

KYC Procedures

Date	Version
24.05.2024	Version 1.0
29.01.2025	Version 2.0

All procedures taken from Bluewave Interactive N.V AML Policies and Procedures

6.1 SIMPLIFIED DUE DILIGENCE

A Simplified Due Diligence process will be the first stage of a risk based process. Simplified Due Diligence is carried out between Registration and First Deposit on Customers that hail from low risk jurisdictions.

Simplified due diligence is performed by the customer providing identification details prior to registration.

Every registering player must provide all the details / fields included in the registration process document of the company. This document meets the requirements for “identification of customers”, and include:

- the date of birth;
- the player’s identity;
- the player’s place of residence; and the player’s valid e-mail address.

Every registering player must activate the account via the email. Once a customer completes the registration form and verifies the email, then the account is opened and found within the back office system.

It is company policy not to allow players to deposit or withdraw any funds whatsoever before Standard Due Diligence is carried out.

6.2 REGULAR DUE DILIGENCE

The company conducts Regular Due Diligence in two distinct methods, which are both equally acceptable. Therefore, the company are able to select the method they can adopt from the following:

- Electronic Verification
- Documentary Evidence

6.3 CONTINUED DUE DILIGENCE

When a customer hits the Medium or High on the Risk Based Approach we will carry out further checks on the account and leave a clear note:

Is ID expired? Have new payment methods been used that we need copies of?

Has pattern changed, do we need to update risk level of customer?

If we have SOW questionnaire do the answers still match the pattern?

KYC requests will have the same 30-day grace periods to send documents

A clear note should read something like:

CDD: ID expired, new ID requested, CC**6789 not yet received, requested now. Deposit and gameplay pattern remains unchanged

Any failure to provide documents and complete CDD measures will result in remitting the funds to the same source through the same channels used to receive funds (subject to approval in case of medium and high risk players).

6.4 DOCUMENTARY EVIDENCE METHOD

KYC- Standard Due Diligence - This is achieved by the following thresholds triggering the Standard Due Diligence process:

- Cumulative Deposits exceeding €2,000;
- Attempt to withdraw to a different card or payment method;
- Attempt to make a name change;

In order to verify the details on their account, the company must ask the customer to send a photo or scan of one document from each of the categories listed below:

- 1) Personal Identification - one photo ID from the following list (valid for 6 months):
- 2) Current Signed passport
- 3) Current photo-card Driver's License (Provisional or Full)
- 4) Current Full Driver's License (old style paper version)
- 5) Current Identity Card (Different Types accepted depending on the country)

Address Verification - one of the following:

- 1) Utility bill (within last 3 months)
- 2) Current photo-card Driver's License (Provisional or Full) (Applies for UK DL's)
- 3) Current Full Driver's License (old style paper version)
- 4) ID card with address + Passport or additional ID
- 5) Bank/Credit Union/Building Society/Credit Card statement or passbook (within last 6 months)
- 6) Council tax bill or payment book (within last 6 months)
- 7) Recent mortgage statement (within last 6 months)
- 8) Current local council rent card or tenancy agreement (private tenancy agreements are not acceptable)
- 9) Home Insurance certificate or policy
- 10) Motor Insurance certificate or policy
- 11) Electoral roll
- 12) Credit reference agency
- 13) Mobile bills are not accepted

Source of Payment Verification/Proof of Payment - one of the following:

- 1) Registered Credit or Debit card

- 2) Copy of Credit or Debit card account statement of a card registered (less than 6 months old)
- 3) Copy of bank statement - must have Company transaction or card number visible on it (less than 3 months old)
- 4) Screenshot of Back office showing ownership (E-wallets, Skrill, Neteller, etc.)

When requesting such documentation, the customer must always be informed that:

- 1) The card number must be blanked out leaving only the last four digits visible together with the start and expiry date.
- 2) The documents must be clear and legible and in colour.
- 3) The documents should show the residential address.

6.5 ENHANCED DUE DILIGENCE

Following a risk based approach for customer due diligence, certain triggers or thresholds will require enhanced due diligence to take place. The triggers for the enhanced due diligence process to take place are as follow-:

- 4) Customer identified as politically exposed persons (PEPs);
- 5) Lifetime customer deposits exceeding EUR 15,000 (Net Deposits); EUR 40,000 and EUR 100,000 +.
- 6) Customer identified as high risk when carrying out Risk Assessment;
- 7) Customers identified at medium risk (if necessary)
- 8) Regular Due Diligence identifies heightened risks;
- 9) Significant anomalies in gaming or funding activity;
- 10) Source of Wealth provided by customer cannot be verified following soft verifications and the customer is a High Spender or has Disproportionate Spending.

When performing Enhanced Due Diligence on a customer we always make sure to:

- Ask for additional ID Verification which include document showing Nationality and Place of Birth (Eg: Passport if only ID/DL is available)
- Ask for additional Proof of Address
- Validation of documents – we can request certified copies of documents to validate name, address, date of birth and source of funds; and/or
- Internal corroboration of user identity – this could emanate from a variety of sources from customer monitoring, other databases, gaming activity etc.; and/or
- External corroboration – this can entail the use of a 3rd party solution to provide enhanced soft background checks on public records;

6.6 SOURCE OF FUNDS/WEALTH

Source of Funds refers to how the funds to be used in a particular transaction (or future transactions) will be generated.

Source of Funds checks consisting of the following:

- Last 3 Payslips
- Employment Contracts
- Proof of Deposits
- Bank Statements
- Inheritance Confirmations/Wills
- Investment gains
- Deed of Donation
- Sale of Real Estate
- Gambling Winnings
- Any additional document deemed necessary to deem how funds were generated.

6.7 SOURCE OF WEALTH QUESTIONNAIRE/DOCUMENTATION

Customer due diligence is an ongoing process and as a result there are trigger events which warrant the collection of supporting documentation.

Source of Wealth refers to how someone generated their wealth throughout their lifetime.

Upon classifying a player as High risk the client will be requested to complete a Source of Wealth (SOW) questionnaire and if warranted the client will be asked to provide SOW documentation.

It is understood that the players may not have at hand the requested information thus the company has determined an acceptable timeframe of 30 days shall pass before we close the customer's account.

During this period, the players' account will remain partially operational.

6.8 PENDING WITHDRAWAL CANCELATION

KYC will be requested by the RPF Agents. A reminder will be sent to customers in 4 days. If no documents are received within 30 days from the initial KYC request, the customer's account will be closed. If no further communication is received the account will remain closed and the withdrawal will be cancelled. The RPF Agents will also send an email to the customer, explaining the situation and letting them know that prior to opening account, we will need to receive the required KYC documents.

6.9 CLIENTS REFUSING TO SEND DOCUMENTS

Any client who refuses to send documents will have their account disabled.

Customer Support will try to explain to the client the importance of receiving and verifying their documents, however if the client is still refusing to listen and will not send documents, the customer's account will be reviewed for any suspicions of AML/CFT.

The MLRO will be notified if any accounts are deemed suspicious and will then review the clients account and communications and consider whether to submit an STR to the FIAU, providing all details and information as appropriate, if the MLRO decides not to submit an STR they need to include their reason/s in the suspicious register.

Once it is stipulated that their account is of no risk the customer's funds will be remitted back to the same source and channels used for depositing.

7.3 KYC DOCUMENTATION REVIEW

The below mentioned table depicts the manual trigger event based on KYC aging, warranting a player review (player interaction required) or desk top review (no player interaction review required).

Risk Rating	Frequency from date of last review or customer interaction	Registered through conventional channel
High	Every 3 months or upon withdrawal	Check Identification document expiry date, collect new one where warranted and assess if an updated SOW document needs to be collected
Medium	Every 6 months or upon withdrawal	Check Identification document expiry date, collect new one where warranted and assess if an updated SOW document needs to be collected
Low	As triggered through the transaction monitoring process	Check Identification document expiry date, collect new one where warranted and assess if an updated SOW document needs to be collected

The Company must carry out PEP checks at the first possible opportunity.

These checks are carried out on customers' first deposit.

When a player is a confirmed PEP, it will be classified as high risk and senior management approval will be sought before any business is undertaken. In such cases, adequate measures will be taken to establish the source of funds and source of wealth involved in the prospective business relationship. If senior management decides to establish a relationship with the PEP, enhanced ongoing monitoring will be carried out in order to mitigate this high risk.

As a general company policy, the Company prefers not to accept any PEPs, however senior management has discretion to alter the policy.

Politically Exposed Person is defined as any of the following resident in any country:

(a) 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;
- 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 organisation; and
- an honorary consul;

(b) any of the following family members of a person mentioned in sub-paragraph (a) —

- a spouse;
- a partner considered by national law as equivalent to a spouse;
- a child;
- the spouse or partner of a child;
- a sibling;
- a parent;
- a parent-in-law;
- a grandparent; or
- a grandchild;

(c) any close associate of a person mentioned in sub-paragraph (a), including —

- any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;
- any natural person who has sole beneficial ownership of a legal entity or legal arrangement that is known to have been set up for the benefit of such a person;
- any natural person who is in a position to conduct substantial financial transactions on behalf of such a person.

These clients are classified as High risk.

Any client which is flagged in these lists:

- Will have his account locked;
- the client may be asked for enhanced due diligence to verify the customer

Clients in this list are required to send:

- Passport/Driver's licence
- Send an original utility bill not older than 3 months;
- Any other documentation that is deemed necessary

4.2 SANCTION CHECKS

Sanction checks are carried out upon registration.

When a customer has been confirmed as being on a Sanction List, the account will be blocked immediately.

If in the event a Sanction check was missed and a transaction has occurred, or in the event a current customer is now on the Sanctions List and previous transactions have occurred, the account will be marked as high risk and the account will be frozen (all transactions will be stopped from going through).

An email will be sent to management and the MLRO to inform of this occurrence.

As stated in the Guidance note on the application of Article 17(6)(a), (b) and (c) of the National Interest (Enabling Powers) Act, Once the MLRO is aware of this instance an email will be sent to sanctions.mfea@gov.mt

Changes and updates to the email address may be found here <https://foreign.gov.mt/en/Government/SMB/Pages/SMB-Home.aspx>

Sanctions List means the “Specially Designated Nationals and Blocked Persons” list maintained by OFAC, the Consolidated List of Financial Sanctions Targets and the Investment Ban List maintained by HMT, or

any similar list maintained by, or public announcement of Sanctions designation made by, any of the Sanctions Authorities.

As a general company policy, the Company will not accept any Sanctioned Individuals

These clients are classified as High risk.

Any client which is flagged in these lists:

- Will have his account locked;
- the client may be asked for enhanced due diligence to verify the customer

Clients in this list are required to send:

- Passport/Driver's licence/ID
- Send an original utility bill not older than 6 months;
- Any other documentation that is deemed necessary

4.3 ADVERSE MEDIA

Adverse media, from a compliance perspective, is generally considered to include allegations found in reputable news and other publications that link a person or entity to involvement in money-laundering, corruption, sanctions exposure, terrorism and threat financing, or other unlawful activity.

These clients are classified as High risk.

Any client which is flagged in these lists:

- Will have his account locked;
- the client may be asked for enhanced due diligence to verify the customer

Clients in this list are required to send:

- Passport/Driver's licence
- Send an original utility bill not older than 3 months;
- Any other documentation that is deemed necessary

4.4 PEP SCREENING

All customers who have deposited for the first time will have undergone an automatic PEP check within the Hooyu system.

On-going checks are currently conducted via a manual upload within Hooyu's system.

On a monthly basis we run a report of all active first time depositors and this report is then manually uploaded to Hooyu ongoing monitoring database. This report is uploaded by either the MLRO or Senior Analysts on the first working day of each month. In order to ensure all accounts are successfully uploaded a popup notification will show as successful, if not the same popup notification will show the data row of the error.

Once customers are uploaded here they will be checked constantly for any changes in their profile. If and when a customer has now appeared as a PEP, on a Sanctioned list or has had any adverse media, this will trigger an alert for the Risk Fraud and Payments team to handle and review the account.

This policy will be updated on a yearly basis, or updated as required