

Anti-Money Laundering Policy

Operator: B2bseven B.V. (Reg. No. 152184), Kaya Richard J. Beaujon Z/N Landhuis Joonchi II, Willemstad, Curaçao

Website: www.b2bseven.bet

License: Curaçao Gaming Authority (CGA), License No. OGL/2024/636/0578

Overview

Money Laundering (ML) is the process of making funds that originate from criminal activities appear as being originated from a legitimate source. Funding of Terrorism (FT) is the process of using such funds to fund terrorism. We are obliged by law to combat both ML and FT. Our services, since they are widely used, might become a target from criminals to perform ML and FT; by laundering money via online betting games and casinos.

Abbreviations used in this document

- **AML/CFT:** Anti-money laundering / combating funding of terrorism
- **CDD:** Customer due diligence
- **EDD:** Enhanced customer due diligence
- **EU:** European Union
- **FIU:** Financial Intelligence Unit
- **ML/FT:** Money laundering and funding of terrorism
- **MLRO:** Money Laundering Reporting Officer
- **PEP:** Politically exposed person
- **RBA:** Risk-based Approach
- **STR:** Suspicious transaction report

1. Know Your Customer (KYC)

1.1 Registration

In order to use our service, customers are required to register. For registration customers need to provide our business with the following details:

1. Email address
2. Username
3. Password
4. Password confirmation
5. Full name (first name, last name)
6. Date of birth

7. Permanent residential address (street and street number, city, postal code, country)
8. Identity reference number
9. Mobile number (optional)

To complete the first registration phase (before CDD/EDD), the customer needs to verify the provided email or mobile number. A table indicating the customer privileges based on the verification stage is provided below.

#	Registration phase	Can login	Can play	Can deposit	Can withdraw
1	Registration without email/mobile verification	NO	NO	NO	NO
2	Registration with email/mobile verification but not CDD/EDD	YES	YES, but subject to limited number of bets (verification pending)	YES, but limited amount of deposits or total amount of deposits (verification pending)	NO
3	Registration with full verification	YES	YES	YES, however subject to EDD procedures based on risk	YES, however subject to EDD procedures based on risk

1.1.1 Registration Procedure

1. Customer visits our web-based service to register
2. Customer's country origin (via IP address) is checked to verify that it is within the countries of our operation
3. Customer completes the registration form
4. Customer details are validated with the following rules:
 1. Email must be unique among other registered customers
 2. Username must be unique among other registered customers
 3. Identity number must be unique among other registered customers
 4. Mobile number must be unique among other registered customers
 5. Passwords must be strong. A minimum of 8-10 characters long phrase that should at least include: 1 uppercase letter, 1 lowercase letter, 1 number and 1 special symbol
 6. Passwords should not contain the username, email, mobile number, date of birth or identity number of the customer
 7. Customer age is calculated based on the given date of birth. Customers should not be minors.
5. If validation is successful, the customer is registered

6. Service sends verification email to the customer's email address; once verified, the customer can login to our application
7. (Optional) Service sends verification SMS to the customer's mobile number

1.1.2 Working with minors

- Registrations with birth dates that indicate that a customer is a minor are not accepted by the service.
- If minors register with false details and provide legitimate documents for identification, this will result in their account being closed.

1.2 Verification

Since during registration, the customer is not physically present but rather performs it via the internet, we apply CDD and risk-based EDD. EDD is always required as the customers' risk level for ML/FT activities is considered high, due to the nature of the service (over the internet non face-to-face transactions).

1.2.1 Email Verification Process

1. Customer registers with a unique email address
2. A verification email is sent to the email address specified by the customer, including a verification link
3. Customers click on the link to verify their email address
4. Email address of the customer's account is verified

1.2.2 Mobile Verification Process

1. Customer registers with a unique mobile phone
2. A verification message (SMS) is sent to the mobile number of the customer, including a 6-digit code (numbers)
3. The customer inputs the code in the mobile verification page of our service
4. Upon successful completion, the mobile of the customer is verified

In most countries, including the country/ies in which this service operates, mobile numbers of a natural person are registered and are associated with the natural person. Verification of the mobile can be considered as a means of CDD, since it is verified by mobile providers.

1.2.3 Customer Due Diligence (CDD)

- CDD always takes place after the user registration and before the user withdraws any funds from their account.
- CDD also can take place before the customer deposits any amount other than the default limited amount that is meant to be allowed so that customers can test how the service works and what functionality it provides.

1.2.3.1 CDD Measures

- Identity Verification
- IP-check

- Double customer Check

1.2.3.2 Identification details

Upon registration customers are required to provide additional documents so that their identity can be established/verified. CDD is needed to identify potential money laundering activity. The customer's profile needs to be updated constantly so any unusual and suspicious activity can be identified and addressed. The identification details that need to be verified so that the customer can be considered as verified are the following:

- Official Full Name
- Date of Birth
- Identity Reference Number
- Permanent Residential Address
- Nationality

1.2.3.3 Verification Documents

Verification takes place by making reference to official documents, data or information obtained from a reliable and independent source. For the purposes of verification, a reliable and independent source is considered one of the following: a government authority, department or agency, a regulated utility company or a subject person carrying out relevant financial business in Malta or a member state of the EU. This is because such entities would already have verified the identity and characteristics of the person to be verified by our service.

Thus for the verification of full name, date of birth, identification number and nationality, we consult one of the following documents:

- Valid unexpired passport
- Valid unexpired national identity card
- Valid unexpired driving license
- Valid unexpired residence card

For the verification of the residential address, it is performed by making reference to any of the following documents. The documents must not be more than 6 months old, thus any provided document must specify the date it was issued. The customer's full name and address must be present and be accurate in all of the listed documents.

- a utility bill (water supply company; power supply company; heating supply company; communication services — landline; mobile phone bills will not be accepted, since the residential address is not considered permanent)
- a statement from a recognized credit institution or bank
- an official conduct certificate
- correspondence from a central or local government authority, department or agency
- a record of a visit to the address by a senior official of the subject person

- an identification document listed (passport; national identity card; driving license; residence card) where a clear indication of the residential address is provided
- any other government-issued document not mentioned above

1.3 Enhanced Customer Due Diligence (EDD)

Since our customers are not face-to-face and our services are provided over the internet, the ML/FT risk is by default considered to be high and EDD must be applied. However, the extent to which we apply the EDD is determined by the individual customer's risk level and our risk management procedures. All customers are subjects of EDD. When we apply EDD, we essentially apply extra measures to our customers so that we can have more identification details and minimize the risks of ML/FT. Currently, EDD is performed:

- Always for new payment details (deposit/withdraw) debit/credit cards, bank accounts
- Periodically, based on customer risk level

In order to properly address the needs arising from EDD, we apply one or more of the following measures:

1. Establish the identity of the customer with additional documentation and information
 1. As provided in section Verification Documents (sections in this document)
 2. Documents for EDD must be additional to the documents of CDD
 3. Documents for EDD that are of the same type (e.g. utility bill) with documents obtained for CDD purposes, must be issued from different entities/service providers
2. Use supplementary measures to verify the provided documentation
 1. Certification by legal professional, accountancy professional, a notary or a person undertaking relevant financial business
 2. Obtained documents must be a true copy of the original, seen and verified by the certifier, including a photo of the subject customer
 3. The certification must include the certifier's signature, profession, contact details and the document's review date
 4. Extra attention should be paid to certified documents originating from high-risk jurisdictions
3. Confirm (certify) the documentation, using a person carrying out relevant business with the subject

1.3.1 Politically Exposed Persons (PEPs)

A PEP is defined as a natural person who is or has been entrusted with prominent public functions. Close family members or persons known to be close associates of such persons (PEPs) are also considered as PEPs in the eyes of the law. Close family members include:

- spouse/partner (recognized by law)
- children and their spouses
- the parents

PEPs are considered a high risk in regards to ML/FT because of their position which makes them vulnerable to bribery via funds that originate from illegal activities. Based on that, we apply extra EDD measures in relation to PEPs. These are:

- Ask for senior management approval (risk management officer)
- Establish the source of wealth and funds of the PEP
- Enhanced monitoring

To identify PEPs we consult the available PEP lists available in the countries of our operation. In case that the details of a customer potentially show that the subject customer is a public figure or a relative of one, we contact the customer and we apply EDD as described above.

2. Risk-based Approach (RBA)

Risk-management procedures are applied to control and mitigate higher risk situations. Although RBA is optional, we have decided that it is a more appropriate approach to follow for the purposes of our business instead of the rule-based approach. The purpose of the RBA is not to restrict our customers from performing transactions with our business but rather evaluate the risks and when appropriate tackle them in an effective manner by performing EDD procedures. All customers regardless of their risk level go through the CDD procedures, even if they are marked as low risk customers.

2.1 Company's Risk Profile

1. Risk originating from Customers (target customers): our customers are non face-to-face customers; thus, the risk is HIGH (6-8/10)
2. Risk originating from Service/Product: we operate a web-based betting platform; thus, the risk is HIGH (6-8/10)
3. Risk originating from the Interface (connecting customers with the service): the Internet connects our business with our customers and vice versa; thus, the risk is HIGH (6-8/10)
4. Risk originating from Geographical location: the business can operate in several countries (based on the respective licenses); thus the risk is HIGH (6-8/10)

As it can be observed our business has a HIGH risk based on these 4 factors. Since our customers are not face-to-face, the risk is by default considered to be high and EDD must be applied. We are not accepting cash as a payment method; certain risks are minimized because the payment options we offer to our customers go through verified and reputable payment providers that also apply CDD and EDD procedures. However, this only means that we have a better chance of identifying ML/FT activities and not that we will solely rely on these services to perform AML/CFT.

2.2 Customer identification programme

Initially all customers are obliged to submit:

- A document for establishing their identity

- A document for verifying their residence address
- A document for verifying the ownership of the accounts used for transactions

2.3 Customer risk Classification

Customers are classified from a scale of low to high risk. This scale is indicated by 1-6. When a customer joins our business we by default give a risk level of 3 which is considered the default risk for new users on our platform. As discussed, due to the fact of dealing with non face-to-face customers, all customers go through both CDD and EDD, by default. What changes is the frequency, intensity of such verifications and also other factors, such as bet, deposit and withdrawal limits.

Subsequently, the customer risk level is calculated and adjusted based on the customer's activity and activity patterns. Higher levels of risks indicate the need of applying further EDD but also might result in restricting the use of the service and/or reporting incidents to the respective authorities. In relation to mitigating the risks, we do not solely perform EDD, but also we apply certain service limitations for customers with high risks:

- Bet limits can be applied (amount)
- Bet delay can be applied (in seconds)
- Customers might be restricted to use certain payment methods of the service
- Customers might be restricted from using certain parts of the service (e.g. casino section)
- Customers might not be able to perform transactions at all until EDD checks are completed
- Customers will be reported to the official authorities (FIU) in case that we identify ML/FT activities

2.4 Monitoring

Implementing effective risk management processes requires monitoring. In accordance to that we:

1. Monitor mitigation strategies (controls) and risks so that controls are always updated in accordance to the risks we face
2. Monitor changes over the customer details and behavior, so that we can better identify risks for specific customers
3. Perform audits to review risk management, mitigation strategies and employee compliance

2.5 Employee Training

- Employees are given adequate training and documentation so that they are aware of and compliant to our AML/CFT processes.
- Employees' training and compliance are checked periodically.

3. Record Keeping

Customer records that are related with CDD, EDD and transactions are required to be stored for the purposes of complying with the AML/CFT regulations. Such records may be requested from the FIU in case an investigation for a customer takes place.

The records to be retained include the following:

- records of the CDD/EDD documents used for customer identification/verification (copy of ID document; copy of bank/credit statement; copy of utility bills)
- records containing details relating to the transactions performed by the customer (deposit/withdrawal methods; ID of the person performing the transaction; destination of funds; volume of transactions)
- records of the findings of the examination of the background and purpose of the relationship and transactions carried out

3.1 Retention Period

The records are retained for a period of at least 5 years (or the years required for a specific region of operations) from the end of the business relationship with the customer. Storing such records is an obligation by law, and the General Data Protection Regulation (GDPR) will not have an impact on such records (strictly related with the documents presented above).

4. Money Laundering Reporting Officer (MLRO)

The MLRO is always notified when there is suspicion about ML activities. The MLRO receives training about the ML/FT risks of the company. The responsibilities of the MLRO are:

1. Receive reports of knowledge or suspicion for ML/FT
2. Evaluate such reports to determine whether ML/FT suspicion is evident (subsists)
3. Report knowledge or suspicion of ML/FT to the FIU (STR)
4. Respond promptly (within 5 days) to any request for information made by the FIU
5. Keep up to date with AML/CFT legislations
6. Supervise the AML training that is periodically given to staff
7. Record and update risks

Note that the MLRO is responsible to contact the FIU within 5 working days from the moment an incident involving a suspicious person or transaction is identified.