

Moon Technologies B.V (Curaçao)

AML/CTF/PF POLICY AND PROCEDURES

V2.1



Version Number	V2.1
Status	Active
Authorization and approved by	The Director of Moon Technologies B.V.
Review	Annual

Effective date	Version	Comments
09/03/2021	v.1.0	Initial Release
16/09/2024	v.2.0	Revision to reflect the new Curacao AML law, version table and tracking table added, typos correction, formatting adjustments. Addition of Anti-Money Laundering Compliance Program and Restricted Jurisdictions. Updates of Risk Based Approach, Customer Due Diligence, Record Keeping and Reporting
May 2025	v.2.1	Revision per the LOC. Version/tracking table added. Update to section 6. and 8.

a

Table of Contents

1.	5	
2.	6	
3.	7	
4.	8	
	MONEY LAUNDERING	8
	PROLIFERATION FINANCING	8
	TERRORIST FINANCING	9
	HIGH RISK COUNTRY	9
	POLITICALLY EXPOSED PERSON (PEP)	10
	SANCTIONS	10
	FIAT CURRENCY	10
	CRYPTO (DIGITAL) CURRENCY	10
5.	11	
	BUSINESS RISKS (BRA)	11
	CUSTOMER RISKS (CRA), PRODUCT RISKS (PRA), TECHNOLOGY RISKS (TRA)	11
6.	12	
	DUE DILIGENCE	12
	BENEFICIAL OWNERSHIP	14
	PEPS & SANCTIONS:	14
	ENHANCED DUE DILIGENCE	16
	SIMPLIFIED DUE DILIGENCE	18
	THE TERMINATION OF THE BUSINESS RELATIONSHIP	19
	ONGOING MONITORING:	20
7.	23	
	DEPOSITS & WITHDRAWALS:	21
	CRYPTOCURRENCY TUMBLERS & MIXERS	23
8.	27	
	SUBMITTING A FORMAL UNUSUAL (SUSPICIOUS) TRANSACTION REPORT	26
9.	30	
10.	30	
	INTRODUCTION	28

INTERNAL POLICIES, PROCEDURES AND CONTROLS	29
THE APPOINTMENT OF A COMPLIANCE OFFICER	29
THE EMPLOYEE SCREENING AND ONGOING TRAINING PROGRAM	30
AN INDEPENDENT AUDIT FUNCTION	30

11. 33

W

1. POLICY APPROVAL

Moon Technologies B.V. (the 'Company') is a company registered and incorporated in Curaçao with Company registration: 152185.

The Company is committed to ensuring that it takes all appropriate steps to prevent its systems from being used for the purposes of money laundering, terrorist financing or other crime, including but not limited to.

These measures include:

- the appointment of a suitably qualified Anti-Money Laundering & Compliance Officer
- board approved policies and practices
- risk-based approach to all business relationships
- applying appropriate use of technology and tools to help identify and mitigate risk
- ensuring all employees are suitably trained
- reporting suspicious activity to relevant law enforcement agencies
- an annual independent audit of its Anti-Money Laundering Compliance Program

This document has been produced to ensure that the Company acknowledges and applies appropriate measures to address the higher level of risks associated with the acceptance and use of crypto (digital) currencies in relation to its products and services.

This document has been reviewed and approved by a resolution of the Management Board of the Company.

All future versions and updates will be reviewed by the Management Board before being approved and issued.

The latest version of this document will replace all previous versions within the Company's operations.

All changes, additions and approvals to this policy will be captured in the tracking tables on the page 2 for the record purposes.



2. GENERAL PROVISIONS

The Company is licensed and regulated by the Government of Curaçao to offer interactive (online) remote betting and gambling products (games of chance) and services under a license issued by The Curacao Gaming Control Board (GCB) with:

Gaming License Number: OGL/2023/111/0069

In accordance with the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63) (NOOGH).

The company is further approved to accept and transact with customers in either fiat (traditional currencies), crypto (digital or virtual) currencies or a combination of both.

Under the terms of its operating licence the Company is required to have in place adequate policies, processes and procedures to prevent its systems from being used for the purposes of money laundering, proliferation financing, terrorist financing or other criminal activity.

This document will be reviewed on regular basis and ad-hoc basis as required by changes to laws and regulations, changes to licence conditions, introduction or implementation of new products and services or in accordance with the Company's risk management practices and procedures.



3. LAWS & REGULATIONS

The designated supervisory Authority for service providers offering their services from the jurisdiction of Curacao, or under a license issued by a Curacao service provider or master licensee is The Curacao Gaming Control Board (GCB).

The Company is required to comply with all applicable laws and regulations, including:

- The National Ordinance Criminal Code (P.B. 2011, no. 49);
- The National Ordinance of November 23, 2015 amending the National Ordinance identification for services (P.B. 2015, no. 69);
- The National Ordinance on Identification when Rendering Services or NOIRS (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92); and
- The National Ordinance on the Reporting of Unusual Transactions or NORUT (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99).

These Ordinances require that all service providers offering online games of chance (including but not limited to sports-betting and casinos) from the jurisdiction of Curacao must have in place adequate practices and procedures to prevent the Company and its systems from any activity that facilitates money laundering, proliferation financing, funding of terrorism or other criminal activities.



4. DEFINITIONS

MONEY LAUNDERING

Money laundering defined as:

- the conversion or transfer of funds or property derived from criminal activity;
- retaining funds or property derived from criminal activity;
- participation in such activity such as for the purposes of concealing, or disguising the illicit origin of the funds or property or assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions;
- acquisition, possession or use of funds or property derived from criminal activity, or property obtained instead of such funds or property, knowing, at the time of receipt, that such funds or property was derived from criminal activity or from an act of participation;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, funds or property derived from criminal activity.

Furthermore, Money Laundering consists of three phases:

- **Placement.** During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- **Layering.** This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- **Integration.** The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

PROLIFERATION FINANCING

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

TERRORIST FINANCING

Terrorist financing is defined as:

- the allocation or raising of funds to plan or perform acts which are deemed to be acts of terrorism or to finance operations of terrorist organizations, or in the knowledge that the funds allocated or raised will be used for the aforementioned purposes.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

HIGH RISK COUNTRY

A high-risk country is defined as:

A country or territory where the risk of money laundering, terrorism or financial or other crime is considered to be higher than other countries or territories, as may be determined by organizations such as:

- Financial Action Task Force (FATF)
- Moneyval
- International Monetary Fund (IMF)
- US Office of Foreign Asset Control (OFAC)
- European Union
- United Nations

The term high risk can be applied to either the country or jurisdiction or to nationals, citizens or residents of the country or jurisdiction. Equally, nationals, citizens or residents of high-risk countries or jurisdictions may be subject to Sanctions checks preventing or limiting a business relationship.

W

POLITICALLY EXPOSED PERSON (PEP)

A Politically Exposed Person is defined by the National Ordinance on Identification when Rendering Services (NOIRS) as:

- an individual or person who holds or has a prominent public function with the exception of those who have held this position for less than a year, and the immediate family members or close associates of these persons.

SANCTIONS

Sanctions may be imposed on countries, companies or individuals.

Sanctions listed individuals are defined as:

- individuals subject to regulatory or financial sanctions or enforcements, known terrorists, money launderers, fraudsters and black-listed persons.

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly, or indirectly, to or for the benefit of any designated persons or entities.

FIAT CURRENCY

Fiat currency is currency that is issued and declared to be legal tender by a national government such as British pound, or a political or economic coalition such as the EU and the Euro.

It is issued by a central authority and whilst transactions can be peer to peer most electronic transactions are facilitated by a third-party payment processor.

CRYPTO (DIGITAL) CURRENCY

Crypto currency is a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority or payment processor.

It works in the same way as fiat currency in that it has a monetary value and can be transferred in exchange for goods or services.

The decentralization and strong encryption used to transfer cryptocurrencies allows users to make transactions without disclosing personal information, providing end users with anonymity, and therefore increasing the risks of money laundering or links to crime.

5. RISK BASED APPROACH

The Company is committed to taking a risk-based approach through its Anti-Money Laundering Compliance Program. Its primary goal is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

The company will implement a set of policies and practices to identify and mitigate risks including:

- identify and assess the level of risk (low to very high)
- assess the impact of risks identified
- identify and implement controls to mitigate against the risk and its impact
- ensure on-going monitoring to evaluate and ensure the effectiveness of the controls
- periodically review and update its risk management policies and processes in accordance with events, the introduction of new products or technology or changes in laws and regulations.

The company will conduct a full assessment in relation to identifying and implementing controls to mitigate:

BUSINESS RISKS (BRA)

- e-commerce
- sector specific
- partners, suppliers and associates
- employee
- National Risk Assessment (NRA)

CUSTOMER RISKS (CRA), PRODUCT RISKS (PRA), TECHNOLOGY RISKS (TRA)

- geographical and location
- PEPs and Sanctions
- customer interactions
- product risks
- payments risks
- channel risks
- technology risks

The company shall also properly document all its risk assessments, including everything that has been done and the reason for this being done.



6. CUSTOMER DUE DILIGENCE

The Company will apply appropriate customer due diligence measures to all customers in accordance with applicable laws and regulations. Due to the technical and virtual nature of crypto (digital) currencies, initial due diligence will also include checks relating to technical identifiers.

Through the Anti-Money Laundering Compliance Program, the company shall implement the appropriate set of procedures and policies and processes for identification of the player by collecting the relevant information to:

- to establish the purpose and nature of the business relationship
- to verify player's identify and age
- to assess any and all risks that might be associated with the player
- to build a customer profile
- to assess how the player is going to act within the framework of the business relationship

DUE DILIGENCE

The Company will apply due diligence checks as part of its customer registration (onboarding) procedures.

The company is to undertake Customer Due Diligence measures when:

- when players engage in financial transactions equal to or above Naf. 4,000¹ (2,000 eur)
- carrying out occasional transactions¹ above the monetary equivalent of Naf. 4,000² (2,000 eur)
- there is a suspicion of money laundering or terrorist financing
- the casino has doubts about the veracity or adequacy of previously obtained customer identification data

Prior to establishing a business relationship or allowing its products or services to be used by the player (upon the account registration) the Company will also conduct minimum, or enhanced, due diligence checks where the based on the risk scenarios following information will be collected: using external third-party verification providers to confirm the following:

- i. Date of birth
- ii. Full name
- iii. Permanent residential address

¹ An occasional transaction refers to a one-time interaction with a customer who is not anticipated to return. This typically occurs in land-based casinos, where creating an account is not necessary to participate in gaming activities.

² Note: A transaction can be a single occurrence or a series, combination, or pattern of transactions that collectively exceed the monetary equivalent of Naf. 4,000.

- iv. Nationality
- v. Place of birth
- vi. Identity number

In a low-risk scenarios, the company may limit the identification to only three personal details set out in (i) to (iii) above. However, in the high-risk situations the company shall consider collecting further personal details as necessary for mitigation of the higher risk of ML/TF.

Further to the above, Sanction screening and PEP status screening will also be performed, where the said checks are to take place prior entering the business relationship with the player or performing an occasional transaction for the first time with the player.

In instances where players are required to create an account to access demo games, and such accounts may also be used for paid games, the company is obliged to collect personal information from the player during the account registration process. This ensures compliance with regulatory requirements and facilitates the secure and seamless transition between demo and paid gaming experiences.

The company will check published lists of known or suspected terrorists or other sanctioned persons or companies:

- [UN Sanctions](#)
- EU sanction list

For the PEP status screening the company might rely on the combination of internal open-source checks and third-party verification tools.

In addition to the due diligence checks conducted prior to the establishment of a business relationship, the Company will also verify at registration, and thereafter every log-in, deposit and withdrawal:

- email address
- device (hardware) machine fingerprint
- IP address
- browser information

Information is being cross-checked using a combination of technology and internal tools to identify links and associations with any other active or historical accounts.

Where such a link is identified the customer account will be suspend pending additional checks to establish the operator (controller) of the account and eliminate any risk of multi-accounting or use of bots.

These technical checks are also applied and used for customers using fiat currency but may not always form part of the initial due diligence check at on-boarding.

Customers that do not pass due diligence or are identified as a possible PEP or Sanctions listed individual will be subject to enhanced due diligence checks prior to having a business

relationship established.

Enhanced due diligence will be conducted by a number of methods, including but is not limited to:

- Verification based on personal documents e.g. passport, identity card, proof of address, etc.
- Social media and publicly held data
- Privilege information from other operators, sources
- Financial or corporate data
- Third-party data providers



There is a higher risk of cryptocurrency being associated with Sanctions listed individuals who may be the subject of regulatory or financial sanctions, or resident in a country or jurisdiction which is a subject to financial, regulatory or other sanctions, limiting or restricting their use of the established financial and payments eco-systems.

As a result, Sanctions checks form a key aspect of the initial due diligence applied to new customers using crypto (digital) currency.

BENEFICIAL OWNERSHIP

The company has a strong stance towards the account registration and engagement in transactions to be allowed only for those players, who act on their own behalf and out of their own will. The company stance is also stipulated in its General Terms and Conditions. All players are required to familiarize themselves with General Terms and Conditions and their agreement is recorded through the acceptance during the account registration.

PEPs & SANCTIONS:

The definition of a Politically Exposed Person (PEP) in the National Ordinance on Identification when Rendering Services (NOIRS) is as follows:

Persons who hold or have a prominent public function with the exception of those who have held this position for less than a year, and the immediate family members or close associates of these persons.

In line with its obligations (Article 2 of NOIRS), the Company will:

- a. Implement appropriate risk management systems to determine whether a client or ultimately interested party is politically vulnerable;
 - b. obtain approval from the persons responsible for the overall management of the service provider, for entering into a business relationship with or effecting a transaction for such client, or beneficial owner as well as obtaining such approval if during the business relationship the client or beneficial owner becomes a politically exposed person;
 - c. take risk-based and adequate measures to identify the source of political capacity prominent person and the funds used in the business relationship or transaction to pose; and
 - d. maintain on-going monitoring and tight control of the business relationship.
1. The following persons shall be persons performing prominent public functions, and subject to a PEP check:
 - a) a state, head of government, minister and deputy or assistant minister;
 - b) a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors, or of the board of a central bank;
 - c) an ambassador, a chargé d'affaires or a high-ranking officer in armed forces;
 - d) a member of an administrative, management or supervisory body of a State-owned enterprise;



e) a director, deputy director or member of the board, or equivalent function, of an international organization, except middle-ranking or more junior officials.

2. The following persons are considered family members of a person performing prominent public functions:

- a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or a local politically exposed person;
- b) a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person;
- c) a parent of a politically exposed person or local politically exposed person.

3. The following persons are considered close associates of a person performing prominent public functions:

- a) a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person or a local politically exposed person;
- b) a natural person who has 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 or local politically exposed person.

Where a PEP is positively identified, the Company will conduct a full review and gain approval from the management board or service provider prior to establishing a business relationship.

The Company will conduct on-going PEP screening checks as part of its on-going due diligence procedures.

The following is taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

This means that the measures taken can be tailored to the risks in a specific case. Screening for PEP status shall be carried out before establishing the business relationship or conducting the occasional transaction.

The Company will ensure that it conducts appropriate due diligence checks to identify any individuals that may be subject to regulatory or financial sanctions or enforcements, known terrorists, money launderers, fraudsters and black-listed persons.

Where a Sanctions listed individual is positively identified the Company will not establish a business relationship but will conduct a review to establish is a disclosure should be submitted to law enforcement and notify the management board and/or service provider.

The Company will conduct on-going Sanctions screening checks as part of its on-going due diligence procedures.



ENHANCED DUE DILIGENCE

The Company will conduct enhanced due diligence irrespective of any other triggers or 'red flags' in the following circumstances:

- a) in accordance with Curacao money laundering thresholds of 5,000.00 NAF (ANG) (or equivalent in any currency fiat or digital) which equals to approx. 2,400.00 EUR for a single or consolidated deposit or withdrawal transaction for any customer;

W

- b) where a customer makes a deposit using one payment method and wishes to withdraw to another where the ownership of each payment method is not verified e.g. using a pre-paid card or voucher.

In addition to the checks above, the Company will also conduct additional source checks, if applicable, to identify the provenance and origin of funds used, including but are not limited to:

- Bank account bank statements
- Proof of income or ownership of payment methods
- Financial record and accounts
- Source of Funds (SOF)
- Source of Wealth (SOW)

The Company will conduct enhanced due diligence at any time where the customer's risk profile or established pattern of behavior or activity changes based upon any number of 'red flags', including but not limited to:

- where a potential customer is reluctant to provide supporting evidence to allow us to verify their identity and/or provide information on the entity we are potentially doing business with;
- where a potential customer presents unusual, inconsistent or suspicious identification documentation;
- where a customer or potential customer is reluctant to provide information in relation to the source of their wealth or funds;
- where a customer uses multiple credit cards to deposit money within a short period of time, also known as 'tumbling';
- where a customer deposits a sum of money and makes a request to withdraw it having engaged in minimal or no gameplay;
- where a customer is situated in a higher-risk jurisdiction or is identified as being listed on the international sanctions list (subject to the special procedure for U.S. sanctions described below);
- where a customer is associated or linked with other customer accounts in any way (including active, dormant or suspended/terminated accounts)
- where a customer attempts to open several accounts using either variations of their own or different names;
- where a customer's registered location and active IP address does not match;
- where the registered payment method details do not match the player's registered details;
- where there is a mismatch between the customer's country of residence and the location of their method of payment;
- where the customer logs into their account from multiple countries or attempts to circumvent geo-location controls to access the Company account from a prohibited jurisdiction;
- where different players are identified as sharing bank accounts from which deposits or withdrawals are made;
- where a customer uses one payment method to make a deposit and requests a withdrawal to



- be made to a different account;
- where a customer initiates payments which are just below reporting or recordkeeping limits [i.e. 5,000 NAF (ANG) or equivalent], or the Company's maximum transaction limits;
- where a customer attempts to hide the size of a large transaction by breaking it into multiple, smaller transactions;
- where a customer engages in unusual or inconsistent gameplay or financial activity; and
- other indicators of higher risk identified in the 'Ongoing Monitoring' section of this policy.

In situations presenting a higher risk of ML/TF, the Company shall request the source of funds information from time to time even though there may not be any change in pattern or activity conducted by the customer.

SIMPLIFIED DUE DILIGENCE

Where the risks of money laundering or terrorist financing are lower, the company will conduct simplified CDD measures, which shall take into account the nature of the lower risk.

The examples of the measures the company might chose in such scenarios to implement are, but not limited to:

- not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing, then it is only necessary for the company to obtain the player's identity. In this case casinos may limit identification to the first three personal details (I,ii,iii) in as stated under section 6 Due Diligence of this document
- verifying the identity of the customer and the beneficial owner after the establishment of the business relationship
- the extent of verification may also vary depending on the risk posed by the particular business relationship. In a low risk situation, the company can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements, Utility Bills³ etc.)
- the extent of personal details verified can also vary. In low risk situations, the company shall only take the mandatory approach to verify the basic identification details, while the verification of any other personal details will be upon the company and its internal decision, as long as it has sufficient comfort that it knows who its customer is

³ Only fixed-line telephone bills are accepted as valid proof of address for phone bills



- reducing the frequency of customer identification updates

- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold

Simplified CDD measures shall not be applied by the company in those cases, where a reasonable suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

THE TERMINATION OF THE BUSINESS RELATIONSHIP

In the cases where the above conditions under part 6 of this document cannot be met, the company shall not establish the business relationship with the customer. In those cases where the business relationship is already established, however there is a reasonable ground to for suspicion of any ML/FT/PF activity, the company might also terminate the business relationship with the customer. This action would be followed by appropriate report to the FIU. Termination of the business relationship might also occur in those scenarios where the player is reluctant to provide the sufficient documentation to verify the player's identity.

In all the scenarios the company will document all the factors and information it has in its disposal as well as the steps taken in order to make the necessary documentation and information available.

In those cases where the termination of the business relationship takes place, however there is no reason for the retention of funds, the company shall return the funds back to the player. This shall be done through the same channels used to receive the funds.

W

ONGOING MONITORING:

The Company has a continuing duty to conduct ongoing monitoring of all customer relationships and to be vigilant with regard to money laundering and terrorist financing at all times and to report any suspicious transactions or circumstances.

The Company will monitor all customer transactions and activity in accordance with industry best practice, international recommendations and guidelines including but not limited to:

- Player identity; player due diligence and identification data;
- Player financial habits and behaviors, to ensure that the transactions are consistent with the licensee's knowledge of the player's risk profile;
- Player gaming habits and behaviors to ensure that the transactions are consistent with the Company's knowledge of the player's risk profile;
- Individual or linked transactions which are complex or unusually large with no apparent economic or lawful purpose;
- Unusual patterns of transactions with no apparent economic or lawful purpose;
- Transactions which exceed certain limits with no apparent economic or lawful purpose;
- Very high account turnover inconsistent with the balance;
- Transactions or behaviors which are outside of the player's regular activity pattern;

The conditions of ongoing monitoring such as frequency or the extent of the checks shall be determined by the risk level assigned during the stage of risk assessing the customer.

Where the Company is not able to complete due diligence checks it will suspend the business relationship until such time as all checks have been satisfactorily completed.

Where the Company suspects or believes there is a risk of money laundering or terrorist financing it will submit a report to the relevant law enforcement authority.



7. CRYPTOCURRENCY TRANSACTIONS

Due to the higher level of risk associated with cryptocurrencies the Company will apply additional due diligence requirements and security checks to those customers and accounts who wish to deposit and transact using crypto currencies.

The due diligence and security checks detailed below are in addition to the checks already applied to customers using fiat currencies, not instead of.

Where the Company is not able to complete any check to its satisfaction it will suspend the customer account until such time as checks have been completed.

Where it is not able to complete all necessary checks or assure itself of either the identity of the customer or the source of funding, the matter will be referred to the management board and /or service provider for review and final decision.

Where the decision is to terminate the relationship any retained customer funds will be held in a seized funds account and declared as part of any suspicious activity report made to law enforcement.

DEPOSITS & WITHDRAWALS:

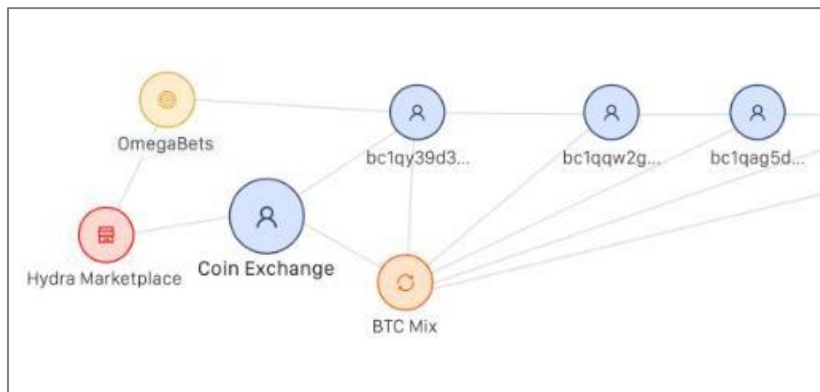
Due to the enhanced risks associated with crypto (digital) currencies the Company will apply specific checks to customers and transactions made using non-fiat currencies.

Such checks will be conducted at each deposit and withdrawal request made by any customer until such time that the Company has established a risk profile for the player.

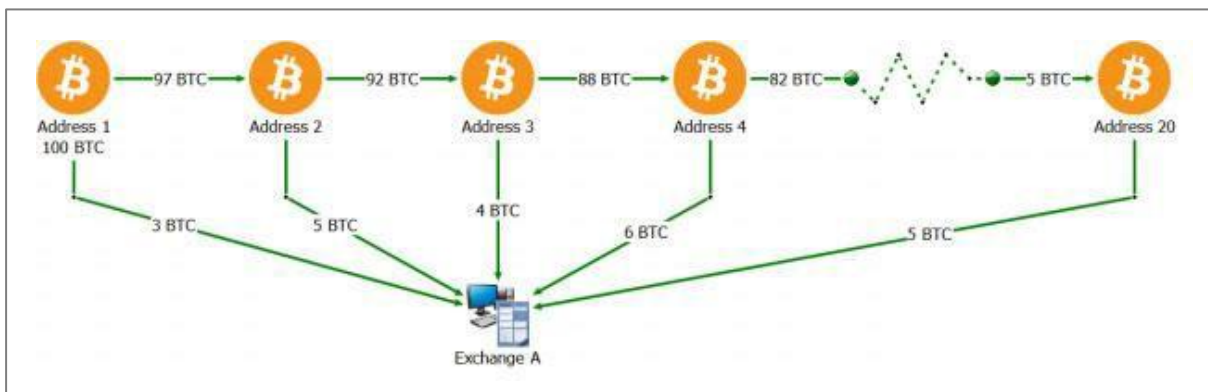
Incoming deposits will be screened based upon the unique cryptocurrency (wallet) address using software that is designed to establish the identity of the entity (not individual) that controls the cryptocurrency wallet.

The same software will also allow the Company to track how and where the cryptocurrency has been used before being used as a deposit coming into the Company.

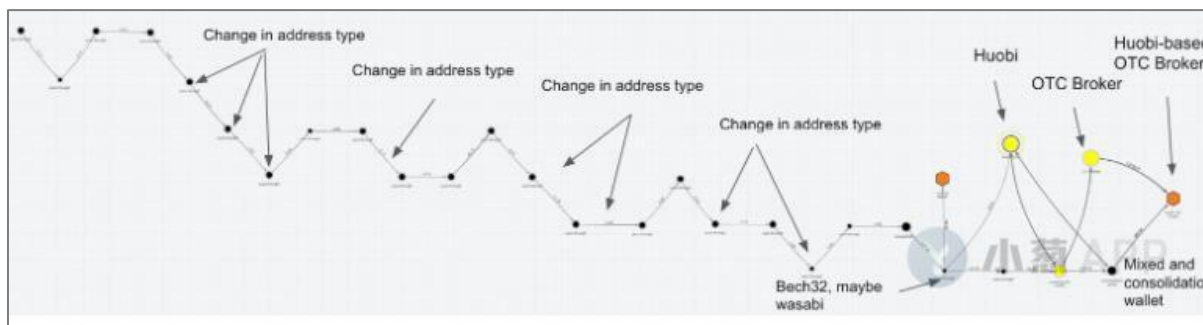




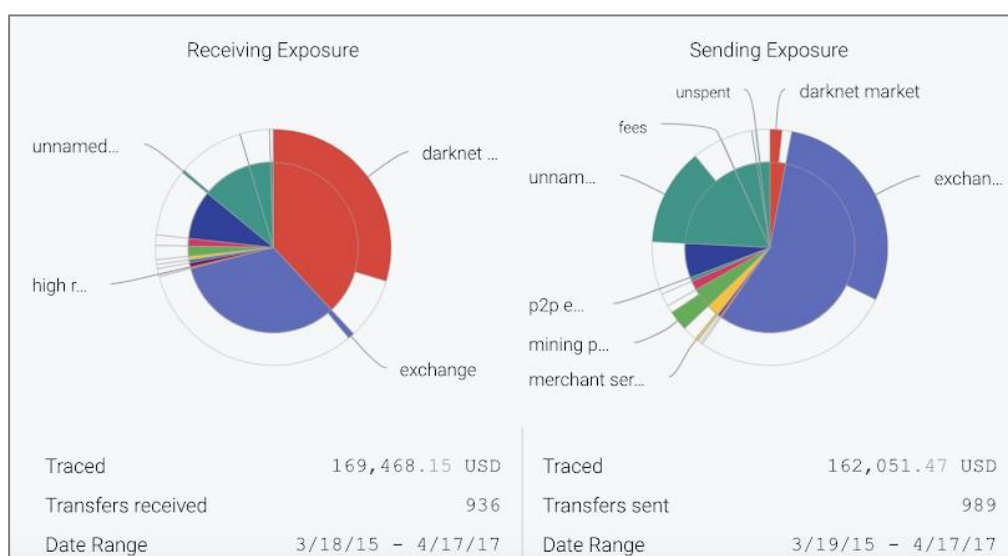
The software will help to identify whether the deposit is linked in any way to a 'peel chain' - chains of e-wallets that hackers use to transfer funds to make the movement of illegally obtained crypto funds unintelligible and undetectable.



Peel chains can be very complex as hackers add more and more cryptocurrency wallets to disguise the source of the funds.



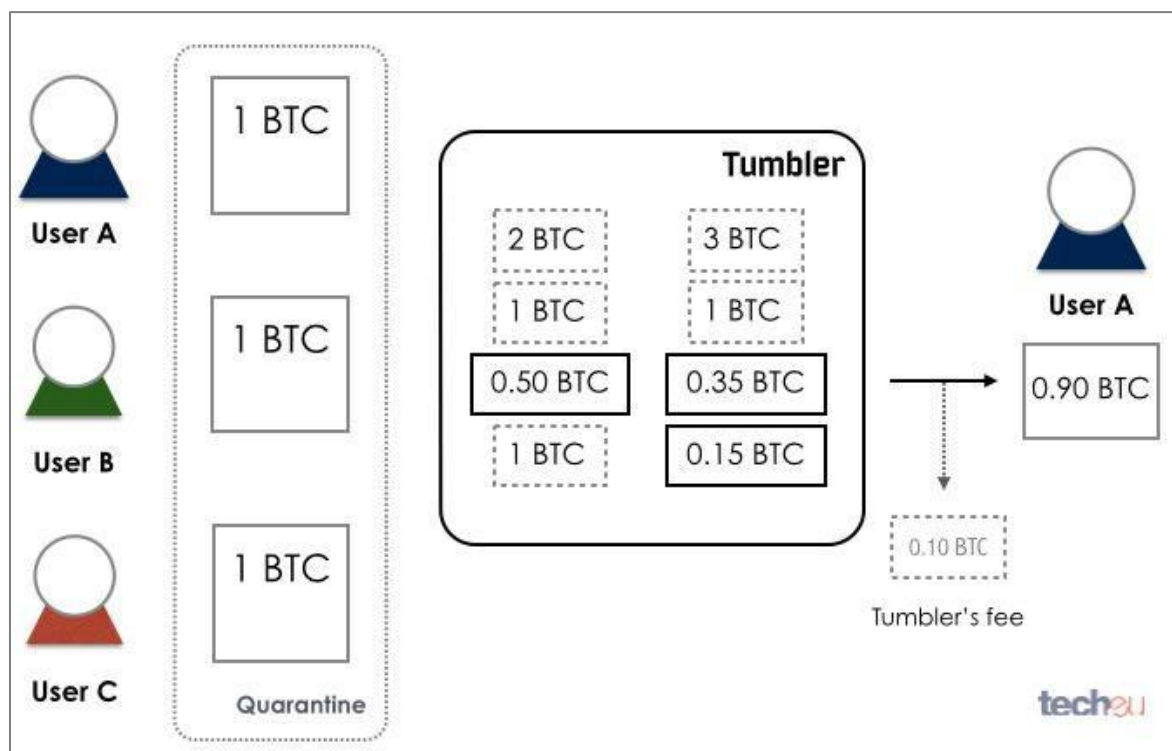
The application also helps identify whether the use of a particular crypto currency wallet is linked to any negative, blacklisted or illegal activity such as a hacked wallet or exchange, or on the black market or the 'dark web'.



CRYPTOCURRENCY TUMBLERS & MIXERS

The Company will also use technology and external services to help to identify whether the crypto (digital) coins that have been processed through a cryptocurrency tumbler or cryptocurrency mixing service.

a



Cryptocurrency tumblers or mixers are a third-party service designed to break the connection between a wallet address sending coins and the addresses receiving coins so as to obscure the trail back to the fund's original source.

Where the Company suspects or has reason to believe that funds are linked to a tumbler or mixer service i.e. already laundered before coming to the Company it will immediately suspend the customer account.

Irrespective, the Company will submit a suspicious activity report to the law enforcement authority as it now has information to reasonably suspect or believe that the funds are linked to money laundering and notify the management board and/or service provider.

The Company will use a combination of analytical tools, monitoring and verification checks that may allow for a cryptocurrency address to be linked to a specific individual.

Any 'red flags' which identify multiple, associated or suspicion use of a cryptocurrency address will result in an investigation and the transfer of funds and the customer account suspended until such time as the investigation is completed, including establishing if activity from a group or cluster is normal behavior for that customer.

a

8. REPORTING SUSPICIONS AND UNUSUAL TRANSACTIONS

The Company shall submit a formal suspicious activity report to law enforcement in respect of any individual that is positively identified as being on a Sanctions list, in accordance with the process set out in the Company's AML Policy.

In accordance with Article 1 of the National Ordinance on the Reporting of Unusual Transactions or NORUT (Landsverordening meldingongebruikelijke transacties (LMOT), PB 2017, no. 99) ('NORUT') the Company has a duty to report unusual (suspicious) transactions which may be linked to money laundering, the financing of terrorism or other criminal activity. This duty is also stated in Article 4 of the AML/CFT/CFP - Regulations released on May 20, 2024 by the Curacao Gaming Control Board.

The company is required to detect and report not only suspicious transactions, but also unusual transactions. This is achieved by having adequate procedures in place where the following areas are being covered:

1. The recognition of unusual transactions
2. The Documentation of unusual transactions
3. The reporting of unusual transactions

An unusual transaction can be a single or a series or a combination of transactions inconsistent with the player's profile. The Company management is also to provide its staff with specific guidance and training in recognizing and adequately documenting unusual transactions.

The following transactions or intended transactions are deemed unusual:

1. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
2. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
3. Transactions in the amount of NAf. 5,000 (2,500 eur) or more regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:
 - a. A cashless transaction in the amount of NAf. 5,000 (2,500 eur) or more.
 - b. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
 - c. Accepting or releasing a deposit in the amount of NAf. 5,000 (2,500 eur) or more at the request of the client;
 - d. Sale to a customer of chips in the amount of NAf. 5,000 (2,500 eur) or more. "Chips" include but is not limited to tokens and credits.



- e. A cash out in the amount of NAf. 5,000 (2,500 eur) or more⁴;

The Company is also required to report both actual and intended (attempted) transactions.

Where there are any concerns regarding any customer or any actual or attempted transaction, employees should in the first instance send an internal report to the Compliance Officer / Money Laundering Reporting Officer. The steps to making a formal report as are follows:

1. An internal suspicious transaction report must be made to the Compliance Officer / Money Laundering Reporting Officer no later than 24 hours between the execution of the transaction (or the intention to execute a transaction).
2. The Compliance Officer / Money Laundering Reporting Officer will have 10 working days to complete any additional investigations needed to ascertain the risk of money laundering, terrorist financing or other crime.
3. Following the period of investigation any unusual (suspicious) transaction report must be submitted within 48 hours of the Money Laundering Reporting Officer making the decision to submit a report.

If this is not possible the Company will submit a request for dispensation (5 days) in writing to the FIU, stating the reasons for the extension.

The Money Laundering Reporting Officer will also notify the management board and/or service provider that a formal report has been submitted.

SUBMITTING A FORMAL UNUSUAL (SUSPICIOUS) TRANSACTION REPORT

All reports must be submitted using the FIU online reporting system: FIU Curaçao and goAML reporting portal. All supporting documentation is to be included in such report and available in English.

The Company and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU. It is also not permitted to disclose information to the customer nor to third parties.

There are two types of indicators which are used to determine the type of report to be made:

1. Objective indicator - the circumstances under which a transaction is to be considered as

⁴ The indicated examples are not limited, also credit card transactions and e-wallet transactions are to be reported to the FIU.

unusual.

2. Subjective indicator - the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, and any other circumstance that may be relevant) has reasonable indications to presume that a transaction is related to money laundering or terrorism financing. For subjective indicators, red flags can be suggested by the supervisors and/or the FIU that indicate such possible presumptions.

The indicator letter for providers of Providers of Internet Gambling is: G

The indicators for internet (online) gaming and gambling operators are as shown below.

Objective indicators

<i>A. A transaction which is reported to the police or judicial authorities</i>	
Indicator	Definition
G0000111	A transaction which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism.
<i>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.</i>	
G0000114	An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions National Ordinance.
<i>C. A transaction amounting to NAF (ANG) 5,000.00 or more, regardless 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 comprises in any case the following situations:</i>	
G0000135	1. <i>A giro-based transaction amounting to NAF (ANG) 5,000.00 or more:</i> A giro-based transaction is a transfer from a bank account of the service provider to a local or international bank account carried out at the request of the client addressed to the service provider.
	2. <i>The taking into deposit or the releasing out of deposit of an amount of NAF(ANG) 5,000.00 or more, at the request of the client.</i>
	3. <i>Sale of tokens to a client in the amount of NAF (ANG) 5,000.00 or more.</i> The term "tokens" includes at least chips and credits.
	4. <i>Payout of prizes in the amount of NAF (ANG) 5.000,-- or more.</i>
	5. <i>All other cases.</i>
NB In case of Indicator G0000135: please also indicate the applicable sub-indicator (1,2,3,4 or 5) when reporting a transaction. In case of sub-indicator 5, please always provide a description of the situation.	

Subjective indicator

<i>Suspected money laundering transactions or financing of terrorism.</i>	
Indicator	Definition`
G0000211	A transaction giving cause to assume that it may be connected with money laundering or terrorist financing.

9. RECORD-KEEPING

The Compliance Officer / Money Laundering Reporting Officer will maintain a full record of and notify the management board and/or the service provider of the following:

- all internal reports received;
- review and decision-making process;
- all formal unusual (suspicious) transaction reports made to the FIU
- all individuals that are identified as a PEP
- all individuals that are identified as a possible Sanctions listed individual and the outcome of any review of that individual

The Company shall store and maintain for a period of minimum 5 years all necessary records on transactions. All records obtained through Due Diligence measures (such as ID cards, driving licenses, passports, and more) shall be also kept for a minimum period of 5 years since the date of the last occasional transaction or since the day due to which the business relationship with the customer has ended.

10. ANTI-MONEY LAUNDERING PROGRAM

INTRODUCTION

An anti-money laundering program is an essential component of the Company compliance regime. The primary goal of the program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

The core elements the Anti-Money Laundering Compliance Program is addressing, are:

1. A system of internal policies, procedures and controls;
2. A designated compliance officer with day-to-day oversight over the AML program;
3. An employee screening program and ongoing employee training program; and
4. An independent audit function to test the AML program.

The Company tests the anti-money laundering program systematically and adapts the program to the current risks that arise within the Company's own organization. The AML program has the approval of senior management.



INTERNAL POLICIES, PROCEDURES AND CONTROLS

The Company is committed to combat any possible abuse of its facilities, products and services for purpose of Money Laundering, Terrorist Financing and the Proliferation Financing. For this purpose, the Company puts in place specifically designed policies, procedures and controls which are being periodically revisited to ensure their ongoing efficiency of their design.

This policy is in place as the master policy of the Company for AML/CTF/PF areas, where further details on practices and guidelines are included in the Companies' AML/CFT/PF procedures and internal controls. All policies, procedures and controls are reviewed and approved by senior management or the board of directors.

THE APPOINTMENT OF A COMPLIANCE OFFICER

The Company shall formally designate a senior officer at management level and independent from the game's operations, responsible for the detection and deterrence of money laundering and terrorist financing. The Company will also ensure that the designated individual has sufficient experience, time and resources in order to perform this role and its responsibilities.

The duties of the Compliance Officer are, but not limited to:

- To design, implement and maintain the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the Company's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;

The above-mentioned responsibilities shall be included in the job description of the compliance officer. The job description shall be signed off and dated by the officer, indicating his/her acceptance of the entrusted responsibilities.

The current Compliance Officer is:

Name: Ondrej Zlesak

Contact details: ondrej.zlesak@yolo.com



THE EMPLOYEE SCREENING AND ONGOING TRAINING PROGRAM

All new employees are subject to screening for criminal background and designated procedures are in place for the onboarding process. The Company also has a training program in place for its both new and current staff. All employees are receiving training / re-training based on their role designation and the time period passed since the initial training.

All new employees who will handle customers or their transactions, irrespective of their level of seniority, shall received the training of the nature and process of Money Laundering and Terrorist financing. This also extends to any and all the Company's audit staff, AML Compliance staff, supervisors and managers, senior managers and the board of directors.

Following records shall be also kept at all times in the designated training register:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

AN INDEPENDENT AUDIT FUNCTION

An independent audit is being performed on the Company's AML Compliance Program on an annual basis, to test the robustness and efficiency of the AML policies, procedures and controls. The audit is performed by the Company's independent internal audit team.

The sets of tests shall include, but not be limited to:

- An evaluation of the institution's anti- money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The scope of the testing and the testing results shall be documented, with any deficiencies reported to senior management and/or the Board of Supervisory Directors, and to the



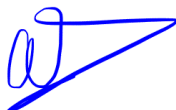
designated officers with a request to take prompt corrective actions by a certain deadline.

11. Restricted Jurisdictions

- Curaçao
- Netherlands
- France
- Belgium
- Germany
- Lithuania
- USA
- UK
- Australia
- Estonia
- Afghanistan
- North Korea
- Iran
- Syria
- Yemen
- Serbia
- Myanmar
- Ukraine
- Malta

Document Name: AML/CFT Manual – AML/CFT Policy and Procedures v2.1
Authorized By: eMagnus Curacao B.V./Andrea Engelhardt
Updated By: Nicky Degarbriele
Author: Moon Compliance Department
Date: May 2025

Signed:



5/26/2025

