

Virtual Asset Risk Management Policy

Policy No.: 001
Date of Issue: 01-11-2024
Audience:

Version Control

Name	Description
Document Name	Virtual Asset Policy
Version	1.0

Version	Description	Date
1.0	Initial Version	01-11-2024

Table of Contents

1. Rationale	4
2. Scope	4
3. Regulatory Framework	5
3.1 Regulatory Scope	5
4. Categorisation of Virtual Assets	5
5. Acceptance Policy	5
5.1 Summary	5
5.2 Authorised Currencies	6
6. Prohibited Activities	6
6.1 Mixing and Tumbling Services	6
6.2 Use of Privacy Coins	6
6.3 Blacklisted Wallets	6
6.4 Exchange Services	7
7. Rate of Exchange	7
8. Red Flags	7
9. Preventative Measures	8
9.1 Risk Mitigation Strategies	8
9.2 Key AML Safeguards	9
10. Blocking and Freezing of Accounts	10
11. Ongoing Monitoring	10
12. Suspicious Transaction Reporting	11
12.1 Submission of a STR	11
13. Dispute Resolution	11
14. Staff Training	11
15. Record Keeping	12
16. Non-Compliance	12
Appendices	13
Appendix I- Definitions	13

1. Rationale

The purpose of this Policy is to provide a consistent, proportionate and effective Risk Based Approach (“RBA”) to deter and detect Financial Crime (“FC”), by managing the risks associated with the use of Virtual Assets (“VAs”) through a framework of core compliance requirements.

In this Policy, the term FC covers the following subjects:

- Money Laundering (“ML”);
- Terrorist Financing (“TF”)
- Fraud; and,
- Sanctions.

This VA Policy should be read and implemented in conjunction with the wider Anti-Money Laundering (“AML”) Policy.

Integrating VAs for deposit or withdrawal requires a comprehensive risk assessment to identify and mitigate potential vulnerabilities. Virtual assets pose unique risks, including pseudonymity and cross-border transfer capabilities, which can facilitate money laundering and terrorism financing.

To address these risks, the Company compiled this Virtual Asset Risk Management Policy identifies high-risk jurisdictions, transactional patterns, and customer behaviors that may indicate misuse of VAs. We will deploy advanced analytics tools and external risk databases to continuously monitor these risks. Tailored controls will be implemented to mitigate identified vulnerabilities, such as setting transaction thresholds and limiting transactions involving jurisdictions flagged by the FATF or other regulatory authorities.

See Appendix I which contains a list of defined terms.

2. Scope

This Policy is mandatory for the entirety of the Company. Where the requirements of this Policy conflict with applicable local laws or regulations, the jurisdictional requirements must take precedence, and the business must record these instances in country specific variations to the AML Policy.

The Company has no appetite for being a conduit for FC. To reflect the Company's commitment and risk appetite, this Policy clearly articulates a set of standards and requirements that the business and its relevant employees and agents must comply with.

3. Regulatory Framework

3.1 Regulatory Scope

All Curaçao gambling licensees are subject to the jurisdiction's anti-money laundering and counter-terrorism financing laws. The key statutes are:

- National Ordinance on Identification when Rendering Services;
- National Ordinance on the Reporting of Unusual Transactions;
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54).

Since 2019, the GCB has been the official AML/CFT supervisor for all gambling activities in/from Curaçao. In early 2025, the CGA issued updated AML/CFT Regulations for casinos and online gaming ("Regulation"), aligning Curaçao's standards with EU and FATF recommendations.

The new rules include virtual currency transactions, which are considered a high risk factor due to their anonymity nature. As such, operators accepting cryptocurrencies are required to apply a risk-based approach with enhanced scrutiny, due diligence, and transaction monitoring. This includes documenting risk management procedures and being prepared to report any suspicious activity involving crypto assets to the Financial Intelligence Unit (FIU).

4. Categorisation of Virtual Assets

Cryptoassets include VA's that can be used as a means of payment or for other financial activity within a remote gaming operation or environment.

Not all Cryptoassets are Virtual Assets, for example, Non-Fungible Tokens ("NFTs"), such as digital collectibles, are unique assets that are distinguishable from each other and so do not have the fundamental fungible quality of various means of payment. Therefore, the Company does not accept NFTs as means of payment.

5. Acceptance Policy

5.1 Summary

The Company permits deposits and withdrawals using VA's. All withdrawal requests permitted using VA's must be made using the same VA to either the Wallet addresses that have been used by a Customer to make deposits or, where there are security concerns or other justifiable and credible reasons, to a new Wallet address that is operated by a regulated VASP.

Where the use of an alternate wallet address is used, the Company must clearly document the reasons, with clear approval from the Compliance Officer.

5.2 Authorised Currencies

BTC, BCH, ETH, LTC, USDT, DOGE

6. Prohibited Activities

6.1 Mixing and Tumbling Services

VAs, Wallets and VASPs that are known to be used for the concealment or obfuscation of identity or the Source of Funds ("SOF") (including so called mixing and tumbling services) are prohibited within the gaming ecosystem. The Company actively prevents the use of such identity and source concealment tools for remote gaming transactions and takes all the necessary measures to identify and address any attempts to circumvent transparency measures.

Measures implemented to prevent this include:

- In accordance with the AML Policy, Due Diligence Process in Three Steps, all Customers (irrelevant of whether the Customer makes fiat or VA deposits) must provide personal information such as full name, date of birth, permanent residential address, nationality, and identity number. This will ensure that no Customers are able to register with fictitious names or anonymous accounts¹.
- When depositing equal to or over 2,000 EUR (or equal to or above Naf. 4,000) or withdrawing any amount users are directed to a subpage where they must submit their unexpired, government-issued document containing photographic evidence of the customer's identity (e.g. passport, identity card) for the purpose of biometric checks by Sumsb KYC tool. Where such a document does not allow verification of the player's residential address, we will request other documents like a bank statement, utility bill, letter from a public authority or rental agreement, which should not be more than six months old to verify the residential address.
- As the use of virtual assets constitutes a high-risk factor, any customer engaging in unusual patterns of virtual asset transactions or any other high risk behaviour will be subject to a new risk assessment. Should the updated risk assessment determine that the customer presents a high-risk profile, enhanced due diligence (EDD) measures will be applied accordingly.
- Duplicate accounts will not be allowed, and checks will be made at the time of registration to ensure that Customers/Players do not have more than one account.

6.2 Use of Privacy Coins

The use of Privacy Coins that may render the Customer anonymous are strictly prohibited. They are not allowed, and the list of accepted coins doesn't have any, please see 5.2 Authorised Currencies list for reference.

6.3 Blacklisted Wallets

The Company takes a heavy stance on blacklisted wallets, whether blacklisted or sanctioned by

¹ Please note: All Customers, irrelevant of deposit method (fiat or VA) will undergo the same due diligence process. Please see the CDD Procedure that details this further.

Authorities. Our Payment provider registered VASP is responsible for this to prevent any transactions with such wallets.

6.4 Exchange Services

The Company shall not provide VA custody or exchange services to Customers and cannot enable Customers to transfer VA's directly to other players. As such, the Company will only be offering remote gaming services to Customers which can include the use of VA's to make payment for remote gaming services.

7. Rate of Exchange

Any exchange rate used for the conversion of fiat currencies, VAs' are explicitly shown on the website. The applicable fees, as charged by the VASPs, along with any additional fees related to such conversions, will also be stipulated on the website.

There will be no hidden fees or undisclosed penalties for making a conversion.

All information regarding conversion rates applicable to deposits and withdrawals will be readily available to all Customers on the website.

8. Red Flags

In accordance with the FATF Guidelines and industry best practice, the following factors may be considered red flag indicators for the risk of Money Laundering ("ML") and Terrorist Financing ("TF"):

- **Anonymiser software, IP mixers, coin mixers and anonymity enhanced VA's:** Such tooling is designed to obfuscate the origin and destination of VA's, making it difficult to trace transactions. Their use may indicate an attempt to conceal illicit activities such as ML or TF. Our registered VASP payment provider is responsible for preventing this.
- **IP does not match registration details provided:** If the IP address used for transactions or account access is from a different geographical location than the one provided in the Customer's registration details, it may suggest an attempt to hide the true location of the user, raising suspicion of fraudulent activity.
- **Significant transactions in Virtual Assets where the frequency or value is unusual:** Large or frequent transactions that deviate from the Customer's typical transaction behavior or profile may indicate suspicious activity. This could include sudden large purchases or sales of VAs that are inconsistent with the Customer's known financial situation or history.
- **Transactions involving Virtual Assets that are not plausible given the information known about the customer:** Transactions that do not align with the Customer's known income level, or stated purpose for using VAs can be a red flag. For example, a Customer with a modest income making large VA transactions without a clear SOF.

- **Source of Funds (“SOF”) or Wealth (“SOW”) is unclear or cannot be verified:** If the origin of the Customer's funds is unknown or cannot be reasonably verified, it increases the risk of those funds being derived from illegal activities. This includes situations where the Customer is unable or unwilling to provide sufficient information about how they acquired their wealth.
- **Transactions involving jurisdictions with weak AML/CFT controls:** Engaging in transactions with countries known for weak regulatory oversight or high levels of corruption can increase the risk of ML and TF.
- **Rapid movement of Value:** Quick successive transfers between different VASPs(CASPs) and Wallets, especially across different jurisdictions, may indicate layering which is a common ML technique used to obscure the origin of funds.
- **Use of anonymous payment methods for funding VA transactions:** The use of payment methods that offer anonymity can be a red flag, as they make it difficult to trace the source of funds. This is mitigated with use of registered VASP, which is not allowing anonymous payments and following Travel Rule regulations.

9. Preventative Measures

9.1 Risk Mitigation Strategies

The Company shall implement risk mitigation strategies to address the threat posed by illicit transactions and sources of funding, including:

- **Illicit Source Monitoring:** including specialised screening software designed to:
 - Monitor incoming Virtual Asset deposits for potential links to sources associated with illicit activities.
 - VASPs will be responsible for detecting illicit sources of VA funds and transactions associated with criminal activities, and appropriate measures will be taken by the Company accordingly based on the information provided.
 - Flag suspicious patterns or behaviours indicative of involvement in illicit activities.
- **SOF & SOW:** for high-value transactions, including deposits or withdrawals of equal or over EUR 50,000 (or Naf 200,000), or where there are other risk indicators, we require customers to provide evidence of the origin of their VAs (or how the value was obtained) under the EDD requirements.
- **Country Risk:** in accordance with the AML Policy, the countries in respect of which customers on boarding and transactions are prohibited and those where greater due diligence is required given the increased risks.
- **Training:** Regular training for staff on identifying and responding to illicit activity risks and the use of VAs for illicit activities. Training topics will include recognizing red flags specific to VAs, utilizing blockchain analytics tools, and understanding regulatory expectations.
- **Business Risk Assessment (“BRA”):** The Regulation requires all casinos to carry out a business risk assessment to identify the ML/TF risks they are exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. This includes analysing factors such as the types of products and services offered, transaction methods, customer demographics, and delivery channels. Recognizing that certain products or

services are inherently riskier and more attractive to criminals, especially those involving specific anonymous payment methods like VAs, are classified as high-risk factors.

- **Customer Risk Assessment (“CRA”):** At the customer level, the Company performs customer risk assessments to determine the risk profile of each customer, as required in the Regulation. This involves evaluating the customer's transaction behavior, location, and the nature of their engagement with the services. Particular scrutiny is applied to customers utilizing VAs, given the higher risk associated with such payment methods. If a customer's use of VAs exhibits unusual patterns or behaviors, a new risk assessment is initiated.
- **Regulatory Technology Mapping:** The Company also recognizes the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism. Consequently:
 - The management shall retain a close eye on technological developments that are taking place particularly in relation to phishing activity, identity fraud, money laundering etc.
 - In addition, the Company shall engage with technology partners who are at the forefront of software and IT security and are engaged to maintain the on-going integrity of the website, servers and backup.
 - The Company is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solutions.

9.2 Key AML Safeguards

Some of the key safeguards in terms of AML/CTF with the use of virtual assets include:

- **Customer Verification:** Upon reaching a transaction threshold of EUR 2,000 (or its equivalent in virtual assets), customer identification and verification will be mandatory. Deposits and withdrawals are facilitated via integration with a registered VASP. Alternatively, withdrawal funds may be sent either to the customer's wallet address as specified by the VASP, to a wallet address associated with the customer's account within the VASP platform.
- **Payments:** Fiat and VA payments shall be maintained separately and cannot be exchanged; the deposit method must be the same as the withdrawal method and the Company must also maintain logs of failed deposits and withdrawals. VA payments are only allowable on approved online betting platforms.
- **Responsible Gambling Limits:** Responsible Gambling limits are applicable regardless of whether payment is made in fiat or by a VA.
- **Transaction Monitoring:** Transaction monitoring shall be conducted on all VA transactions by registered VASP payment provider following all AML/CTF requirements. All flagged transactions will be reviewed by our compliance team to determine whether they warrant filing a Suspicious Activity Report (“SAR”).
- **Conversion Rates:** Conversion rates must be up-to-date for value-based thresholds/alerts;
- **SOW & SOF:** For transactions exceeding defined thresholds or involving high-risk factors, additional measures, including the collection of SOF and SOW information, will be mandatory. This ensures that customers' VAs are derived from legitimate sources. Wallet screening using blockchain analytics tools will also be performed by registered VASP(CASP) payment provider for crypto.
- **High Risk Customers and the Application of Enhanced Due Diligence (“EDD”):** In certain cases, highlighted by the risk assessment, the Company may consider that a Customer or

transaction poses a higher risk. In these circumstances, EDD will be requested and collected by the Company. Customers who pose an additional risk will be recorded as High risk within the administrative system and a report of their transactions and any other relevant information made available to the Compliance Officer.

10. Blocking and Freezing of Accounts

The Company will be able to immediately suspend Customer accounts so that:

- Transactions are prevented with Customers that are subject to financial sanctions or AML/CFT investigation;
- Where the risk rating of the Customer requires additional verification measures before a transaction can take place; and
- Where there is a perceived risk of unauthorized or fraudulent transactions taking place on the Customer's account.

11. Ongoing Monitoring

The Company uses registered VASP(CASP) payment provider for monitoring mechanisms to track transactions involving VA's including those conducted via VASPs(CASPs) and Self-hosted Wallets.

Any suspicious activities or transactions that raise concerns regarding the SOF or destination of funds will be promptly reported to the competent authorities.

Regular audits and reviews of VA activities involving Customers will be conducted to ensure compliance with regulatory requirements.

Further to this, The Company will maintain records of illicit activity monitoring activities and outcomes. The Compliance Officer (Money Laundering Reporting Officer ("MLRO")) shall have full access to information and records of the Company that the compliance team considers necessary to evaluate internal reports received.

If the Compliance Officer considers that there is knowledge of, suspicion or reasonable grounds to suspect money laundering or terrorist financing, the Officer is responsible for:

- Submitting the necessary information to the Financial Intelligence Unit ("FIU");
- Recording the disclosure in the register of disclosures; and,
- Dealing with subsequent production or account monitoring orders if there are any.

Furthermore, the Company takes responsibility to collaborate with law enforcement agencies and regulatory bodies in investigations related to illicit activities and transactions with the use of VAs.

12. Suspicious Transaction Reporting

The Company must be aware of its obligation (including that of its employees) to raise a Suspicious Transaction Report ("STR").

12.1 Submission of a STR

- The reasons for filing a STR, as well as the procedures for identifying, documenting, and reporting suspicious transactions, are comprehensively outlined in the company's AML policy. The policy details the criteria for suspicion, the internal escalation process, the obligations of staff to report suspicions promptly, and the formal submission process to the competent Financial Intelligence Unit (FIU) in accordance with applicable legal and regulatory requirements.

13. Dispute Resolution

Any disputes related to VA transactions will be addressed through the established dispute resolution mechanism, as detailed in Terms of Conditions.

14. Staff Training

In addition to the general AML/CTF training outlined in the company's AML Policy, specific training related to VAs shall be provided to relevant employees.

Staff involved in processing or monitoring VA transactions receive targeted instruction on:

- The specific money laundering and terrorist financing risks associated with virtual assets, including anonymity, rapid fund movement, and cross-border risks.
- Recognition of red flags such as the use of mixers, privacy coins, or chain-hopping activities.
- CDD and EDD requirements related to VA transactions, particularly upon reaching regulatory thresholds (e.g., EUR 2,000 aggregate).

AML Compliance staff receive additional training on blockchain analytics tools, suspicious transaction reporting for VAs, and emerging regulatory developments.

Supervisors, managers, and senior management are briefed on the institutional risks associated with virtual assets and their compliance oversight responsibilities.

Refresher training is provided annually or when significant changes occur.

Records are maintained on the content, attendance, dates, and results of all VA-specific training sessions.

15. Record Keeping

The Company will:

- Maintain, for at least 5 years, all necessary records on transactions, including domestic and international;
- Maintain on transactions (both domestic and international), to enable them to comply with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.; and,
- Keep records obtained through CDD including copies and records of official documentation account files and business correspondence, for at least 5 years after the business relationship has ended, or after the date of the occasional transaction.

16. Non-Compliance

If any aspect of this policy, or any of the related procedures are breached by an employee (or any individual who is subject to these policies) the incident must be reported to the MLRO and be subject to further investigation.

Appendices

Appendix I- Definitions

- **AML Policy:** the wider AML policy that is in place in respect of all customers and transactions however payment or withdrawal is made (as varied by this policy)
- **Business Risk Assessment (BRA):** A comprehensive assessment of the risks facing a business.
- **Cryptoasset:** A type of virtual asset that uses cryptography for security.
- **Customer Due Diligence (CDD):** The process of verifying a customer's identity and assessing their risk profile.
- **CDD Procedures:** the CDD policy and procedures in place for CDD and EDD requirements.
- **Enhanced Due Diligence (EDD):** Additional CDD measures applied to higher-risk customers or transactions.
- **Financial Crime (FC):** A broad term encompassing various illegal activities that involve financial systems, including money laundering, terrorist financing, and fraud.
- **Financial Intelligence Unit (FIU):** A government agency responsible for receiving, analyzing, and disseminating information about potential money laundering and terrorist financing activities.
- **Money Laundering (ML):** The process of concealing the illegal origin of money by making it appear legitimate.
- **NFTs:** Non-Fungible Tokens that do not have the features of VAs. Often used as rewards and for in-play entertainment.
- **Terrorist Financing (TF):** The process of providing funds or financial support to individuals or organizations involved in terrorist activities.
- **Privacy Coin:** A type of cryptocurrency designed to enhance anonymity and privacy.
- **Risk-Based Approach (RBA):** A methodology for identifying, assessing, and mitigating risks based on their likelihood and potential impact.
- **Sanctions:** Economic and trade restrictions imposed by governments against countries, individuals, or entities.
- **Self-Hosted Wallet:** A type of wallet where the user has sole control over the private keys and assets.
- **Source of Funds (SOF):** The origin of the value used in a transaction.
- **Source of Wealth (SOW):** Information about how a customer created wealth.
- **Suspicious Transaction Report (STR):** A report filed to the FIU to flag potential money laundering or terrorist financing activity.
- **VASP (Virtual Asset Service Provider):** A business that provides services related to virtual assets, such as exchanges, custodians, and transfer agents. Also known as **CASP (Crypto Asset Service Provider)**.
- **Virtual Asset (VA):** A digital representation of value that can be digitally traded or transferred and used for payment or investment purposes.
- **Wallet:** A digital storage mechanism for holding and managing virtual assets.