

BMbit N.V.

Anti-Money Laundering and Combating Financing of Terrorism Policy

V 5.0 Effective Date: 12.12.2025 approved by CO Derek Hendriks



Next Review Date: 12.12.2026*

*The policy shall be reviewed at least once every year or earlier, where triggered by material change (e.g. significant process/system change, or regulatory/supervisory update).

Version Control

Date	Author	Version	Description
12.01.2021	Thomas Mifsud Tommasi	1.0	Policy Updates
27.02.2022	Jean Noel Azzopardi	2.0	General Updates
10.01.2024	Jean Noel Azzopardi	3.0	General Updates
01.07.2024	Jean Noel Azzopardi	4.0	General Updates
01.09.2024	Jean Noel Azzopardi	4.1.	Details added regarding AML Screening tool to highlight the third-party tool enhanced screening process.
12.03.2025	Jean Noel Azzopardi	4.2.	General Updates
12.12.2025	Jean Noel Azzopardi	5.0	Restructured, added and amended details to meet the latest regulatory requirements: 1) Policy Statement. 2) Audience expansion: add subcontractors, suppliers, PSPs, VASPs. 3) Definitions section (AML terms, PEP, SOF, SOW, UTR, FIU, sanctions). 4) Policy Implementation section describing governance and execution. 5) Responsible Office (Compliance Department). 6) Effective Date and Next Review Date. 7) Customer Acceptance Policy (CAP) as a standalone section. 8) Identification and verification of UBO for all accounts. 9) Explicit statement: CRA performed at onboarding and during relationships. 10) Freezing & Blocking Procedure: including,

			immediate freeze when sanctions/ML suspicion, MLRO must notify FIU + CGA within 24 hours. 11) AML Program Summary section. 12) MLRO full contact details (name, email, phone). 13) Consequences of Non-Compliance section (employee + regulatory). 14) Independent audit function for AML program. 15) Third-party reliance rule: FATF-equivalence, written agreements, ongoing monitoring.
--	--	--	---

Table of Contents

1. Policy Statement.....	5
2. Purpose.....	6
3. Audience.....	7
4. Definitions.....	8
5. Policy Implementation.....	11
5.1. Business Risk Assessment.....	11
Transactional Risk.....	12
Transfer of Fund.....	12
Multiple Source of funds.....	12
Multiple accounts.....	12
Shared Platforms/Games involving multiple operators.....	12
5.2. Customer Risk Assessment.....	13
Customer & Geographical Risk.....	13
Geographical Risk management.....	13
Politically Exposed Persons.....	18
Sanctioned Countries and Individuals.....	18
High Risk Countries.....	19
Customer Behaviors.....	19
Player limits/ Tags.....	19
5.3. Customer Acceptance Policy.....	20
5.4. Customer Due diligence.....	22
5.5. Ongoing Monitoring.....	25
Customer Identity Verification.....	26
5.6. Reliance on third parties to perform CDD.....	26
5.7. Reporting of unusual transactions.....	27
5.8. Anti-Money Laundering Compliance program.....	27
6. Compliance and Consequences of Non-Compliance.....	33
7. Related Information.....	34

1. Policy Statement

BMbit N.V. (trading as Betmaster) maintains a zero-tolerance approach to the use of its products, services, platforms, payment flows, and operational infrastructure for money laundering, terrorist financing, or proliferation financing (together, “ML/TF/PF”). The Company is committed to implementing and maintaining an effective, risk-based AML/CFT/CPF compliance framework designed to prevent, detect, deter, and appropriately report ML/TF/PF risks, and to protect the integrity of the Curaçao gaming sector and the Company’s licence to operate.

This Policy applies to:

- All directors, officers, employees, and temporary staff of BMbit N.V.;
- All contractors, consultants, agents, and other persons acting on behalf of the Company (including outsourced service providers performing AML-related activities);
- All products and services offered by the Company, including all games, payment methods, customer journeys, and channels;
- All customers/players, accounts, and transactions conducted in the course of offering online games of chance under the Company’s Curaçao licensing status and any transitional or successor licensing regime under Curaçao law.

The Company will not establish or continue a customer relationship, process transactions, or permit withdrawals where required AML/CFT controls cannot be completed or maintained to the standard required by applicable law and supervisory expectations. Where grounds exist to treat activity as unusual or suspected, the Company will take proportionate risk-mitigating action (including restriction/suspension of activity, enhanced review, and escalation) and will ensure reporting obligations are met in accordance with Curaçao requirements.

2. Purpose

The purpose of this Policy is to:

- Set out the Company's minimum AML/CFT/CPF standards and governance expectations and provide clear direction on how BMbit N.V. prevents, detects, and responds to ML/TF/PF risks arising from its operations as an online gambling operator.
- Ensure compliance with Curaçao's legal and regulatory framework applicable to the gaming sector, including (as applicable) the National Ordinance on identification when rendering services (LID/NOIS) and the National Ordinance on the reporting of unusual transactions (LMOT/NORUT), together with related decrees, guidance, and supervisory requirements for gambling providers operating in and from Curaçao.
- Support compliance with the current online gaming regulatory regime under the National Ordinance on Games of Chance (LOK) and the supervisory expectations communicated by Curaçao's competent gaming authority in relation to AML/CFT obligations for the sector.
- Establish a consistent internal basis for risk-based controls, including (as further detailed in subsequent sections of the Policy) business and customer risk assessment, customer due diligence, ongoing monitoring, escalation, recordkeeping, staff training, independent testing/assurance, and reporting.
- Ensure effective identification and reporting of unusual transactions to FIU Curaçao without delay, including maintaining operational capability to report through the FIU's goAML reporting portal in line with FIU procedures.
- Protect the Company from regulatory, legal, operational, and reputational harm, including the risk of enforcement actions, financial loss, de-banking/payment-provider impacts, and adverse licensing outcomes.

3. Audience

This Policy applies to, and is binding on, the following stakeholders (together, the “Audience”), insofar as they perform activities for or on behalf of BMbit N.V. (trading as Betmaster) that may create, manage, process, approve, monitor, or report ML/TF/PF risk:

- Board of Directors and Senior Management – accountable for governance, resourcing, and oversight of the AML/CFT/CPF framework and for ensuring the Company maintains compliance with Curaçao’s AML/CFT requirements applicable to gaming operators.
- Compliance Officer / Money Laundering Reporting Officer (MLRO) – appointed by the Board as the owner of AML/CFT risk assessment, controls, policies, and procedures; empowered to act independently, with access to information and operations required to execute duties, including internal escalation handling and external reporting.
- All employees (permanent/temporary; full-time/part-time), including (without limitation) Customer Support, KYC/Onboarding, Payments, Fraud/Risk, Finance, Legal, Product, Engineering/IT, Data/Analytics, Marketing/Affiliates, and Operations – required to understand and comply with this Policy, complete role-based training, and promptly escalate relevant concerns or unusual activity through internal channels.
- Contractors and secondees performing operational work for the Company (including outsourced staff handling customers or transactions) – subject to this Policy and required to follow Company procedures and escalation protocols.
- Third-party suppliers and service providers where their services may affect AML/CFT/CPF controls, including (as applicable) KYC and PEP/sanctions screening providers, virtual asset service providers (VASPs), payment service providers (PSPs), banking partners, game/content providers, platform/hosting providers, and affiliates – required to meet contractual AML/CFT obligations and support the Company’s compliance requirements, including information-sharing and audit/cooperation obligations where applicable.
- Customers/Players – subject to customer due diligence, sanctions/PEP screening, ongoing monitoring, and related risk-mitigating actions (including restrictions or account blocking) in accordance with Curaçao’s AML/CFT framework for gambling services.

4. Definitions

Term	Definition (Policy Use)
AML/CFT/CPF	Anti-Money Laundering / Countering the Financing of Terrorism / Countering Proliferation Financing framework applied by the Company to prevent, detect, deter and report ML/TF/PF risks.
Money Laundering	Conduct intended to conceal, disguise, convert, transfer, acquire, possess, use or otherwise deal with proceeds derived from criminal activity, in a manner criminalized under applicable Curaçao law.
Terrorist Financing	The act of providing, collecting, making available or otherwise dealing with funds or other assets with the intention or knowledge that they will be used, in whole or in part, to carry out terrorist acts or support terrorists/terrorist organisations.
Proliferation Financing	The act of providing funds or financial services used, in whole or in part, for the proliferation of weapons of mass destruction, including activity connected to applicable sanctions measures.
Customer / Player	A natural or legal person to whom (or for whose benefit) the Company provides services, including participation in online games of chance or other online games.
Customer Due Diligence (CDD)	Risk-based measures to identify and verify the customer's identity (and, where applicable, beneficial owner), understand the nature and purpose of the relationship, and support ongoing monitoring.
Enhanced Due Diligence (EDD)	Additional CDD and monitoring measures applied to higher-risk customers, relationships, or transactions (e.g., PEPs, higher-risk jurisdictions, adverse media, atypical transaction behaviour).
Simplified Due Diligence (SDD)	Reduced CDD measures that may be applied only where permissible and justified by documented low risk, and never where higher risk or suspicion is present.
Ultimate Beneficial Owner (UBO)	The natural person(s) who ultimately owns or controls a legal person/arrangement, including through ownership interests or other means of control.

Politically Exposed Person (PEP)	A person who holds or has held a prominent or high-ranking public function, and (as applicable) their close family members and close associates (“connected persons”).
Sanctions	Binding restrictive measures (including asset freezes and prohibitions on making funds/economic resources available) imposed under applicable sanctions laws and implementing measures.
Sanctions Screening	Screening customers and relevant counterparties against applicable sanctions lists, with escalation and required action on a match (including restrictions/freezing where required).
Freezing of Funds / Asset Freeze	Measures that prevent the movement, transfer, alteration, use, access to, or dealing with funds/economic resources, as required by applicable sanctions measures.
Transaction	Any act or set of acts conducted by/for the customer in connection with the Company’s services, including deposits, wagering, transfers, and withdrawals.
Ongoing Monitoring	Ongoing review of customer identity information and transactional behaviour to ensure activity is consistent with the customer risk profile and expected pattern, and to detect unusual or suspicious activity.
Risk-Based Approach	The principle that AML/CFT controls are designed and applied proportionate to identified ML/TF/PF risks, supported by business and customer risk assessments.
Business Risk Assessment (BRA)	Assessment of the ML/TF/PF risks inherent in the Company’s products, services, delivery channels, geographies, payment methods and operating model, used to design adequate controls.
Customer Risk Assessment (CRA)	Assessment of ML/TF/PF risk posed by a specific customer at onboarding and throughout the relationship, used to determine risk rating and applicable CDD/EDD and monitoring.
Customer Acceptance Policy (CAP)	The Company’s rules for accepting/declining customers and applying appropriate levels of CDD/EDD based on the CRA, including requirements for PEP and sanctions screening.
Unusual Transaction	A transaction that meets one or more legally established indicators for unusual transactions and is subject to reporting to FIU Curaçao in accordance with the reporting ordinance.

Unusual Transaction Report (UTR)	A report of an unusual (including intended) transaction filed with FIU Curaçao via the prescribed mechanism (goAML) in line with legal requirements and FIU procedures.
Financial Intelligence Unit Curaçao (FIU)	The Curaçao authority that receives unusual transaction reports and performs FIU functions under the reporting framework.
goAML	The portal/system used for submitting unusual transaction reports to FIU Curaçao (in use for reporting since 1 January 2021).
Tipping-Off	Prohibited disclosure that could alert a customer or third party that an unusual transaction report, investigation, or related escalation has been made or is contemplated, except where permitted by law.
Account Restriction / Blocking	Risk-mitigating controls that limit deposits, wagering, withdrawals or account access pending completion of CDD/EDD, resolution of screening concerns, or investigation outcomes, applied consistently and mindful of tipping-off constraints.
Reporting Entity	An entity required by Curaçao law to report unusual transactions to FIU Curaçao.
Source of Funds (SoF)	The origin of the funds involved in a business relationship or occasional transaction. This includes the activity that generated the funds used (e.g., salary, business income, sale of an asset, inheritance).
Source of Wealth (SoW)	The origin of the customer's total wealth (overall net worth) and how it was accumulated over time (e.g., employment/business income, investments, inheritance, sale of assets).

5. Policy Implementation

The Compliance Department, led by the Compliance Officer/MLRO, is the Responsible Office for:

- dissemination of this Policy and supporting procedures to all in-scope personnel and relevant third parties;
- maintaining document control (versioning, approvals, distribution lists, repository access);
- coordinating periodic reviews and policy updates (including regulatory-change implementation); and
- overseeing execution of the AML/CFT/CFP program across the first and second lines of defense, including reporting to Senior Management and the Board as required.

MLRO Contact Details:

Name: Jean Noel Azzopardi

Email: j.azzopardi@betmaster.com

5.1. Business Risk Assessment

The company regularly conducts a risk assessment to

- a) Identify ML/FT Vulnerabilities;
- b) Identify ML/FT Threats;
- c) Identify ML/FT consequences/ impact;
- d) Identify any new requirements;

This assessment is conducted at least annually, and also earlier where there are material changes which may affect the risk exposure. The internal teams investigate this assessment, which typically includes, but is not limited to:

- a) Customer base;
- b) The countries which the company operates in;
- c) The products or services offered;
- d) Transactions;
- e) Delivery channels

Dependent on the outcome of the risk assessment and should it be deemed necessary to minimize risk exposure identified the following controls are revisited and amended accordingly:

- a) Measures;
- b) Policies;
- c) Controls;
- d) Procedures.

The overall risk assessment is updated whenever significant changes to the company's systems, processes or overall operations are going to be affected, for example an integration of a new payment provider, releasing of a new product/vertical, launching of a new jurisdiction, etc. Updates of the risk assessments also occur due to external influences such as changes in legislation and regulatory communications or publication of guidance by relevant authorities.

The risk assessments and all related measures, policies, controls, procedures, etc. are documented, approved by the Board of directors and stored by the company and are readily available for review by any appropriate regulatory bodies when required.

Transactional Risk

Transfer of Fund

Transfer of funds between customers is not permitted and there is no facility that would enable this to occur.

Multiple Source of funds

Usage of multiple payment methods at any one time represents a risk. Hard coded restrictions and limitations are currently in place to ensure risk exposure is minimized at any given point in time.

Multiple accounts

Internal controls are in place to restrict the use of multiple accounts.

Shared Platforms/Games involving multiple operators

While the company makes use of B2B game providers/platforms which are used by other operators there is no possibility of customers transacting with each other across platforms. Peer 2 peer gaming is not offered fully mitigating risk such as chip dumping and other forms of collusion.

Product Risk

The product or service that a customer chooses is an important factor in risk assessment and is therefore clearly documented within the due diligence performed.

The AML team regularly examines the customer's background using open sources and other tools to substantiate the investigation conducted into complex, inconstant and large transactions when compared to the customer's past activities in determining the likelihood of money laundering.

Appropriate records are securely kept at important stages of the customer's ongoing monitoring to ensure that significant events in the customer's relationship are properly informing the risk assessment conducted. All relevant information is stored within the customer due diligence documentation held on individual customers.

The product or service used by the customer will be reviewed from an AML perspective in conjunction with other risk factors to form an assessment of the overall risk level. Within the review and investigation conducted the company will pursue to make use of all software and tools at its disposal such as game providers and payment bank offices to fully investigate the transactions executed.

The company shall not introduce any product, service, business practice, or technology which poses a significant risk of money laundering. Whenever a risk is identified through the risk assessment processes, this will be appropriately mitigated before the new product, service, business practice is released or integrated.

5.2. Customer Risk Assessment

The customer risk assessment is performed at onboarding and throughout the entire business relationship based on the following areas, which are reviewed in conjunction with several risk factors, including but not limited to:

Customer & Geographical Risk

Geographical Risk management

This is the risk posed by the geographical location of the customers, however also the geographical locations of its suppliers and service providers. The element to be considered in respect of this fraud management procedure is primarily that attributable to the customers and the source of funds of the said customers. The entered country and/or IP address of a customer should be considered as these might be indicative of a heightened geographical risk. Countries that have a weak anti-

money laundering and counterfeit terrorism system, countries known to suffer from a significant level of corruption, and countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction will be considered as high risk.

The Company uses information on www.knowyourcountry.com for deciding regarding the geographical risk of each registered customer. The Basel AML Index and the FATF High Risk & Other Monitored Jurisdictions publications may also be considered when assessing the geographical risk.

Risk assessments are 'works in progress'. Such assessments are to be constantly re-evaluated as new risks emerge. Risks may emerge due to changes in technology, which may render money laundering, or the funding of terrorism attempts easier to carry out.

Other changes include the widening of the customer-base or the addition of games and payment methods which present a different risk profile from those already offered, which will thus require a revision of the business risk assessment.

In the absence of any such changes, BMbit N.V. will re-assess its business risk assessment at least once a year, to evaluate whether any changes thereto are necessary. In determining the level of risk posed by a customer, the accumulation of all of the relevant indicators will be taken into consideration.

To deal with the different risks and different states of wealth in different regions on the earth, BMbit N.V. categorizes every country in two different regions of risk - low and high.

Region one: Low risk countries

For each person from such a country the regular three-step due diligence process is applied, with thresholds for deposits and withdrawals checks are triggered after completing deposits or withdrawals equaling to or surpassing EUR 2,000 (or equaling to or surpassing Naf. 4,000)) within any given period. Step Three will be executed once deposits or withdrawals are equaling to or surpassing EUR 50,000 (or equaling to or surpassing Naf. 100,000) in any period.

Region two: High risk countries

High-risk countries are those, which are not Low risk countries. These are the countries according to the "FATF list of High - Risk Jurisdictions subject to a Call for Action" and the persons with nationality, residence or place of birth in these countries are excluded

from doing business with the company. These designations are regularly monitored and updated by the company.

Due Diligence Process in Three Steps

Step One Identification

Every user and customer are required to complete Step One Identification before making any withdrawals. This applies regardless of the chosen payment method, payment amount, withdrawal amount, withdrawal method, or the user/customer's nationality. Step One Identification involves filling out a form containing personal information such as full name, date of birth, permanent residential address, nationality, and identity number. By performing this identification, and given the nature of the company's services, the Ultimate Beneficial Owner as well as the purpose of the business transaction are settled by these factors. The customer is the UBO, and the nature of the business transaction is their participation in online gambling games offered by the company.

Step Two Verification

Verification service provider: Sumsub

Users depositing equal to or over 2,000 EUR (or equal to or above Naf. 4,000) or withdrawing any amount must undergo Step Two Verification. Withdrawals or deposits will be held until this verification is completed. During Step Two Verification, 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 Sumsub 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.

Only official IDs are accepted, and the electronic check ensures the accuracy of information provided in Step One Identification. If the electronic check fails, users must provide a confirmation of their current residence, such as a government-issued certificate of registration.

Step Three Due Diligence

Users making deposits or withdrawals equal to or exceeding EUR 50,000 (or equal to or above Naf. 100,000) in any period must undergo Step Three Due Diligence. Withdrawals or deposits will be held until this verification is completed. Step Three Due Diligence requires users to provide a source of wealth.

The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. In identifying the level of risk inherent in a relationship, BMbit N.V. will be assessing what would be the likelihood that a customer would be able to launder proceeds of crime through the Company's service. A high earning customer who spends a fourth of his monthly wage in wagering is not likely to constitute a high risk, even if the amount being wagered is large. On the other hand, a minimum wage earner who spends his only wage on wagering will more likely constitute a high risk.

Furthermore, the individual will be screened to determine whether he is a politically exposed person (PEP), or in any way associated to a PEP, which would be classified as high risk. Checks would also be carried out to ensure that the individual is not subject to any sanctions or other statutory measures.

Comply Advantage is Sumsub's watchlist screening provider. It offers real-time sanctions and watchlist screening by accessing global lists, governmental, law enforcement, and regulatory databases.

Each customer undergoes AML screening at registration and the relevant AML employees are alerted about any detected warnings listed below:

Warning types

- ☒ Sanctions, Warnings and Fitness & Probity
 - ☒ Sanctions
 - OFAC, Local sanctions lists
 - ☒ Warnings
 - Wanted persons lists, disqualified directors etc.
 - ☒ Wanted fitness & Probity
 - e.g. US System for Award management exclusions
- ☒ Politically Exposed Persons
 - ☒ Heads of State, National Parliaments, National governments (PEP Class 1)
 - ☒ Regional governments, Regional parliaments (PEP Class 2)
 - ☒ Senior management & Board of SOEs (PEP Class 3)
 - ☒ Mayors and members of local city councils (PEP Class 4)
 - ☒ Unclassified PEP (Also initiates search for all PEP classes above)

Additionally, also adverse media search is performed taking into consideration a wide variety of FATF & EU AML Directive 22 predicate offences, such as:

- Fraud-linked (eg. forgery, identity theft)
- Financial (eg. Insider trading, tax-related smuggling)
- Narcotics (eg. drug trafficking or distribution)
- Violence (eg. people/ sex/organ trafficking)
- Terrorism (eg. terror/terrorist financing; member of a terrorist organization)
- Cybercrime (eg. Illegal access to information systems)
- Regulatory (eg. product dumping, collusion),
- Other (eg. drug possession)
- general (eg. Organized crime, corruption)

To sum up, the watchlist screening helps find applicants that are:

- Known or suspected terrorists,
- Sanctioned persons,
- Politically exposed persons (PEPs),
- Persons with criminal background,

-Persons mentioned in adverse media.

Politically Exposed Persons

Politically Exposed Persons (PEPs) including family members and/or close associates of PEPs, shall not be accepted as customers by the company unless Board of Directors' approval has been obtained and enhanced due diligence is carried out. Such customers shall be specifically identified, subject to enhanced ongoing monitoring, and will need to mandate source of funds/ wealth verification on all transactions executed on the customer account.

Where a PEP or a close associate of a PEP is accepted by the company, enhanced due diligence will continue for a minimum period of 12 months following the PEP ceases to hold a prominent public function.

Sanctioned Countries and Individuals

The data within the currently used third-party service provider is derived from information on sanctions watch or regulatory and law enforcement lists. This includes all major international and national lists published by governments and independent, nongovernmental organizations (OFAC, UN, HMT, EU, DFAT and many more lists from around the world including U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List Specially Designated Nationals and Blocked Persons and EU Sanctions List).

The information is updated daily.

If Curaçao publishes a local list with designated persons and organizations, the Company that local list is considered.

The data consists of PEP information, as well as information about individuals and entities not found on official lists but who instead are reported to be connected to sanctioned parties or reported to have been investigated for, or convicted of engaging in, financial crime, slavery, and human abuse-related activities (SIP and SIE). Comply Advantage also forms profiles with unfavorable information (risk data) on public and private entities. The information is found in adverse media, or negative news: these are both 'traditional' news outlets, niche media organizations, government and regulatory press releases, and reliable blogs.

The Company check for amendments of Sanctions Decrees and Regulations on a regular basis and updates policies and procedures accordingly to reflect

such amendments.

Individuals whose name is included in any Financial Sanctions lists compiled, including the United Nations, European Union, and Curacao are not accepted as customers. Whenever a customer has been accepted and subsequently appears within the sanction list, the account will be immediately closed and an internal suspicious report escalated to the MLRO in line with the suspicious transaction report procedure.

High Risk Countries

Where we identify that a person was born/ originates from a country that is considered as high risk of money laundering or financing of terrorism as indicated by the Financial Action Task Force (FATF) such a customer would not be allowed to open a gambling account.

Should a customer be found to have used a VPN connection to circumvent any of the geographical risk controls, committing fraud or disguise the true nature of their business relationship the account should be escalated for a review by the MLRO.

Customers who have recently requested to or proceeded to change their address, identity verification shall be required to provide new identity documents and address verification. Only upon successful verification of the newly obtained documentation will that customer be allowed to continue to transact.

Customer Behaviors

The following potential high-risk behaviors will be subject to a new risk assessment while applying a risk-based approach is these reviews:

- a) Changing or unusual spending patterns (including unusual transactions- either single or a series, combination or pattern of transactions involving a total amount more than the monetary equivalent of NAf. 4,000)
- b) Regularly changing address/account information
- c) High spenders
- d) Disproportionate spending

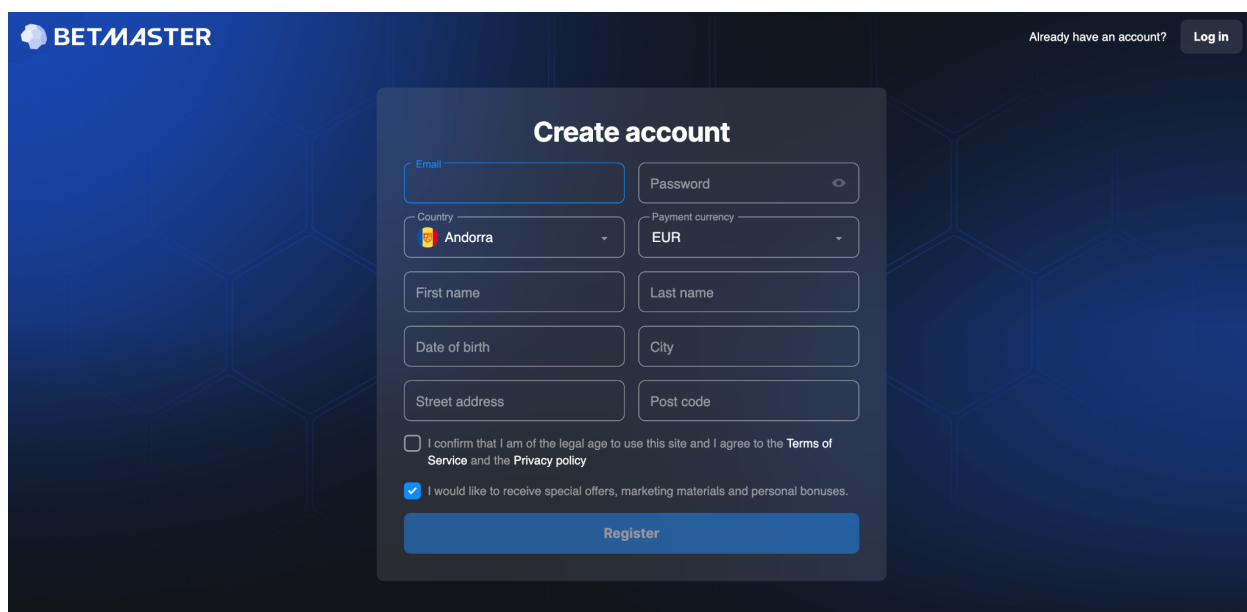
Player limits/ Tags

Tags are applied on individual customer profiles to enhance reporting capabilities or to impose conditions or limitations on specific accounts and groups of customers.

5.3. Customer Acceptance Policy

The Company's services are available only to customers located in jurisdictions where online gambling, including casino games and betting, is legally permitted. It is the responsibility of the customer to ensure that their participation in our services complies with the laws and regulations of their local jurisdiction. The Company does not accept customers from jurisdictions where online gambling is prohibited. The business activities offered by the Company include casino games such as slots, blackjack, roulette, poker, and other table games, as well as sports and event betting.

Before registering an account with the Company, the client must accept the Terms and Conditions, confirming that they are not prohibited from using the Company's services. At the registration stage, this verification is fully automated. We technically check the client's age, restrictions, and run AML, PEP, and sanctions alerts. If our internal system flags an issue with a client, we will respond accordingly and, based on the results of the investigation, decide whether to open or close the account. AML-related triggers are handled by the Compliance Team, while triggers related to age or gambling restrictions fall under the responsibility of Customer Support. **It is important to note that any decisions made by Customer Support must be approved by the Chief Customer & Operations Officer.**



The screenshot displays the 'Create account' registration form on the BETMASTER website. The form is centered on a dark blue background with a hexagonal pattern. At the top left is the BETMASTER logo, and at the top right is a link for users who 'Already have an account?' with a 'Log in' button. The form itself contains the following fields and options:

- Email**: A text input field.
- Password**: A text input field with a toggle icon for visibility.
- Country**: A dropdown menu currently showing 'Andorra' with a flag icon.
- Payment currency**: A dropdown menu currently showing 'EUR'.
- First name**: A text input field.
- Last name**: A text input field.
- Date of birth**: A text input field.
- City**: A text input field.
- Street address**: A text input field.
- Post code**: A text input field.
- Terms and Conditions**: A checkbox with the text 'I confirm that I am of the legal age to use this site and I agree to the Terms of Service and the Privacy policy'.
- Marketing Opt-in**: A checked checkbox with the text 'I would like to receive special offers, marketing materials and personal bonuses.'
- Register**: A prominent blue button at the bottom of the form.

In order for the Clients to utilize the services of the Company, the Clients must represent and warrant that:

- e) They are a natural person;
- f) They have carefully read and understood all the provisions of this Agreement and other documents published on the Website;
- g) They are over 18 years of age or of the legal age allowed to gamble in the respective jurisdiction, whichever is higher;
- h) They are not restricted by limited legal capacity;
- i) They are not acting on behalf of another party;
- j) They are not a compulsive player;
- k) They have not added themselves to the list that defines gambling restrictions for them as individuals;
- l) Only they have access to and are using the Personal Account;
- m) They have provided all necessary, accurate, and true information and materials at the Company's request;
- n) Their personal details are correct and updated in case of any change such as, for example, surname change due to marriage;
- o) Their residence address is current and updated in case of move;
- p) They are not depositing money originating from criminal and/or other unauthorized activities into their Personal Account;
- q) They are not conducting criminal activities, directly or indirectly, in relation to their Personal Account;
- r) They will inform the Company immediately if they are or become a politically exposed person (PEP) and agree to undergo enhanced due diligence procedures by the Company;
- s) They are not participants in the Matches for the Events on which they place Bets, as defined in the product rules;
- t) They accept that they are responsible at all times for ensuring the legality of using or registering for the Company services in the country or region where they are located. If they are living or residing in a country where remote gambling is forbidden, they are not allowed to use the Company's services, nor are they allowed to use VPNs or any other technical measures to circumvent any blocks installed by the Company in their location in order to access the Company's services.

during their registration process on the Company's platform through reading and consenting to the terms and conditions of the Company.

In order for the Company to ensure compliance with the warranties highlighted above, the Company requires from the Clients to register with the Company with their name, date of birth, and address.

After the customer's personal details are entered and confirmed, the company will conduct a screening by SUMSUB based on the name provided by the customer. If a positive alert is triggered, the AML team will initiate an investigation, which will require the customer to provide due diligence documents. If the investigation concludes that the alert was false, the customer may continue using the company's services. However, if the investigation confirms the alert, the customer's account will be blocked, and they will no longer be able to access the company's services.

If the documents submitted by the customer reveals to the Company the fact that the Client is unable to fulfill any of the warranties mentioned above, the Client will be denied access to the services of the Company and depending on the warranty that the Client has failed to fulfill, will further report it to the relevant authorities in case the law prescribes the Company to do so (for example in case of registration by a sanctioned person).

The Company does regular due diligence checks on the Clients at different points in time after the registration to ensure that the warranties made above stand to be true after the passage of time.

5.4. Customer Due diligence

The customer due diligence Procedure defines the process carried out to conduct customer due diligence (CDD) and outline the requirements needed to undergo enhanced due diligence (EDD). Customers rated as high risk will automatically require enhanced due diligence (EDD) to be performed.

Due diligence documentation is created, updated and enhanced over the course of the business relationship, taking a risk-based approach in line with the operational resources which shall reflect the established policies and procedures.

The formal identification of customers on entry into commercial relations is a vital element, both for the regulations relating to money laundering and for the KYC policy.

The customer due diligence relies on the following fundamental principles:

- A copy of the customer's passport, ID card or driving license.
- An employee may do additional checks, if necessary, based on the situation.

Proof of Address

Proof of address is done via electronic checks, which use two different databases. If an electronic test fails, the user/customer has the option to make a manual proof.

A recent utility bill sent to the customer's registered address, issued within the last 6 months or an official document made by the government that proves the address of residence.

For example: An electricity bill, water bill, bank statement or any governmental post addressed to customer.

An employee may do additional checks, if necessary, based on the situation.

Source of Wealth

If a player makes deposits or withdrawals of equal or over EUR 50,000 (or Naf 200,000) in any period, there is a process of understanding the source of wealth (SOW).

Examples of SOW are:

- Ownership of business
- Employment
- Inheritance
- Investment
- Family

It is critical that the origin and legitimacy of that wealth is clearly understood. If this is not possible, an employee may ask for an additional document or proof.

The account will be frozen if the same user deposits either this amount in one go or multiple transactions which amount to this. An email will be sent to them manually to go through the above and the information on the website itself.

BMbit N.V. also asks for a bank wire/bank card to further ensure the identity of the user/customer. It also gives additional information about the financial situation of the user/customer.

Basic information for registration

The basic information will be accessible via the settings page on BMbit N.V. Every user must fill out the following information:

- First name
- Second name
- Nationality

- Gender
- Date of Birth

High risk is defined by the Business Risk Assessment, referenced on page 8 of this document, as adjusted based on external/market changes deemed such changes to be necessary.

High risk customers may warrant Senior Management review, this should be determined while applying a risk-based approach, however the following scenarios should always be escalated:

Customer who originates from a high-risk country

- a) Customer who originates from a high-risk country
- b) Politically Exposed Persons
- c) Customer who has a high velocity of spend
- d) Customers who for any reason are identified by the operations teams as posing an additional risk to the company or in any way raise suspicion of the individual or their activity.

Where Senior management review has taken place, any decision made in relation to the business relationship, including guidance provided and the rationale should be documented and maintained by the operational teams.

Whenever public or 'open' sources are used to verify customer information, these are used to validate evidence received by the customer and should not be used as the primary source of information collected as standard practice. Only in exceptional circumstances open-source information may be permitted for verification and subject to approval by Senior Management.

Depending on the customer's risk profile, customers who have been requested to complete any CDD/EDD measure may have their account restricted during this period. When a customer is requested to complete EDD, withdrawals will be suspended, and funds will be retained on the gambling account in all cases.

Should the CDD/EDD requests not be successfully completed within thirty (30) days of such a request, the customer's account shall be considered to have failed completing CDD/EDD and thus will be closed accordingly. The raising of a Suspicious Transaction Report (STR) will be considered. Such a decision is taken and recorded by the MLRO.

Unless a STR has been raised and consent sought to affect a transaction/ clearing off an available balance, deposited funds still present on the customer's account will be returned to the deposit method where possible.

5.5. Ongoing Monitoring

AML-Compliance ensures that an "ongoing transaction monitoring" is conducted to detect transactions which are unusual or suspicious compared to the customer profile.

This transaction monitoring is conducted on two levels:

1) The first Line of Defense

BMbit N.V. works solely with trusted Payment Service Providers who all have effective AML policies (and relevant authorizations or licenses in the given jurisdiction) in place to prevent most suspicious deposits onto BMbit N.V. from taking place without proper execution of KYC procedures onto the potential customer.

2) The second Line of Defense:

BMbit N.V. makes its network aware so that any contact with the customer or player or authorized representative must give rise to the exercise of due diligence on transactions on the account concerned. These include:

- Requests for the execution of financial transactions on the account;
- Requests in relation to means of payment or services on the account;

Also, the three-step due diligence with adjusted risk management should provide all necessary information about all customers of BMbit N.V. at all times.

All transactions must be monitored by employees under the supervision of the AML compliance officer, who is ultimately overseen by senior management.

The specific transactions submitted to the customer support manager, possibly through their Compliance Manager must also be subject to due diligence.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to the knowledge of the customer (KYC), their financial behavior and the transaction counterparty. These checks will be done by an automated System, while an Employee cross checks them for additional security.

The transactions observed on customer accounts for which it is difficult to gain a proper understanding of the lawful activities and origin of funds must therefore rapidly be considered atypical (as they are not directly justifiable).

Any BMbit N.V. staff member must inform the AML division of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known to the customer.

3) The third Line of Defense:

As a last line of defense against AML, BMbit N.V. will do manual checks on all suspicious and higher risk users to fully prevent money laundering. If fraud or Money Laundering is found the authorities will be informed.

Customer Identity Verification

To ensure that the information held on customers remains accurate and up to date new documentation is requested prior to the recorded expiry date. If the updated details do not satisfy our checks, the account will be locked until sufficient evidence can be obtained that will fully verify the updated details.

The ongoing monitoring conducted on customers will also consider any extraordinary circumstances or unprecedented events such as the COVID-19 global pandemic which will require additional interaction with customers to mitigate heightened AML concerns where identified. Individuals that have been previously verified may be subject to employment disruptions (furloughed, loss of business, temporary/ permanent loss of employment). Revised operational procedures will require escalations to be made that will ensure appropriate decision-making in such situations.

5.6. Reliance on third parties to perform CDD

BMbit N.V. may use third-party providers to perform specific elements of the CDD control environment (e.g., identity verification tooling, sanctions/PEP screening tooling, PSP controls). However, the Company remains ultimately responsible for AML/CFT compliance and for ensuring these controls meet Curaçao requirements.

Minimum third-party governance requirements:

- documented due diligence before onboarding (capability, controls, data security, audit rights);
- contractual requirements (service levels, incident notification, audit/inspection support, data retention);
- ongoing performance oversight and periodic reassessment.
- where agents/affiliates perform onboarding or customer interaction, the Company ensures the same AML checks apply; activities by an agent/group company are treated as activity performed by the operator for responsibility purposes.

5.7. Reporting of unusual transactions

The Company maintains procedures to ensure the recognition, documentation, and reporting of unusual transactions (intended or completed), including staff training and internal escalation to the MLRO in a management-approved format with supporting documents.

Internal escalation:

- all staff must escalate unusual or suspicious activity promptly to the MLRO;
- documentation must include relevant account history, CDD data, transaction evidence, and the rationale for concern;
- strict confidentiality applies (anti-tipping-off).

External reporting to FIU Curaçao (goAML):

- unusual transactions must be reported to FIU Curaçao without delay in accordance with the reporting ordinance and indicators framework;
- external reporting is submitted through the FIU's goAML portal (registration required), and the FIU reporting process is conducted via that portal.
- reporting is prepared by the MLRO and includes supporting documentation, in the format/language required by FIU procedures.

5.8. Anti-Money Laundering Compliance Program

BMbit N.V. maintains a documented, risk-based AML/CFT/CFP compliance program designed to prevent, detect, deter, and report money laundering, terrorist financing, and proliferation financing risks arising from its online gambling operations. The program establishes minimum, organisation-wide standards reasonably designed to ensure compliance with Curaçao's applicable AML/CFT legal framework and the AML/CFT/CFP regulations and supervisory expectations for the gaming sector.

5.8.1. Core program components (minimum standards)

The AML compliance program includes, at a minimum, the following elements:

Internal policies, procedures, and controls

- Written policies and legal/regulatory obligations into workable operational controls.
- Internal controls enabling the MLRO/Compliance function to identify deviations from expected procedures and risk tolerances.

- A documented process to track and implement regulatory changes and update the program accordingly.
- Board/Senior Management approval and dissemination to employees.

Designated Compliance Officer / MLRO with independence and access

A senior officer independent from gaming operations, with timely access to customer identification/C DD data, transaction records, and other relevant information, and authority to act independently.

MLRO responsibilities include (among others) designing/maintaining the AML program; ensuring adherence to Curaçao requirements; analysing and escalating transactions against the indicators framework; maintaining records; and ensuring external reporting is completed.

Employee training

BMbit N.V. employees make manual controls on a risk-based approval for which they get special training.

The training and awareness program is reflected by its usage:

- A mandatory AML training program in accordance with the latest regulatory evolutions, for all in touch with finances
- AML learning sessions for all new employees

The content of this training program is established in accordance with the kind of business the trainees are working for and the posts they hold. These sessions are given by an AML-specialist working in the company's AML team.

The company's prospective employees that are to be involved with or connected to activities that would fall within the scope of this policy, are screened before the beginning of their employment to ensure that they are fit and proper to occupy positions in which they will participate in the provision of services to the customer.

Due diligence documentation and where needed, the use of third-party screening providers may be engaged to ensure the suitability of prospective employees.

The company conducts restricted and privacy-sensitive monitoring of the activities of its employees during their employment to identify concerns of internal fraud or other criminal activity potentially affecting the company's operations.

Employees are also encouraged to report internal suspicious or fraudulent behavior to

the MLRO and or Directors directly and should they wish to remain anonymous to do this via an anonymous letter or email to the MLRO containing as many facts and information as possible.

The AML program is monitored and evaluated at least annually by an adequately resourced internal audit function or an independent external party, with documented findings and remediation tracking to completion.

5.8.2. Risk-Based Controls

The program is implemented using a risk-based approach informed by the Business Risk Assessment (BRA) and Customer Risk Assessment (CRA), and is supported by controlled procedures covering at least:

- Customer Acceptance Policy (CAP) and risk rating;
- CDD/EDD (including the Company's step-based CDD approach and threshold/risk triggers, and collection of source of wealth/funds where required);
- sanctions and PEP screening;
- ongoing monitoring and alert handling;
- recordkeeping and data protection; and
- unusual transaction reporting and MLRO escalation workflows.

5.8.3. Account blocking/freezing based on suspicion

BMbit N.V. maintains a documented internal procedure defining when and how account restrictions, blocking, and (where applicable) freezing actions are applied in response to ML/TF/PF concerns, including the circumstances in which reporting of unusual transactions leads to blocking/freezing of user accounts.

Triggers (non-exhaustive):

- failure or refusal to complete required CDD/EDD within the prescribed timeframe (including inability to verify identity/address or provide required SoW/SoF);
- suspicion or reasonable grounds to suspect ML/TF/PF based on monitoring, behavioural indicators, structuring, unusual patterns, or adverse information;
- confirmed or unresolved sanctions screening match, requiring restrictions and potential freezing;
- evidence of circumvention of geographic controls (e.g., VPN/proxy use) where linked to fraud/ML typologies;
- law-enforcement requests or other credible intelligence that elevates ML/TF risk.

The MLRO has primary authority to determine restrictions/blocking actions, escalate for Senior Management/Board involvement where required by the CAP (e.g., exceptional high-risk approvals), and ensure decisions are documented with rationale.

Controls applied (as appropriate to the risk):

- restriction of deposits, wagering, and/or withdrawals;
- account locking pending investigation outcomes;
- termination of the relationship where risk cannot be mitigated;
- freezing of funds/economic resources where required under targeted financial sanctions obligations (including ensuring sanctioned persons cannot withdraw).

Staff must escalate concerns immediately to the MLRO; tipping-off is prohibited. Where an activity meets the indicators for unusual transactions, sanctions and ML suspicion, the MLRO must notify FIU and CGA within 24 hours.

Police Requests

We may be contacted by police from certain jurisdictions to request information on a customer. Any requests concerning criminal matters and stemming from a foreign entity must be following mutual legal assistance regulation and should be sent to the company. The company shall then have no issue with passing on the requested information, if it is not subject to other special consideration.

Each Police request shall trigger a customer assessment, and should the profile demonstrate ML/FT concerns, an internal suspicious transaction report will be drafted in accordance with the 'Internal Suspicious Transaction Report Procedure'.

Role of the Compliance Officer/MLRO

The Compliance Officer (hereinafter also as Money Laundering Reporting Officer; MLRO) role is appointed by the Board of Directors to be the business owner of AML/CFT Risk Assessment, Controls, Policies and Procedures.

The appointed MLRO possesses professional experience, training and resources to carry out his/her appointment as per the National Ordinance on Identification when rendering Services (NOIS), the National Ordinance on the Reporting Unusual Transactions (NORUT), the Sanction National Ordinance, the Kingdom Sanction Act and the GCB Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, applicable for Curaçao

casinos and providers of other online games, under the Curaçao jurisdiction.

The MLRO answers directly to the Board of Directors but has the authority to act independently in carrying out his responsibilities, free to have unhindered access to the relevant gambling operations, liaise with law enforcement agencies on any questions of whether to proceed with a transaction and obtaining appropriate defense of appropriate consent.

The MLRO responsibilities include but are not limited to:

- Design and implementation of the company's AML program and making necessary changes to the AML program;
- Verification of the adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- The review of compliance with the company's policies and procedures;
- Organization of the training sessions for the staff on various compliance-related issues;
- Analysis of the transactions and verification whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- Review of all internally reported unusual transactions for their completeness and accuracy with other sources;
- Keeping of the records of internally and externally reported unusual transactions;
- Execution of the closer investigation of unusual transactions if necessary;
- Preparation of the external report of unusual transactions;
- Remaining informed on the local and international developments on money laundering and terrorist financing and making suggestions to senior management and Board of Directors for improvements;
- Preparation of periodic information on the company's efforts against money laundering and financing of terrorism and financing of proliferation;
- Customer Risk Assessment (CRA) procedures and Customer Acceptance Policy (CAP) Risk assessment and risk management.

5.8.4. Documentation and Recordkeeping

Record shall be generated for the purpose of but not limited to:

- a) This AML policy and compliance guides used as a basis for internal procedures
- b) AML Training
- c) All investigations related to potential STRs
- d) Details of monitoring by the MLRO and any delegation of duties by the MLRO
- e) MLRO reporting to senior management

- f) Internal and external escalations of suspicious transaction reporting
- g) Correspondence between MLRO and law enforcement, FIU, etc.
- h) Correspondence with police agencies
- i) Internal reports not acted upon by the MLRO, stating why no further action was taken

Records of data obtained for the purpose of identification are kept for at least five years after the business relationship has ended.

Records of all transaction data are kept for at least five years following the carrying out of the transactions or the end of the business relationship. This data is safely, encrypted, stored offline and online.

5.8.5. Independent Audit

BMbit N.V. maintains an independent testing function for the AML/CFT/CFP program. The Company may carry out an internal audit regime (or appoint an independent external reviewer where appropriate) to test the effectiveness of the implementation of this Policy and supporting procedures within the applicable entity and, where relevant, across the group.

The independent audit/testing framework includes:

- a risk-based audit plan;
- testing of design and operating effectiveness of key controls (BRA/CRA/CAP, CDD/EDD, sanctions/PEP screening, ongoing monitoring, reporting, recordkeeping, and governance/MLRO independence);
- documented findings and recommendations in a formal report presented to Senior Management; and
- any action point derived from the assessment will be promptly implemented where feasible, or a documented action plan will be established (owners, timelines, dependencies, validation testing), reflecting development/capacity constraints.

6. Compliance and Consequences of Non-Compliance

All in-scope persons (employees, contractors, and relevant third parties acting for or on behalf of BMbit N.V.) must:

- comply with this AML/CFT/CFP Policy and all supporting procedures (BRA/CRA/CAP, CDD/EDD, sanctions/PEP screening, monitoring, recordkeeping, and reporting);
- complete assigned AML training and apply a risk-based approach in day-to-day decision-making;
- promptly escalate atypical/unusual activity and all suspicion of ML/TF/PF to the MLRO through the internal escalation process; and
- maintain strict confidentiality and avoid tipping-off in relation to internal investigations and FIU reporting.

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 and may result in one or more of the following:

- mandatory remediation measures (retraining, coaching, supervised work, removal of decisioning authority, access restrictions);
- formal performance management (written warnings, final warnings);
- suspension or reassignment;
- termination of employment for serious or repeated breaches; and/or
- termination of contractor/vendor agreements, including exercise of audit rights, remediation demands, and indemnification or damages claims where contractually available;
- regulatory findings, directives, or sanctions by the Curaçao Gaming Authority (CGA), including outcomes affecting licensing status, supervisory standing, or the ability to operate (CGA is the online gaming regulator under the LOK framework and AML/CFT supervisor for gambling in/from Curaçao).
- financial losses, including chargebacks/fraud losses and increased compliance overhead due to remediation;
- reputational damage (consumer trust, regulator perception, adverse media).

Where a breach or control failure is identified, the MLRO/Compliance function will coordinate immediate risk containment (including account restriction/blocking and, where applicable, sanctions-related freezing actions), analyse root-cause and corrective action plans with owners and deadlines, report to board/senior management for material issues, and assess whether the underlying activity triggers FIU reporting obligations (via goAML) or other competent authority notifications.

7. Related Information

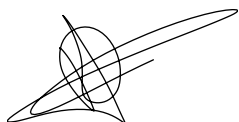
The external instruments and guidance sources listed below provide the legal, regulatory, and supervisory context for this Policy and the Company's supporting procedures:

- Curaçao Gaming Authority (CGA) – [AML regulatory materials](#), including consolidated texts and updates relevant to gambling operators.
- National Ordinance on Identification when Rendering Services (LID / NOIS) – [consolidated legal text](#).
- National Ordinance on the Reporting of Unusual Transactions (LMOT / NORUT) – [consolidated legal text](#).
- [FIU Curaçao reporting requirements](#) and [goAML](#) (reporting channel and operational requirements).
- Central Bank of Curaçao and Sint Maarten (CBCS) [AML legislation and "Provisions & Guidelines"](#).
- [FATF public lists](#) for geographic risk inputs.
- [Curaçao National Strategy and Action Plan to counter ML/TF/PF](#).

BMbit N.V.

Virtual Asset Risk Management Policy

V 2.0 Effective Date: 12.12.2025 approved by CO Derek Hendriks

A handwritten signature in black ink, consisting of a stylized 'D' and 'H' with a long horizontal stroke extending to the right.

Next Review Date: 12.12.2026*

*The policy shall be reviewed at least once every year or earlier, where triggered by material change (e.g. significant process/system change, or regulatory/supervisory update).

Version Control

Date	Author	Version	Description
01.11.2024	Jean Noel Azzopardi	1.0	Initial Version
01.12.2025	Jean Noel Azzopardi	2.0	Added and amended details to meet the latest regulatory requirements: Virtual Asset CDD as a part of AML CDD requirements. Freezing/Blocking for VA wallets – added FIU/CGA notification requirement. VASP Due Diligence – added requirement for annual review and equivalence confirmation.

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.....	7
6.3 Blacklisted Wallets.....	7
6.4 Exchange Services.....	7
7. Rate of Exchange.....	7
8. Red Flags.....	7
9. Preventive Measures.....	8
9.1 Risk Mitigation Strategies.....	8
9.2 Key AML Safeguards.....	9
9.3 VASP Due Diligence and Ongoing Oversight.....	10
9.4 Virtual Asset Customer Due Diligence.....	10
10. Blocking and Freezing of Accounts.....	11
11. Ongoing Monitoring.....	12
12. Suspicious Transaction Reporting.....	12
12.1 Submission of a STR.....	12
13. Dispute Resolution.....	13
14. Staff Training.....	13
15. Record Keeping.....	13
16. Non-Compliance.....	14
Appendices.....	15
Appendix I- Definitions.....	15

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
USDT
USDC
ETH
BCH
LTC
XRP
DOGE
ADA
DAI
BNB
TRX
SOL
TON

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.

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.

- 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 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. Preventive 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.

9.3 VASP Due Diligence and Ongoing Oversight

The Company performs and documents risk-based due diligence on any VASP that it uses or permits for customer-facing virtual asset deposits/withdrawals, custody, exchange, transfer, or related virtual asset services. This control is designed to mitigate ML/TF/PF risks arising from virtual asset transfers and to ensure the Company does not transact with illicit or sanctioned actors through weak or unregulated intermediaries.

Before onboarding or enabling a VASP Counterparty, the Compliance Department will complete a documented assessment including, at a minimum:

- obtain evidence that the VASP is licensed or registered as required in its home jurisdiction(s) and identify its competent supervisor(s).
- assess whether the VASP is operating in a jurisdiction with adequate AML/CFT regulation and supervision for VASPs, including the extent to which the regime requires preventive measures and monitors compliance.
- determine whether the VASP has been subject to any adverse media, public available regulatory actions, ML/TF investigations.

The Company will review each approved VASP Counterparty at least annually. This annual review is the minimum periodic refresh standard and may be increased for higher-risk counterparties. The review will also be performed promptly upon trigger events, including (non-exhaustive): change of ownership/management, new or changed licensing status, material control or product changes, credible adverse media, sanctions exposure, cybersecurity incidents impacting customer data, or regulatory actions/investigations.

9.4 Virtual Asset Customer Due Diligence

Virtual Asset CDD (VA CDD) forms part of the Company’s overall AML CDD requirements. Accordingly, any Customer who uses (or seeks to use) virtual asset deposit/withdrawal functionality is subject to the same baseline AML CDD principles set out in the AML Policy.

VA CDD is applied no later than the point at which the Customer engages in financial transactions reaching the applicable CDD threshold, as required by the Curaçao gaming-sector rules on the timing of CDD measures. VA CDD is also applied or refreshed where the Customer's risk profile changes (e.g., new wallet address, new jurisdictional indicators, new adverse information), there are doubts about previously obtained identification data, or there is suspicion of ML/TF/PF.

For Customers using virtual assets, the Company applies the baseline AML CDD controls described in the AML Policy, including:

- Collection of core personal data (name, DOB, address, nationality, ID number) and creation of the Customer profile;
- Verification of identity using reliable documentation and checks (and additional checks where necessary);
- Proof of Address evidence within the required recency window; and
- Risk-based escalation to EDD (including SoF/SoW collection) for higher-risk Customers and/or higher-risk activity patterns.

In addition to baseline AML CDD, the Company captures and maintains the Customer's withdrawal wallet address(es) as part of the Customer profile.

Where the circumstances give rise to a presumption or suspicion of ML/TF/PF (including where CDD refusal or delay, combined with other risk factors, elevates concern), the Company will consider and, where required, submit an unusual transaction report to FIU Curaçao via goAML.

10. Blocking and Freezing of Accounts

The Company is able to immediately suspend and/or restrict Customer accounts (including virtual asset deposit/withdrawal functionality) to ensure that:

- Transactions are prevented with Customers who are subject to financial sanctions, who are a potential/confirmed sanctions match, or whose account activity is subject to an AML/CFT/CFP review or investigation (including where execution may create ML/TF/PF exposure).
- Where the Customer risk rating (or a triggered alert) requires additional verification measures (e.g., EDD, Source of Funds/Source of Wealth information, clarification of transaction purpose), no transaction will be executed until the required measures are completed to the Company's satisfaction, or the relationship is terminated in line with policy.
- Where there is a perceived risk of unauthorized, fraudulent, or compromised account activity, restrictions are applied to prevent further activity and protect Customer funds and the integrity of the platform.

Where the facts and circumstances indicate that activity is an unusual transaction (intended or completed), or where suspicion of ML/TF/PF remains (including where CDD cannot be completed and a presumption exists), the MLRO will ensure the matter is reported to FIU Curaçao without delay via the goAML reporting portal, and that supporting records are retained.

Where required under applicable sanctions obligations, the Company will freeze/restrict access to funds/virtual assets and make the required report(s) to the FIU without delay, in accordance with applicable sanctions guidance and internal procedures.

As the competent AML/CFT supervisor for gambling in and from Curaçao, the Company will cooperate with the CGA and will make relevant information available upon request, including documentation supporting suspensions/blocks, risk assessments, and control evidence. Where an event is otherwise reportable to the CGA under applicable licensing/supervisory requirements, the Compliance Department will notify the CGA through the prescribed channel and within the applicable timeframe.

-

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

suspicious 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 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, is 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, analysing, 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 organisations 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.