Account Verification and Documents

Aleksander Wilk

Contents

KYC and AML 4
Related documents 12

- **Documents at first withdrawal:** JV-W01: identity document and proof of address; withdrawal to own MiFinity after acceptance of KYC.
- **Documents at repeat withdrawal:** JV-W02: previously accepted KYC preserved, no repeat documents were requested in this episode.
- **Types of requested documents:** ID and a bank statement with an address in JV-W01; for the card route, card data is masked according to the rules: the first 6 and last 4 digits are visible, CVV is hidden.
- **Reason for repeat request KYC:** A repeat request is possible upon a change of address/payment method, document expiry, an unusual transaction or AML risk; in JV-W02 there were no such changes.
- **Verification time KYC:** 12.11.2026 11:02:00–11:11:30+01:00 = 9,5 min; these 9,5 min are included in the confirmation of JV-W01 41,6 min.
- **Verification result KYC:** Documents JV-W01 accepted, name and address matched the profile and the payment instrument; verification status preserved at JV-W02.

KYC and AML

Provision	What the source says
Purposes	Warning of breach of rules, money laundering and terrorist financing, access by children, fraud, collusion, legal, financial and reputational risk.
Assessment	Risk by country, user and transaction using the FATF model. The indicators include EU/FATF lists, EU/UN sanctions, PEP status, signs of corruption and terrorist financing, unusual volumes and combinations of transactions, inconsistent geodata and shared use of account contexts.
Standard verification	In the KYC policy §4 — when the aggregate transaction amount is **at least 1 000 USD/EUR**, there is a substantial AML/CTF risk, suspicion of a breach of rules, or at an employee's decision. A separate rule for withdrawal from §8.3.6 and the cancellation policy — when the requested payout **exceeds 1 000 USD**. There are also general powers to request identification at any time.
Possible documents	Identity document, a card with a matching owner name, a selfie with documents, proof of address if necessary (utility or phone bill or equivalent), bank statement, a letter from an employer or authority, a tax document, a selfie with a sheet showing the registration email, the date of the request and a code, and other materials as the situation requires. A conversation with support is possible, including video.
Images of documents	Original, legible, authentic materials are required. §6.7 prohibits digital retouching, filters, substitution, AI and deepfake. Under certain payment rules, the provided masking is permitted: the passport series and number may be hidden; on the card, the first 6 and last 4 digits remain, CVV2 is hidden, and under the KYC policy the cardholder's name is not hidden. The cancellation policy for card deposits indicates both sides of the card.
Reaction to incomplete or inaccurate data	Restriction of withdrawal during verification, blocking/closure, refusal or delay of verification, annulment of bonuses and winnings, cancellation of pending payouts, retention of funds obtained in breach, possible reporting to authorities. The Company may use manual and automated review of materials and participate in checks with third parties, including regulators.
Enhanced verification	For PEPs, close family members, high-risk jurisdictions and at the operator's discretion. Documents or information on the source of funds (SOF) are required; large deposits may also require confirmation of salary/employment and bank statements. Additional verification is approved by senior management. The player must report their PEP status to support after registration.
Who is classified as a PEP	Heads of state and government, ministers/deputies, parliamentarians, party leaders, senior judges, members of courts of auditors and central bank leadership, ambassadors/chargés d'affaires and senior military officers, management/supervision of state-owned companies, leaders and members of bodies of international organisations. Middle and junior levels are excluded from this definition. Family — spouse/partner, children and spouses/partners of children.
Monitoring of transactions	Owners of payment instruments are checked, including the address in the e-wallet and the account email. If a return to the original instrument is impossible, the KYC policy permits a bank account or another instrument after confirming it belongs to the player. Suspicious cases are referred to the fraud prevention department.
Anonymous instruments	§7 of the KYC policy does not accept anonymous payment instruments and cites cryptocurrencies and anonymous wallets as examples. The cashier and the public storefront simultaneously show specific crypto methods. The crypto route does not remove verification of ownership and origin of funds; in JV-D01 personal funds and a subsequent KYC were used.

Provision	What the source says
Data retention	The policy refers to Directive (EU) 2015/849, the GDPR (EU) 2016/679, Cyprus law 66(I)/2012 and its own privacy policy. For changes to KYC, an e-mail to the registered e-mail address is promised. Further use after notification is treated as acceptance of the terms.

If age cannot be confirmed, the account may be suspended. If it is established that the person is a minor, the regulations provide for closure, annulment of transactions, loss of winnings and return of amounts paid upon request. §6.5.2 speaks of returning deposited funds after coming of age. A separate AML page speaks of returning the relevant deposits without this time limit, as well as cancellation and return of bets for the period of minority. Both wordings have been retained.

- In the document upload materials, KYC separately shows examples of the front and back of an identity document and driving licence, a passport, both sides of a card, e-wallet and bank transfer confirmations, a utility bill, a bank statement and a phone bill. The widget invites you to upload the requested documents and promises to review them "as quickly as possible" without a numerical time limit.

6. IDENTITY VERIFICATION; ANTI-MONEY LAUNDERING REQUIREMENTS

6.1. By using our services, you agree and confirm that:

6.1.1. You are at least 18 years old or meet the age requirements entitling you to gamble in your jurisdiction.

6.1.2. You are the lawful owner of the funds in your account. All information provided during registration or later, including payment data, is true, accurate, current and complete and corresponds to the data of the owner of the payment accounts used for transactions.

6.1.3. You understand that gambling involves the risk of losing money and you accept full responsibility for any losses incurred. You use the services at your own risk and discretion, and the Company is not liable for such losses.

6.1.4. You know the methods, rules and procedures related to our services and to online gambling in general. You acknowledge that you are responsible for the accuracy of your bets and game details. You undertake not to take any actions that could harm the Company's reputation.

6.2. By accepting these Terms and Conditions, you authorise us to carry out any necessary checks to confirm your identity and contact details. These checks may involve third parties, including regulatory authorities.

6.3. During the verification process, you may be temporarily restricted from withdrawing funds from your account.

6.4. If any information you provide turns out to be untrue, inaccurate, misleading or incomplete, you will breach the Terms and Conditions. We reserve the right to immediately close your account and prevent further use of our services, as well as to take other actions we deem necessary.

6.5. If we are unable to confirm that you meet the age requirements for gambling, we may suspend your account. If it is established that you were a minor at the time of entering into any gambling transactions or games, the following actions will be taken:

6.5.1. Your account will be closed.

6.5.2. All transactions carried out while you were a minor will be voided, and any deposited funds will be returned to you upon reaching the age of majority.

6.5.3. Any bets or stakes placed during the period when you were a minor will be deemed invalid.

6.5.4. Any winnings accumulated while you were a minor will be forfeited, and you will be obliged to return any funds paid out from the account.

6.6. For large deposits, we may ask for confirmation of the source of funds (SOF). You may be asked to provide additional information and documents showing that you have sufficient funds to finance your gambling activity. This may include information about remuneration or place of employment confirmed by appropriate documentation, such as bank statements.

6.7. Submission of authentic and unaltered documents

6.7.1. For the purpose of identity verification, payment verification, checking the source of funds or conducting other compliance procedures, you undertake to provide only original, authentic and unaltered documents, photographs and supporting materials.

6.7.2. The use of any photo editing software, artificial intelligence (AI) tools, deepfake technology, image generators, graphic manipulation applications, filters, background changing tools, image enhancement software or any other methods of digital modification to alter, improve, conceal, forge, generate or manipulate identity documents, selfies, payment confirmations or any verification materials submitted to the Company is strictly prohibited.

6.7.3. All documents and images submitted to the Company must be complete, clearly visible and faithfully reflect the original physical document without any modification, concealment, forgery or digital interference.

6.7.4. Detection or reasonable suspicion of the use of edited, manipulated, AI-generated, forged or falsified materials will constitute a material breach of these Terms and may be deemed fraudulent activity in accordance with Clause 11 (Collusion, Fraud, Abuse and Criminal Activity).

6.7.5. In such cases, the Company reserves the right, at its sole discretion, to:

• refuse or delay verification procedures;

• suspend or permanently close your Account;

• void any winnings, bonuses or promotional benefits;

• cancel pending withdrawals;

• confiscate funds obtained in breach of these Terms;

• report the matter to the relevant authorities, financial institutions or regulatory bodies where required by applicable law.

6.7.6. The Company reserves the right to conduct technical, forensic, automated and manual analysis of the submitted materials in order to detect any form of digital manipulation, artificial generation, forgery or interference.

KYC Policy — client verification

1. INTRODUCTION.

This “Know Your Customer” policy (hereinafter the “Policy”) sets out the application of the “Know Your Customer” procedure by the Company (hereinafter the “Company”, “We”, “Us”, “Our”).

For the purposes of this Policy:

a) the website JV.Casino is referred to as the “Service”;

b) any natural person holding an account on the Service is referred to as the “User”.

2. OBJECTIVES OF THIS POLICY.

The Company applies the measures set out in this Policy for the following purposes:

To prevent breaches of the Service Regulations and other applicable documents;

To prevent money laundering, terrorist financing and other breaches of AML/CTF regulations;

To prevent the use of the Service by children;

To prevent fraud, collusion and any other non-compliant or unlawful activities within the Service;

To prevent any legal and financial risks and the danger of reputational loss.

3. RISK ASSESSMENT.

The Company applies the risk-based approach recommended by the Financial Actions Task Force (FATF) in order to assess each User to the extent specified in this Policy.

The risks have been categorised as follows

Geographic / country risk. The Company assesses the User's country of residence/domicile taking into account, among other things, the following criteria:

Whether the User's country of residence (jurisdiction) is identified by the European Commission as a “third country with strategic deficiencies” (in accordance with Commission Delegated Regulation (EU) 2016/1675 or any other regulations amending that regulation) and whether the User's jurisdiction is on the list of “high-risk and other monitored jurisdictions” FATF;

Whether the User's country of residence (jurisdiction) is identified by a credible source as lacking adequate anti-money laundering and counter-terrorist financing safeguards or is identified by credible sources as a country with a high level of corruption, supportive of terrorists or their activities.

User-related risk. The Company checks the User of the Service taking into account, among other things, the following criteria:

Whether the User is a politically exposed person;

Whether the User is subject to sanctions of the European Union or the United Nations;

Whether the User's activity raises suspicion. Examples of suspicious activity include, among others: a) excessive deposits of funds; b) use of multiple devices to access the Service within a short period of time; c) use of the User's device by other Users of the Service; d) use of a single IP address by several Users; e) use of a single

electronic device by several Users.

Transaction-related risk. The Company checks the User's spending to ensure that it is not too large and/or disproportionate. If the User's transaction appears suspicious, the Company applies additional measures (see “transaction monitoring”).

4. VERIFICATION.

The Company carries out standard verification (in the legal sense — exercises due diligence) in the following cases:

A. The total amount of transactions carried out by the User through the Service is at least 1000 USD/EUR;

B. In the risk assessment process it was found that the User poses a significant money laundering or terrorist financing risk;

C. The User's behaviour raises concerns that the User is using the Service in a manner that breaches the Regulations;

D. In other cases — if the Company's employees considered verification to be necessary.

When carrying out standard verification, the Company asks the User to submit documents. These are:

A copy or photo of the User's identity document;

A photo of the payment card that the User used or wants to use to make a deposit on the Service. The cardholder's first and last name must match the first and last name of the verified User. The CVV code and the payment card number (except for the first 6 and last 4 digits) may be hidden or covered. The cardholder's first and last name may not be hidden or covered in any way.

A photo of the User showing the documents required to complete verification.

In some cases, a document confirming the User's address of residence. For example, a utility bill, telephone bill or other document that, under local law, is considered sufficient to confirm the User's address.

In some cases, a bank statement, a letter from a public office or employer.

In some cases, a tax statement.

A photo of the User holding a piece of paper on which the following information is handwritten: a) the User's email address provided during registration and b) the date of the photo request and the confirmation code.

Other documents or data that the given situation may require.

In some cases, the Company may require the User to hold a conversation with the Service's Customer Support (including a video call).

5. ADDITIONAL VERIFICATION OF POLITICALLY EXPOSED PERSONS AND USERS IN HIGH-RISK JURISDICTIONS.

The Company carries out additional verification in the following cases:

A) The User is a politically exposed person within the meaning of Article 3(9) of 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 purpose of money laundering or terrorist financing, or the User is a family member of a politically exposed

person.

Pursuant to Article 3(9) of the aforementioned Directive, politically exposed persons are natural persons who have held or hold prominent public functions, including:

(a) heads of state, heads of government, ministers or deputy ministers;

(b) members of parliament or similar legislative bodies;

(c) members of the governing bodies of political parties;

(d) members of supreme courts, constitutional tribunals and other high-level judicial bodies whose decisions are not subject to appeal, except in extraordinary procedures;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, chargés d'affaires and high-ranking officers of the armed forces;

(g) members of the administrative, management or supervisory bodies of state-owned enterprises.

(h) directors, deputy directors and members of the boards of international organisations or persons performing equivalent functions in those organisations.

The above list excludes middle-ranking and lower-ranking officials.

Article 3(10) of Directive 2015/849 defines a “family member” as follows:

(a) the spouse or a person cohabiting with a politically exposed person;

(b) the child of a politically exposed person and their spouse or a person cohabiting with them.

B) The User's country of residence (jurisdiction) is identified by the European Commission as a “third country with strategic deficiencies” (in accordance with Commission Delegated Regulation (EU) 2016/1675 or any other regulations amending that regulation) and/or the User's jurisdiction is on the list of “high-risk and other monitored jurisdictions” FATF;

C) In other cases – if the company has determined that such a procedure is necessary.

D) The User's country of residence (jurisdiction) is identified by a reliable source as lacking adequate anti-money laundering and counter-terrorism financing safeguards, or is identified by reliable sources as a country with a high level of corruption, supporting terrorists or their activities.

As part of the enhanced verification procedure, the Company requires the submission of documents or information specifying the source of the User's income in accordance with the legal requirements in force in the User's country. In addition, completion of the enhanced verification procedure is ultimately approved by the Company's senior management.

The Company reserves the right to collect additional verification data of the User for the purposes of this Policy. In addition, if: a) the User refuses to undergo verification and/or b) the Company has sufficient grounds to believe that the User is using the Service for unlawful purposes, and the User fails to provide evidence to the contrary, the Company may report this to the relevant regulatory/governmental/financial authorities.

6. MONITORING OF ACTIVITY.

All User operations are checked for suspicious activity. Suspicious activity includes, among other things:

Use of multiple payment cards through various payment agents offered by the Company;

A specific error code returned when attempting a payment;

Use of payment cards issued by different issuers from different regions;

Use of various payment instruments within a short period of time (cards, e-wallets, bank transactions);

The User showing reluctance to verify their account or payment instrument, or refusal to undergo such verification;

Geolocation inconsistency of key User data (citizenship, residential address, mobile network operator, IP address, geolocation, payment card BIN number, etc.);

The User's objection to a phone call or video call and the User's failure to provide a photo of themselves holding an identity document (despite the Company's request);

Match of the User's device identification number (phone, computer, tablet) with the identification number of a device assigned to another account in Our system.

If suspicious activity is detected, the case will be referred to the Fraud Prevention Department to assess the risk posed by the User and take further action. The Fraud Prevention Department will assess the case and redirect it to the appropriate department for further review.

7. MONITORING OF TRANSACTIONS.

All User transactions involving the deposit or withdrawal of funds must meet the following requirements:

For transactions using payment cards, the cardholder's first and last name must match the first and last name of the account owner in the Service. Accordingly, the use of third-party payment cards is prohibited.

For transactions using an e-wallet, the email address linked to the e-wallet must match the address used by the User to create an account in the Service.

If a deposit was made from a payment instrument and the funds cannot be withdrawn to the same payment instrument, the funds are withdrawn to the User's bank account or to another payment instrument – provided that it has been reliably established that this new payment instrument belongs to the given User.

The Company does not accept payments made using payment instruments that provide anonymity (cryptocurrencies, anonymous wallets, etc.).

The Company does not pay out funds deposited by one User to another User's payment instrument.

8. STORAGE OF DOCUMENTS AND USER DATA.

Documents and data collected during verification, as well as other financial data (including transaction data and supporting evidence), are collected, stored, shared and protected in accordance with:

European Union legislation on preventing the use of the financial system for money laundering or terrorist financing, specifically Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on preventing the use of the financial system for money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC;

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or “GDPR”);

The Limitation of Actions Law (Law 66(I)/2012) of the Republic of Cyprus;

The Service's Privacy Policy.

9. AMENDMENTS AND CHANGES.

This Policy may be changed or amended at any time and at the Company's discretion. The User is obliged to periodically check the content of this Policy for changes and amendments. Registered Users are notified of any changes to this Policy by email sent to the address provided during registration of an account in the Service. Continued use of the Service after the notification has been sent is equivalent to having read and accepted the changes to this Policy.

Anti-money laundering — AML

In consideration of these terms, you warrant, confirm and agree that:

You are at least 18 years old or have reached the age that allows participation in gambling legally in your country.

You are the rightful owner of the funds in your account. All information provided to the Company during the registration process and/or at a later date, including transactions requiring the deposit of funds, is correct, current, accurate and fully corresponds to the name(s) on the credit/debit card(s) or other settlement accounts that will be used to deposit or receive funds to/from your account.

The User is fully aware that there is a risk of losing money while using the services on the website and bears full responsibility for any losses related to the use of the services on this site. You agree to use the services solely at your own choice, decision and risk. You have no right to bring any claims against the Company regarding your losses.

You fully understand the general methods, rules and procedures for using online services and games. You understand that you are responsible for ensuring the correctness of bets and games. You agree not to take any actions that could harm the company's reputation.

By accepting the Terms and Conditions, you grant us the right to conduct inspections periodically at our discretion or as required by third parties (including supervisory authorities) in order to verify your identity and contact details ("Verification").

During the verification process, we may restrict the ability to withdraw funds from the account.

If the information you provide is false, inaccurate, misleading and/or incomplete, you are in breach of the terms of the agreement and we are entitled to immediately close your account and/or refuse use of the Service's services, in addition to any other actions at our discretion.

If we cannot confirm that you have reached the permissible age, we are entitled to suspend your account. If, at the time of participating in operations on the gambling-related website, your age was below the permissible age, then:

Your account will be closed;

All transactions made at that time become invalid, and the corresponding funds deposited by you into the account will be returned;

Any bets placed at that time will be cancelled and returned;

Any winnings accumulated during the period when your age was below the permissible age will be forfeited, and upon demand you will have to return to us all funds that were withdrawn from your account.

Related documents

- Sign-in and Account Recovery (17-11-2026-login.pdf) · section “Related operations of the author”
- Withdrawals, Limits and Processing Times (17-11-2026-withdrawals.pdf) · section “Withdrawal and verification of funds”