

BMbit N.V.

Anti-Money Laundering and Combating Financing of Terrorism Policy

Document Information

Subject	Anti Money Laundering and Combating of Funding of Terrorism Policy
Purpose	We seek to offer the highest security to all of our users and customers for that a three-step account verification is done in order to insure the identity of our customers. The reason behind this is to prove that the details of the person registered are correct and the deposit methods used are not stolen or being used by someone else, which is to create the general framework for the fight against money laundering. We also consider that depending on the nationality and origin, the way of payment and for withdrawing different safety measurements must be taken.
Stakeholders	BMbit N.V. is committed to high standards of anti-money laundering (AML) according to the EU guidelines and 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, and requires management & employees to enforce these standards in preventing the use of its services for money laundering and terrorist financing purposes.
Approval	Board of Directors
Review	Each major change of AML policy is subject to approval by the board of directors of BMbit N.V. and the Anti money laundering compliance officer.
Classification	Company Confidential

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

Introduction

Money Laundering (ML) is generally classified as engaging in acts designed to conceal or disguise the nature, control, or true origin of criminally derived proceeds to give the illusion that those proceeds have been derived from legitimate activities or origins and so constitute legitimate assets.

What constitutes Money Laundering:

- a) The conversion or transfer of property, especially money, knowing that such property is derived from criminal activity or from taking part in such activity, for the purpose of concealing or disguising the illegal origin of the property or of helping any person who is involved in the commission of such an activity to evade the legal consequences of that person's or companies action;
- b) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- c) The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from assisting in such an activity;
- d) Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of the actions referred to in points before.

Money laundering shall be regarded as such even when the activities which generated the property to be laundered were carried out in the territory of another state or in that of a third country.

The funding of terrorism (FT) is the process of making funds or other assets available to support terrorist activities directly and indirectly. Most of the implemented controls serve dual purpose in combating the risk exposure of ML and FT.

Whereas ML is the process of making “dirty” money appear legitimate, funds obtained by terrorist organizations may have legitimate/ illegitimate origins and the concealment efforts are specifically aimed towards hiding the receiver of these funds, the members of the terrorist groups themselves.

Proceeds of crime are funds derived from illicit sources and from which a benefit or enjoyment may be obtained. Although the ultimate aim may not necessarily be to launder funds or to fund terrorism, gambling using proceeds of crime for enjoyment is still considered to be illegal and subject persons should always be aware of such activity and report it as if it were ML/FT.

The policies set forth herein are intended to satisfy the statutory requirements of the Curacao and other relevant legislation and to provide direction to the company in complying with its obligations at law by taking all reasonable steps and exercising rigorous due diligence to avoid the commission of an offense of money laundering or terrorist financing.

BMbit N.V. (trading as Betmaster) is aware that criminals may attempt to channel proceeds of crime funds from illegal activities through the company's services whether that be for traditional money laundering or expenditure of proceeds derived from predicate offenses. The company also is vigilant against individuals who attempt to utilize the facilities of the company to finance terrorism.

Scope of the policy

The scope of this policy is to establish a program of internal policies and procedures on internal controls, risk assessment, risk management and compliance to AML/CFT.

These policies and procedures are relevant to all employees, contractors, affiliates, or any authorized individual working on behalf of the company BMbit N.V., licensed by the Curaçao Gaming Control Board (GCB) since 22 July 2024 to offer games of chance under license number OGL/2024/650/0284.

Policies and procedures set out the expectations across the above entities, however the individual processes of implementing and achieving the goals of these policies and procedures may differ due to reasons such as different back offices, software, etc.

The AML program of BMbit N.V. is designed to be compliant with:

1. EU: "Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering"
2. EU: "Regulation 2015/847 on information accompanying transfers of funds"

3. EU: Various regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods
4. Curaçao: 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

Unless specifically indicated phrases and expressions used in the Policy shall have the same meaning as that set out in the applicable laws and regulations.

The company is fully committed to preventing the carrying out of financial activities through its systems that may be related to AML/CFT.

The company shall comply fully with its obligations at law by establishing the necessary and relevant processes to prevent AML/CFT and to ensure that any suspicious activities are escalated to the relevant authorities.

This policy seeks to establish the general and minimum standards of internal anti money laundering and combating funding of terrorism which should be adhered to by employees at all levels.

Compliance Officer (Money Laundering Reporting Officer)

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:

- a) Design and implementation of the company's AML program and making necessary changes to the AML program;
- b) Verification of the adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- c) The review of compliance with the company's policies and procedures;
- d) Organization of the training sessions for the staff on various compliance-related issues;
- e) 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;
- f) Review of all internally reported unusual transactions for their completeness and accuracy with other sources;
- g) Keeping of the records of internally and externally reported unusual transactions;
- h) Execution of the closer investigation of unusual transactions if necessary;
- i) Preparation of the external report of unusual transactions;
- j) 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;
- k) Preparation of periodic information on the company's efforts against money laundering and financing of terrorism and financing of proliferation;
- l) Customer Risk Assessment (CRA) procedures and Customer Acceptance Policy (CAP) Risk assessment and risk management.

Risk based Approach

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.

Customer Risk Assessment

The company's customers are assessed to risk throughout the full business relationship based on the following areas, which are reviewed in conjunction with several risk factors, including but not limited to:

Customer & Geographical Risk

Customer Identity Verification

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: Sumsb

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 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.

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 Parlements, 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

Transactional Risk

Transactional Risk Matrix:

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 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.

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.

Product/Service

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.

Extraordinary circumstances

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.

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.

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 prove.

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 information on the website itself.

BMbit N.V. also asks for a bank wire/credit card to further insure 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 setting 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.

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'.

Suspicious Transaction Reporting

An internal suspicious transaction report is to be sent directly to the MLRO whenever there is a suspicion, knowledge or reasonable grounds to suspect that a customer is engaging in ML/FT.

Once the report has been escalated to the MLRO, it is strictly forbidden to divulge any information to colleagues, line managers and especially to the customer as this may be considered 'Tipping Off'. Tipping off is a criminal offense, and an individual found guilty of tipping off may be held personally liable. An employee who raises a STR must escalate this directly to the MLRO and must only notify and liaise with the relevant team member as per the 'Due Diligence Procedures'.

An employee may only discuss the case or request assistance from the MLRO in case of any uncertainty whether to raise an internal STR. For further guidance please refer to the 'Internal Suspicious Transaction Report Procedure'.

Reports of atypical transactions are analyzed within the AML team in accordance with the precise methodology fully described in the internal procedures.

Depending on the result of this examination and based on the information gathered, the AML team:

- will decide whether it is necessary or not to send a report to the FIU, in accordance with the legal obligations;
- will decide whether it is necessary to terminate the business relations with the customer.

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.

Supplier Reliability

The company ensures that proper and relevant due diligence is made on engagement of business partners and suppliers.

Retention of Records

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.

Auditing

The company may carry out an internal audit regime to test the effectiveness of the level of implementation of this policy within the applicable entity within the group. A report with the findings of this audit together with any recommendations, will be presented to Senior Management for their evaluation. Any action point derived from the assessment will be promptly implemented whenever possible or an action plan will be drafted to ensure full implementation dependent on development capacity.

Data Security

All data given by any user/customer are kept secure and are not sold or given to anyone else. Only if enforced by law, or to prevent money laundering or terrorist financing, data may be shared with the AML-authority of the affected state.

Non-Compliance to Policy

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.