

AML and KYC Policy of StepX B.V.

Last updated: May 7th, 2025, by MLRO of StepX B.V. Mr. Vladyslav Malynovskyi

Introduction:

www.betkin.com is operated by StepX B.V. (hereinafter – the “Company” or “we”) having its office at Heelsumstraat 51, E-Commerce Park Vredenberg, Curaçao, the mailing address: Chuchubiweg 17, Curaçao, Company Registration number 156454 is obliged to observe the anti-money laundering and countering financing of terrorism legislation (hereinafter – AML/CTF Laws) in accordance with the National Ordinance on identification when rendering services (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92), the National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector, LB van 28 januari 2019, no. 19/0282) and the National Decree supervisor unusual transactions gaming sector (Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector, LB van 28 januari 2019, no. 19/0283) and other applicable legislation in order to protect the assets of the Customers (hereinafter - the “Customers” or “Customers”) and to provide the compliance with both international and national trade standards and principles, applicable legislation, best banking practices and applicable market standards including, and, where relevant, other international financial institutions’ standards.

The policies and procedures in this Policy is based on the NOPML, the NORUT and the NOISE which regulations themselves are referring to the Penal Code. The Central Bank of Curacao has introduced a comprehensive framework with provisions and guidelines to prevent and combat money laundering and terrorist financing. Curaçao - as a member of the FATE - has passed the Provisions and Guidelines on, among others, the FATF recommendations.

Both the NORUT and the NOIS are applicable on entities which are offering the possibility to take part in offshore hazard games (online gambling) in or out of Curaçao. The NOIS prohibits subject persons from forming a business relationship or carrying out an occasional transaction with an applicant for business unless said subject person maintains the following measures and procedures established in relation to that business in accordance with the provisions of the NOIS:

- customer due diligence measures;
- record-keeping procedures; and
- internal reporting procedures.

The Company is also obliged to ensure that employees are made aware of applicable AML/CFT legislation as well as the subject person’s policies and measures in this regard. Employees must undergo appropriate due diligence procedures prior to their engagement and are also expected to be provided with training regarding the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism.

Definition of money laundering:

Money Laundering is understood as:

- 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;
- 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;
- 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;
- Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling 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 Member State or in that of a third country.

Objective of the AML Policy:

We seek to offer the highest security to all of our users and customers on www.betkin.com 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 take into accord that depending on the nationality and origin, the way of payment and for withdrawing different safety measurements must be taken.

www.betkin.com also puts reasonable measures in place to control and limit ML risk, including dedicating the appropriate means.

www.betkin.com is committed to high standards of anti-money laundering (AML) according to the EU guidelines, compliance and requires management & employees to enforce these standards in preventing the use of its services for money laundering purposes.

International Sanctions

This AML program is prepared in accordance with the current UN, EU, FATF and OFAC sanction regimes, available on the official resources of the authorities, responsible for establishment and monitoring of sanctions.

Specifically, the AML program of www.betkin.com is designed to be compliant with :

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"

EU: "Regulation 2015/847 on information accompanying transfers of funds"

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

BE: "Law of 18 September 2017 on the prevention of money laundering limitation of the use of cash

We check the sanction lists and monitor the updates of sanction legislation on a weekly basis in order to comply with the applicable sanction regime and maintain the quality and legality of Our services.

We confirm that provision of services to any person directly or indirectly involved into or having connection to sanctioned jurisdiction or being a sanctioned person is out of Our risk appetite and cannot be performed.

AML Scope:

Subject to AML/CTF Laws the Company is obliged to make the following actions when establishing a business relationship with any of its Customers:

- to detect and deter money laundering and financing of terrorism;
- to maintain and enhance the Company's international reputation by adopting, where appropriate, recommendations and regulations issued by the relevant national and international regulatory authorities;
- to contribute to public confidence in the financial system.

By applying for an account with the Company the Customer agrees to the following terms:

The Customers warrants compliance and consent with all applicable anti-money laundering laws and regulations, including but not limited to the AML/CTF Laws and associated rules and regulations (in force from time to time);

The Customer is not aware and has no reason to suspect that:

- the money used to fund the Customer's account in the Company has been or will be derived from or related to any money laundering or other activities deemed illegal under applicable laws or regulations or otherwise prohibited under any international convention or agreement ("illegal activities"); or
- the proceeds of the Customer's investment will be used to finance illegal activities; and
- the Customer agrees to promptly provide the Company with all the relative information that the Company has requested in order to comply with all applicable laws and regulations relating to anti-money laundering.

Security measures carried out by the Company in the course of its business relationship with the Customer include:

- transactions or operations carried out to identify a party;
- collection of information necessary to achieve due diligence;
- identification and prevention of fraud, error or other abuse of compliance with the obligations imposed on the financial institution by law or other act.

In accordance with the Company's AML Policy we will conduct initial and ongoing due diligence for each customer according to risk level posed by the customer.

The Company shall not conclude any contract or enter into any business relationship with persons (individuals, or any party whatsoever) from "black-list" jurisdictions stipulated and regularly updated in annex 1 hereto.

Counterparty Due Diligence

The Company applies the following counterparty due diligence measures, as determined on a risk-sensitive basis taking into account where relevant the type of counterparty, business relationship, product or transaction and country of operation.

1. Identification and Verification of Identity of Counterparty

For identity and due diligence purposes, at the minimum following information shall be obtained, verified and recorded.

2. Information requested from the customer:

- a) Customer's date of birth (showing that the player is over eighteen (18) years of age);
- b) Customer first and last name;
- c) Customer place of residence;
- d) Customer credit card or banking information;
- e) Customer valid email address; and
- f) Customer username and a password
- g) Customer's identity card;
- h) Customer's digital identity card;
- i) Customer's residence permit card;
- j) Customer's citizen's passport;
- k) Customer's diplomatic passport;
- l) Customer's seafarer's discharge book;
- m) Customer's temporary travel document;
- n) Customer's travel document for a refugee;
- o) Customer's certificate of record of service on ships;
- p) Customer's certificate of return;
- q) Customer's permit of return;
- r) the European travel document for return for the purposes of Regulation (EU) 2016/1953 (repatriation certificate).
- s) document proving current permanent address (such as utility bills, bank statements, etc.);
- t) Customer's driving license with picture;
- u) A document specifying a source of funds used to fund the Customer's account;
- v) other documents necessary for the enhanced due diligence.

3. Establishment of Purpose of Business Relationship

The Company takes reasonable measures to duly assess the purpose, intended nature, economic rationale and overall AML-CFT Laws and related integrity aspects of the business relationship in order to avoid being involved in business relationships structured for the purposes of criminal activities or co-financed through funds of possibly illicit origin.

4. On-going Monitoring

On-going monitoring (including monitoring of transactions) is implemented on a risk-sensitive basis to detect possible Money Laundering, Financing of Terrorism or related integrity risks arising throughout the life of the business relationship.

5. Adverse information check

In addition to the information and documents, requested from the Customer, as a part of its Due Diligence procedures, the Company will conduct the check and subsequently monitor the adverse information regarding its Customers, available in the public resources.

Adverse information screening is conducted on a regular basis as a part of DD procedures, no less than at least once a month.

6. The Company shall reject any perspective Customer or Counter-party:

- If Measures specified in sections 1. - 5. are not completed.
- In case the Company is not been able to satisfactorily completed required measures, the Company shall reject any person from becoming Company's Customer and shall withdraw from providing any service to such person.

7. Anonymous or Fictitious:

The Company shall not provide services to anonymous Customers or accounts in the name of fictitious persons.

8. Government Accounts:

The Company shall not provide services to government officials.

9. Proscribed Individuals/Entities:

The Company shall not provide services to Proscribed Individuals, Groups and Entities declared / listed by UNSC (United Nations Security Council), by OFAC (Office of Foreign Asset Control – USA) OR those who are known for their association with such entities and persons, whether under the proscribed name or with a different name.

Dealing with sanctioned persons

In the case that during the client on-boarding due diligence check, or during client's monitoring process, any Employee of the StepX B.V. will become in the possession of the information that the Client is presented in any sanction lists of the mentioned organizations and jurisdictions, or is anyhow connected to the sanctioned jurisdictions or organization, then such client will be reported to the MLRO, his funds and accounts will immediately be frozen until the enhanced due diligence check is conducted by the MLRO.

It is restricted to notify the client or any related third party about subsequent freezing measures to be applied.

Subsequently, if the MLRO will have all the grounds to belief that such client has connections with the sanctioned jurisdictions or organizations, or is a sanctioned individual, then any financial cooperation with such client shall be ceased and the report regarding this client will be submitted to the FIU.

The list of sanctioned jurisdictions is mentioned in the Annex 1 to this AML Policy

Organization of the AML for www.betkin.com:

In accordance with the AML legislation, www.betkin.com has appointed the “highest level” for the prevention of ML: The full management of StepX B.V. are in charge.

Furthermore, an AMLCO (Anti Money Laundering Compliance Officer) is in charge of the enforcement of the AML policy and procedures within the System.

The AMLCO is placed under the direct responsibility of the general Management:

AML policy changes and implementation requirements:

Each major change of www.betkin.com AML policy is subject to be approval by the general management of StepX B.V. and the Anti money laundering compliance officer.

AML and Transaction Fraud

The Company recognizes that gaming environments are often targeted by those wishing to launder money. The speed of transactions and use of multiple payment processing options make gaming businesses especially vulnerable to this activity.

As a result, many of the initial trading and procedural decisions of the directorate are either directly aimed at combating this threat or protections are enhanced as a bi-product of the overall commercial and trading approach/strategy taken by the business.

All staff will be given training in Money Laundering indicators such as (but not limited to):

- Unusual Betting Patterns
- Suspicious deposit and withdrawal patterns (size and frequency)
- Reliability of Card Data
- Customer verification issues and Identity Theft
- Account linkage/multiple accounting

All cases of suspected Money Laundering attempts or suspicious activities must be reported to the AML-officer but that suspicion must not be conveyed to the customer and further actions must await consents. The AML-officer is then responsible for liaising with, submitting Suspicious Activity Reports and seeking consents from the relevant regulatory authorities where and when appropriate. He will also ensure that appropriate registers are kept for all related reporting.

Other key decisions that will enhance these protections include setting period thresholds/velocities for withdrawals to include at outset the requirement for checks and directorate approval prior to processing card withdrawals and bank transfers of over 2000 EUR in one single transaction, a maximum of 3 (three) daily withdrawals and an overall maximum daily withdrawal of 6000 EUR.

The Company shall proceed to Enhanced Due Diligence in cases of withdrawals in excess of 2000 EUR in a single 24-hour period and 6000 EUR in a 90-day period. Simple online verification shall NOT be acceptable in these circumstances.

The Company shall record all transactions for each Customer account. These account histories shall be subject to regular and continual checks against fraud and social responsibility indicators. Where unusual patterns and winning patterns are detected, such patterns shall also be cross- referenced to ensure that staff are not colluding with customers or acting illicitly.

Company will also keep a register of Customers that the Company identifies as high risk or politically exposed. Those accounts will be subject to greater scrutiny and frequency of checks.

The Company shall investigate any case where illegal or inappropriate behaviour by staff is identified. Investigatory and disciplinary procedures shall follow.

AML Officer

The management board of the Company shall appoint an AML Officer, who performs AML/CTF duties and obligations of the Company. An AML Officer reports directly to the management board and has the competence, means and access to relevant information across all the structural units of the Company.

An AML Officer shall be deemed a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties listed below.

The duties of an AML Officer include, inter alia:

- organization of the collection and analysis of information referring to unusual transactions or transactions or circumstances suspected of money laundering or terrorist financing, which have become evident in the activities of the Company;
- reporting to the relevant authorities in the event of suspicion of money laundering or terrorist financing;
- periodic submission of written statements on compliance with the requirements arising from the AML/CTF Laws to the management board of the Company;
- performance of other duties and obligations related to compliance with the requirements of the AML/CTF Laws.

The AML Officer shall perform training duties. (see Section 8 "TRAINING").

The AML Officer shall ensure that Company's employees are fully aware of their legal obligations under the AML/CTF regime, by introducing a complete employees' education and training program.

The timing and content of the training provided is determined according to the needs of the Company. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the business model. The training program aims at educating the Company's employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose.

Three step Verification:

Step one verification:

Step one verification must be done by every user and customer to withdraw. Regarding of the choice of payment, the amount of payment, the amount of withdraw, the choice of withdraw and nationality of the user/customer step one verification must be done first. Step one verification is a document that must be filled out by the user/customer himself. Following information's must be filled in: first name, second name, date of birth, country of usual residence, gender and full address.

Step two verification:

Step two verification must be done by every user which deposit over 2000\$ (two thousand Dollar) or withdraws over 2000\$ (two thousand Dollar) or sends another user over 1000\$ (one thousand Dollar) Until step two verification is done the withdraw, tip or deposit will be hold. Step to verification will lead the user or customer to a subpage where he must send in his ID. The user/customer must make a picture of his ID. While a paperclip with a six-digit random generated number is next to his ID: Only an official ID may be used for ID verification, depending on the country the variety of accepted IDs may be different. There will also be an electronic check if the filled in Data from the step one verification is correct. The electronic check will check via two different databanks to insure the given information's matches with the filled document and the name from the ID: If the electronic test fails or is not possible the user/customer is required to send in a conformation of his current resident. A certificate of registration by the government or a similar document is required.

Step three verification:

Step three verification must be done by every user which deposit over 5000\$ (five thousand Dollar) or withdraws over 5000\$ (five thousand Dollar) or sends another user over 3000\$ (three thousand Dollar) Until step three verification is done the withdraw, tip or deposit will be hold. For step 3 a user/customer will be asked for a source of wealth.

Customer identification and verification (KYC)

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.

This identification relies on the following fundamental principles:

A copy of your passport, ID card or driving license, each shown alongside a handwritten note mentioning six random generated numbers. Also, a second picture with the face of the user/customer is required. The user/customer may blur out every information, besides date of birth, nationality, gender, first name, second name and the picture. To secure their privacy.

Please note that all four corners of the ID have to be visible in the same image and all details has to be clearly readable besides the named above. We might ask for all details if necessary.

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

Proof of Address:

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

A recent utility bill sent to your registered address, issued within the last 3 months or an official document made by the government that proofs your state of residence.

To make the approval process as speedy as possible, please make sure the document is sent with a clear resolution where all four corners of the document is visible, and all text is readable.

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

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

Source of funds

If a player deposits over a five thousand euro there is a process of understandings 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 an information on the website itself.

www.betkin.com 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 document for step one:

The basic document will be accessible via the setting page on www.betkin.com. Every user has to fill out the following information's:

- First name
- Second name
- Email
- Number Phone
- Date of Birth

The document will be saved and created by an AI, an employee may do additional checks if necessary based on the situation.

Reporting Unusual Activity

The Company shall record each unusual transaction individually. Each report about an unusual transaction will include at least the following information:

- a. the identity of the client;
- b. nature and number of the identification document of the client;

- c. the nature, date, time and place of transaction;
- d. the amount, destination and origin of the funds, securities, precious metals, or other values
- e. involved in the transaction;
- f. the circumstances that identified the transaction as unusual.
- 1. In case of manual reporting to the FIU, the following items must be added:
 - a. Company report;
 - b. Date and time of the report;
 - c. Amount of the transaction, including the currency in which it is to be executed;
 - d. Whether or not the Company executed the transaction;
 - e. Any other relevant facts or circumstances pertaining to the Customer or the proposed transaction.

The AML-Officer signs the reporting form if it is submitted manually.

The Company shall not conclude the unusual transaction if the information, necessary for the report, cannot be obtained. The Company shall report to the FIU within 48 hours the details of the transaction as recorded on the reporting form. The Company can use an electronic system approved by the FIU for this purpose, or submit a paper copy of the reporting form. Submission of paper forms shall not be done by fax for the purpose of data security.

Politically Exposed Persons (PEP) Policy:

A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting due to being considered more vulnerable to bribery and corruption. Therefore, full enhanced due diligence must be conducted upon any identified PEPs.

The Company does not distinguish between foreign and domestic PEPs, all are considered high risk. A PEP that no longer holds their prominent public role will also be deemed high risk.

Screening is undertaken by the Company with the help of automated tools as well as using the third party KYC service s to identify PEP and Sanctioned individuals upon customer registration/deposit. This will also pick up on any adverse media relating to the customer.

The screening regarding update in the sanctioned list and publicly available information resources, which might contain information regarding potential PEP and sanctioned persons is conducted mandatory upon registration of the account or fund deposition, as well as regularly on a weekly basis, in order to mitigate the risks and exclude chances for missing the update in the client's PEP or sanction status.

PEP Definition:

A PEP is defined as a natural person who is or has been entrusted with prominent public functions, including:

- A head of state, head of government, minister or deputy or assistant minister;
- A senior government official;
- A Member of Parliament (MP);
- A senior politician;
- An important political party official;
- A senior judicial official;
- A member of a court of auditors or the board of a central bank;

- An ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
- A high-ranking officer in an armed force;
- A senior member of an administrative, management or supervisory body of a State-owned enterprise;
- A senior official of an international entity or organization.

A PEP also includes family members and close associates of the above, including:

- A spouse;
- A partner considered by national law as equivalent to a spouse;
- Other known close personal relationships such as a partner, boyfriend or girlfriend;
- A child;
- A spouse or partner of a child;
- A brother or sister (including a half-brother or half-sister);
- A spouse or partner of a brother or sister;
- A parent;
- A parent-in-law;
- A grandparent;
- A grandchild;
- A joint beneficial owner of a legal person or legal arrangement, or any other close business relationship, with a PEP;
- The sole beneficial owner of a legal person or legal arrangement known to have been set up for the benefit of a PEP;
- A beneficiary of a legal arrangement of which a PEP is a beneficial owner or beneficiary;
- A person in a position to conduct substantial financial transactions on behalf of a PEP.

SEGREGATION OF ASSETS

StepX B.V. declares that, should it hold client assets in the future, such assets will be strictly segregated from the company's own assets. The segregation of assets will be achieved through the maintenance of separate accounts and the implementation of rigorous management practices to ensure that there is no commingling of funds.

Company Assets: Defined as all assets owned or managed by StepX B.V. for its operational activities, including but not limited to cash reserves, investments, and other financial instruments.

Clients' Assets: In the event that StepX B.V. holds assets on behalf of clients in the future, such assets will be maintained in separate, clearly designated accounts to ensure that they are distinct from the company's own assets.

To ensure the effective segregation of assets, StepX B.V. shall implement the following measures:

- StepX B.V. shall establish and maintain distinct bank accounts for its

- operational funds. Should the need arise to hold client assets, separate accounts specifically designated for client money shall be created to ensure a clear demarcation between company and client funds.
- StepX B.V. shall conduct daily reconciliations of all accounts to ensure that the amounts held in any client accounts are accurate and fully reflect the company's obligations to its clients.
- Detailed and accurate records of all transactions involving both company and client assets shall be maintained, ensuring transparency and adherence to this Policy.
- StepX B.V. shall enforce stringent internal controls to monitor and manage the flow of assets, ensuring compliance with this Policy and preventing any unauthorized commingling of funds.

Risk management:

The Regulations require StepX B.V. to adopt a risk-based approach to the application of measures to prevent money laundering and terrorist financing.

Additionally, the Company and its employees must monitor each Client and ascertain the risk posed by each Client. The gradation below highlight some indicators that employees may use to determine the risk posed by a Client. The table is not exhaustive, and employees must liaise with the MLRO if they are concerned about any Client.

Region one: Low risk:

For every nation from the region one the three-step verification is done as described earlier.

Region two: Medium risk:

For every nation from the region two the three-step verification will be done at lower deposit, withdraw and tip amounts. Step one will be done as usually. Step two will be done after depositing 1000\$ (one thousand Dollars), withdrawing 1000\$ (one thousand Dollars) or tipping another user/customer 500\$ (five hundred Dollars.) Step three will be done after depositing 2500\$ (two thousand five hundred Dollars), withdrawing 2500\$ (two thousand five hundred Dollars) or tipping another user/customer 1000\$ (one thousand Dollars). Also, users from a low risk region that change crypto currency in any other currency will be treated like user/customers from a medium risk region.

Region three: High risk:

Regions of high risks will be banned. High risk regions will be regularly updated to keep up with the changing environment of a fast-changing world.

Risk Matrix:

Following an in-depth review of the preceding factors by the Company's senior management the following matrix details the customer due diligence requirements:

DUE DILIGENCE CHECK	LOW	MEDIUM	HIGH
Pep and Sanction Screening	x	x	x
Identity Verification	x	x	x

Screening			
Request ID and Address Verification		x	x
Open Source Check		x	x
Source of Funds	x	x	x
Source of Wealth			x
Additional ID and Address documents			x
Additional 3 rd party verification screening			x

If an employee deems a Customer to be a high-risk of money laundering or terrorist financing, they must inform the AML-officer immediately. The AML-officer may direct the employee to carry out extensive due diligence on the Customer to acquire additional evidence regarding their identity or the source of the funds involved in the transaction. The transactions and activity of any high-risk Customers should be carefully monitored on an ongoing basis.

Identifying a Customer or transaction as being of a higher risk does not mean that the Customer is involved in money laundering or terrorist financing. Furthermore, if a Customer is deemed to be a lower risk, it does not mean that the Customer is not involved in money laundering or terrorist financing. Employees must be vigilant always and report any suspicions to the AML-officer.

Risk criteria

The company applies a developed system of risk analysis, which takes into account various risk criteria, concerning the overall status of the Customer. The list of criteria is prepared in accordance with the applicable AML/KYC legislation, FATF recommendations, and applicable norms of compliance check, implemented by various third parties, whose services might be used in the process of KYC.

Those criteria are:

- usage of the VPN or other proxy servers, which is considered as a factor, influencing risk level of the Customer;
- conformity between Customer address, provided and his IP, difference between the two might result in request of additional documents and rise of risk level;
- conformity between the ID document issuance country, in comparison with IP country, difference might result in additional requests and rise of risk level;
- conformity between country of photo creation and IP and ID document countries, difference might result in additional check and rise of risk level;
- any found criminal records are considered as a significant risk marker, aggravating risk evaluation;
- overall quality of the provided ID document, its fonts, template, image quality, security features, correspondence with the applicable standards for a specific country;
- provision of screenshot images are considered as a risk matter;

- any information, which became available to us or any third party, providing services of KYC check, regarding belonging of the Customer to sanction or black lists, will be considered as a factor, sufficiently aggravating the risk level of the Customer;
- information, confirming or providing us with the grounds to believe that the Customer is a Politically exposed persons (PEP) will be considered as a factor, sufficiently aggravating the risk level of the Customer;
- any information, found in the adverse media, available AML/CTF reports track (public registers), or any other publicly available source of information, confirming inconsistency of the information, provided by the Customer will be considered as a factor, sufficiently aggravating the risk level of the Customer;
- information of any associated persons, involved in illegal, or suspicious activity will result in the increase of the risk level of the Customer;
- difference between estimated age on the photo of the Customer, in comparison with age on the ID document might increase risk level of the Customer or result in additional information request;
- inconsistency between the transaction amounts, and regular financial activity will also be considered as a factor, increasing risk level of the Customer.

Risk screening

Screening of Customers is performed:

- individually upon first deposit request;
- individually upon 2000 EUR threshold is reached by the Customer and verification process is initiated ;
- individually during periodic reviews depending on the risk level of the Customer;
- individually upon identification of high risk triggers;
- each client undergoes compulsory check on a regular basis;
- the whole client database is checked quarterly.

Additional measurements.

In addition, an AI which is overseen by the AML compliance officer will look for any unusual behaviour and report it right away to a employee of www.betkin.com.

According to a risk based few and general experience the human employees will recheck all checks which are done before by the AI or other employees and may redo or do additional checks according to the situation.

In addition, a data Scientist supported by modern, electronic, analytic systems will look for unusual behaviour like: Depositing and withdrawing without longer Betting sessions. Attempts to use a different Bank account to for Deposit and Withdraw, nationality changes, currency changes, behaviour and activity changes as well as checks, if an account is used by it's original owner.

Also a User has to use the same method for Withdraw as he used for Deposit, for the amount of the initial Deposit to prevent any Money Laundering.

Enterprise-wide risk assessment

As part of its risk-based approach, www.betkin.com has conducted an AML "Enterprise-wide risk assessment" (EWRA) to identify and understand risks specific to www.betkin.com and its business lines. The AML risk policy is determined after identifying and documenting the risks

inherent to its business lines such as the services the website offers. The Users to whom services are offered, transactions performed by these Users, delivery channels used by the bank, the geographic locations of the bank's operations, customers and transactions and other qualitative and emerging risks.

The identification of AML risk categories is based on www.betkin.com understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.

The EWRA is yearly reassessed.

Ongoing transaction monitoring

The AML-officer and the Company Management team shall carry out regular assessments of the risks posed by the Company's Customers and the services provided by the Company. The procedures set out in this document shall be regularly assessed against the risks posed by the Company's Customers.

The document and the procedures contained in it will be amended in accordance with the Company's risk profile.

This transaction monitoring is conducted on two levels:

1) The first Line of Control:

www.betkin.com works solely with trusted Payment Service Providers whom all have effective AML policies in place as to prevent the large majority of suspicious deposits onto www.betkin.com from taking place without proper execution of KYC procedures onto the potential customer.

2) The second Line of Control:

www.betkin.com 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. In particular 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 verification with adjusted risk management should provide all necessary information's about all costumers of www.betkin.com at all time.

Also, all transaction must be overseen by employees over watched by the AML compliance officer who is over watched by the general 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 behaviour and the transaction counterparty.

These checks will be done by an automated System, while an Employee crosschecks 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 www.betkin.com 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 of the customer.

3) The third Line of Control:

As a last line of defence against AML www.betkin.com will do manually checks on all suspicious and higher risk users in order to fully prevent money laundering.

If fraud or Money Laundering is found the authorities will be informed.

Reporting of Suspicious transactions on www.betkin.com

In its internal procedures, www.betkin.com describes in precise terms, for the attention of its staff members, when it is necessary to report and how to proceed with such reporting.

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

Depending on the result of this examination and on the basis of 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 provided in the Law of 18 September 2017;
- will decide whether or not it is necessary to terminate the business relations with the customer.

Procedures

The AML rules, including minimum KYC standards will be translated into operational guidance or procedures that are available on the Intranet site of www.betkin.com.

Record keeping

Records of data obtained for the purpose of identification must be kept for at least ten years after the business relationship has ended.

Records of all transaction data must be kept for at least ten years following the carrying-out of the transactions or the end of the business relationship.

These data will be safely, encrypted stored offline and online.

Training:

www.betkin.com human employees will make manual controls on a risk based approve for which they get special training.

Training will be designed to ensure that all relevant staff are made aware of the risk of the Company being used for the purposes of financial crime, the consequences for the firm (as well as staff personally), the requirement to operate systems and controls to mitigate such

risk and the requirement to report suspicious activity. The AML-Officer shall be responsible for conducting relevant training procedures.

Relevant staff include the staff of the Company who handle or are managerially responsible for the handling of customer on-boarding and service provision.

The frequency of the provision of AML training will be determined using a risk-based approach, with those who may be at greatest risk from handling suspicious transactions, or who need to be kept up-to-date with changing vulnerabilities and trends, receiving training at more frequent intervals; relevant staff who are close to transaction processing activity are prioritized for training which may be more detailed in content than the training provided for other staff.

All employees are to be made aware of:

- a. customer due diligence measures;
- b. record-keeping procedures;
- c. internal reporting procedures;
- d. policies and procedures on internal control;
- e. policies and procedures on risk assessment and risk management; and
- f. policies and procedures on compliance management and communication.

Employees shall also be made aware of the following:

- a. the provisions of the NORUT and the NOIS;
- b. the provisions in the Criminal Code on AML & CTF;
- c. the provisions of the P&G;
- d. the offenses and penalties in relation to any breach of the NOIS or the NORUT

AML training shall be performed with the relevant staff and will include the following elements:

- a. Legal and regulatory obligations under Curacao law;
- b. Practical means of identifying unusual and suspicious transactions; and
- c. Internal processes and advice on how to act when presented with suspicious activity

Auditing

Internal audit regularly establishes missions and reports about AML activities.

Data Security:

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

www.betkin.com will follow all guidelines and rules of the data protection directive (officially Directive 95/46/EC)

Contact us:

If you have any questions and If you have any complains about our AML and KYC Policy or about the checks done on your Account and your Person, please contact us:

- By email: complaints@batgame88.com

Annex 1 to the AML Policy of the StepX B.V.

List of Sanctioned and Prohibited Jurisdictions:

Afghanistan;

American Samoa;

Barbados;

Botswana;

Burundi;

Cambodia;

Cameroon;

Central African Republic;

Cuba;

Curacao;

Ethiopia,

North Korea (DPRK);

Democratic Republic of

the Congo;

Fiji;

Guam;

Iran;

Iraq;

Lebanon;
Libya;
Mali;
Mozambique;
Myanmar (Burma);
Netherlands;
Nicaragua;
Nigeria;
Pakistan;
Palau;
Palestine;
Samoa;
Senegal;
Somalia;
South Sudan;
Sudan;
Syria;
Trinidad and Tobago;
Uganda;
United States of America;
Venezuela;
Yemen;
Zimbabwe;

Contested territories that are not internationally recognized: Luhansk, Zaporizhzhia, Kherson and Donetsk regions of Ukraine, Transdniestria, The Crimea Region (Ukraine), Abkhazia, South Ossetia etc.