight (48) hours after execution.
- Reports under subjective indicators must be submitted as soon as reasonably possible, but not later than ten (10) business days after detection.

5.7.3. Record Keeping and Retention

The Company maintains all records required under the NOIS, NORUT, and Sanctions Ordinance for at least five (5) years after the end of the business relationship or completion of a transaction. This includes:

- Customer identification and verification data;
- Risk assessments and due diligence records;
- Copies of Unusual Activity and Transaction Reports;
- Training, audit, and compliance review records.

Records are stored securely and made available promptly upon request by the FIU, CGA, or other competent authorities. Data retention and destruction follow the Company's data protection and confidentiality procedures.

5.8. Termination of Business Relationship

5.8.1. Termination of Player Accounts

The Company may terminate a player account whenever continuation of the relationship poses a legal, regulatory, or reputational risk. Termination may occur where a player fails to complete due diligence within required timeframes, where there is suspicion or evidence of money laundering, terrorist financing, or proliferation financing, or where false or misleading information has been provided.

The Compliance Officer reviews each case and documents the reasons for termination. Once the decision is confirmed, the account is suspended and any remaining funds are held pending review or guidance from the Financial Intelligence Unit (FIU) Curaçao. The player is notified of the closure only if doing so does not breach the prohibition on tipping-off. All actions and records relating to the termination are retained for at least five (5) years.

5.8.2. Termination of Providers and Third Parties

The Company may also terminate relationships with affiliates, payment service providers, or other partners that fail to meet its AML/CTF/CPF standards or cooperate with compliance requests. Where a business partner is suspected of involvement in unlawful or non-compliant activity, the Compliance Officer prepares a recommendation for termination, which is reviewed and approved by Senior Management.

Terminations are executed in accordance with contractual obligations and Curaçao law. If the case indicates possible money laundering or terrorist financing, a report is submitted to the FIU Curaçao. Records of such decisions are kept for a minimum of five (5) years.

5.9. Anti-Money Laundering Compliance program

The platform will establish a comprehensive monitoring process to track customer transactions and activities, with oversight designed to ensure AML guidelines are followed, escalating and actioning when appropriate. This will include, but not be limited to the following:

- **Transaction Monitoring:** All customer transactions will be monitored for unusual or suspicious activity. Automated systems will analyze transaction patterns to identify red flags such as:
 - Large or frequent transactions inconsistent with the customer's usual behavior.
 - Transactions involving high-risk jurisdictions or entities.
 - Any actions that trigger alerts under AML guidelines.
- **Behavioral Monitoring:** In addition to transactions, the platform will monitor customer behavior across the system. This may include account access patterns, login locations, and usage of specific platform features.
- **Real-time Alerts:** The platform will implement a real-time alert system that flags transactions or activities requiring further investigation. Alerts will be based on predefined risk parameters and thresholds.
- **Risk Scoring:** Each customer will be assigned a risk score based on various factors, including transaction history, geographic location, and account activity. Higher risk scores will trigger more frequent or in-depth reviews.
- **Threshold Guidelines:** During both deposit and payout stages, established thresholds require additional verification and escalation to detect and report cases that fall within the AML guidelines established by the gaming CGA

5.9.1. Appointment of a Compliance Officer

The Company has appointed a Compliance Officer at management level, independent from day-to-day gaming operations.

The Compliance Officer is responsible for the design, implementation, and continuous monitoring of the Company's AML, CTF, and CPF framework and for ensuring adherence to Curaçao laws and regulations.

The Compliance Officer shall have:

- Unrestricted access to all information necessary to perform their duties, including customer data, transaction records, and system logs;
- Authority to request cooperation from any employee or department;
- Direct communication with Senior Management and, where applicable, the Board of Directors;
- Responsibility for maintaining the AML program and reporting to the Financial Intelligence Unit (FIU) as required under the National Ordinance on the Reporting of Unusual Transactions (NORUT).

The Compliance Officer's duties include, but are not limited to:

- Monitoring and assessing the Company's compliance with AML, CTF, and CPF obligations;
- Maintaining and updating internal AML procedures and risk assessments;
- Receiving and reviewing internal Unusual Activity Reports and determining whether they meet criteria for reporting to the FIU;
- Preparing and submitting Unusual Transaction Reports (UTRs) via the goAML platform;
- Providing regular compliance reports to Senior Management;
- Organizing AML-related staff training and maintaining the training register;
- Advising management on new regulatory developments and ensuring timely policy updates.

5.9.2. Employee Screening

To ensure integrity and probity, the Company implements pre-employment and ongoing screening measures for all staff, including:

- Identity verification and reference checks;
- Assessment of criminal or regulatory history;
- Evaluation of role-related conflicts of interest or vulnerabilities to coercion.

Additional screening applies to employees in sensitive or decision-making roles related to payments, player verification, and AML operations. Records of all employee screenings are retained for at least five (5) years.

5.9.3. Employee Training

The Company provides AML training to all employees proportionate to their roles and exposure to AML/CTF/CPF risks.

The training program includes:

- Induction AML training for all new employees;
- Annual refresher training for existing staff;
- Ad hoc training when laws, internal systems, or products change.

Training covers the identification of unusual or suspicious activities, the internal reporting process, tipping-off prohibition, and employee legal responsibilities under the NORUT. The Compliance Officer maintains a register of all training conducted, including dates, attendees, content, and evaluation results.

5.9.4. Independent Audit Function

An independent audit of the AML compliance program shall be conducted at least once annually. The audit will:

- Review adherence to Curaçao AML, CTF, and CPF laws and internal procedures;
- Assess customer files, transaction monitoring systems, and FIU reporting;
- Evaluate the effectiveness of staff training, risk assessments, and controls.

Findings and recommendations from the audit are documented, presented to Senior Management, and followed by corrective action plans with defined timelines

5.9.5. Examination by the Curaçao Gaming Authority

The Company shall cooperate fully with any AML, CTF, or CPF examination conducted by the Curaçao Gaming Authority.

At all times, the following must be readily accessible:

- The AML Policy and Business Risk Assessment;
- The name and duties of the appointed Compliance Officer;
- FIU reports and supporting documentation;
- Training schedules and audit reports.

6. Compliance and Consequences of Non-Compliance

Compliance with this Policy is mandatory for all Company employees, officers, agents, and contracted third parties.

Failure to comply may expose both the Company and individuals to:

- Administrative fines or sanctions from the CGA or FIU Curaçao;
- Suspension or revocation of licenses;
- Criminal prosecution under Curaçao law;
- Reputational and financial damage.

Employees who breach this Policy may face disciplinary measures, including suspension, termination, or referral to law enforcement.

Third-party providers found non-compliant with AML obligations may have their contracts terminated. All compliance breaches are investigated by the Compliance Officer, with findings reported to Senior Management and remedial actions implemented promptly.

7. Contact Information

For any questions regarding this Policy or AML compliance matters, please contact:

Compliance Officer

Thot Management N.V.

Email: admin@thot-mgmt.net

8. Policy History

This is an updated version (January 2025) of the established policy 2018

Thot Management N.V. AML-Policy-Document-v3.1.

Final Audit Report

2025-11-06

Created:	2025-11-06
By:	Naomi Clifton (naomi.clifton@hbmgroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA23Z2E6BwwketZvCMM0G7DSOL0_AHJsgL

"Thot Management N.V. AML-Policy-Document-v3.1." History

-  Document created by Naomi Clifton (naomi.clifton@hbmgroup.com)
2025-11-06 - 1:10:07 AM GMT
-  Document emailed to Herman Oosten (herman.oosten@hbmgroup.com) for signature
2025-11-06 - 1:10:12 AM GMT
-  Document emailed to Bryon Finies (bryon.finies@hbmgroup.com) for signature
2025-11-06 - 1:10:13 AM GMT
-  Email viewed by Herman Oosten (herman.oosten@hbmgroup.com)
2025-11-06 - 11:53:50 AM GMT
-  Document e-signed by Herman Oosten (herman.oosten@hbmgroup.com)
Signature Date: 2025-11-06 - 11:54:07 AM GMT - Time Source: server
-  Email viewed by Bryon Finies (bryon.finies@hbmgroup.com)
2025-11-06 - 2:38:49 PM GMT
-  Document e-signed by Bryon Finies (bryon.finies@hbmgroup.com)
Signature Date: 2025-11-06 - 2:42:21 PM GMT - Time Source: server
-  Agreement completed.
2025-11-06 - 2:42:21 PM GMT