



VSMARKETS LTD

(previously Klips CY Ltd)

AML and Account Verification Policy

Version 2.0 | September 2026



1. INTRODUCTION

- 1.1. VSMarkets Ltd (formerly Klips CY Ltd), is a company incorporated in the Republic of Cyprus under registration number HE 431041. The Company is authorised and regulated by the Cyprus Securities and Exchange Commission (“**CySEC**”) as a Cyprus Investment Firm under licence number 434/23 with registered address at 11 Riga Fereou Street, Ground Floor, 3095 Limassol, Cyprus (the “Company”, “**we**”, “**us**” or “**our**”).
- 1.2. This AML and Account Verification Policy (the “**Policy**”) explains, in summary, the measures applied by the Company to prevent its services from being used for money laundering, terrorist financing, proliferation financing, sanctions evasion or other financial crime. It also describes the identification, verification and payment requirements that apply to applicants and clients.
- 1.3. This Policy is client facing and does not replace the Company’s internal Prevention of Money Laundering and Terrorist Financing Manual, risk assessment, procedures or controls. The Company may apply additional or enhanced measures where required by law or by its risk based approach.

2. LEGAL AND REGULATORY FRAMEWORK

- 2.1. The Company maintains policies, procedures and controls designed to comply with the Prevention and Suppression of Money Laundering Activities Law of 2007, Law 188(I)/2007, as amended (the “**AML Law**”), the applicable CySEC Directive for the prevention and suppression of money laundering and terrorist financing, applicable sanctions legislation and other binding legal and regulatory requirements, as amended from time to time.
- 2.2. The Company applies a risk based approach. The nature and extent of due diligence, verification and ongoing monitoring may therefore differ according to the risks presented by the client, beneficial owner, jurisdiction, product, service, delivery channel, transaction pattern, source of funds and source of wealth.

3. SCOPE

- 3.1. This Policy applies to prospective and existing clients of the Company, including natural persons and legal persons, and to persons acting on their behalf. Relevant requirements also apply to beneficial owners, directors, shareholders, authorised representatives and other connected persons where appropriate.

4. CUSTOMER DUE DILIGENCE

- 4.1. Before accepting or continuing a business relationship, the Company applies customer due diligence measures appropriate to the circumstances and risk. These measures include:
 - identifying the client and verifying the client’s identity using reliable and independent documents, data or information;
 - identifying and taking reasonable measures to verify the identity of any beneficial owner and understanding the client’s ownership and control structure;
 - understanding the purpose and intended nature of the business relationship;
 - obtaining information on the client’s occupation or business, financial profile, source of funds and, where appropriate, source of wealth;



- screening relevant persons against applicable sanctions, politically exposed person and other risk related data sources; and
 - conducting ongoing monitoring and keeping due diligence information up to date.
- 4.2. Identity verification is normally completed before the business relationship is established. Where applicable law permits verification to be completed during establishment of the relationship, the Company will do so only where justified, with appropriate risk controls, and will complete verification as soon as practicable. The Company may restrict deposits, withdrawals, trading or other account functionality until the required checks are complete.

5. VERIFICATION REQUIREMENTS FOR NATURAL PERSONS

5.1. Proof of Identity

- 5.1.1. The Company generally accepts a valid, unexpired passport or national identity card issued by a competent governmental authority. The document must be clear, legible and complete and must contain sufficient information to identify the holder, including the holder's full name, photograph, date of birth, document number, issuing country or authority and expiry date, where applicable.
- 5.1.2. The Company may require images of both sides of the document, a live photograph or selfie, a liveness check, video identification, or other electronic identity verification measures. Alternative documents may be accepted only where permitted and considered reliable in the circumstances.

5.2. Proof of Residential Address

- 5.2.1. Where proof of residential address is required, the document must show the client's full name, current residential address, date of issue and the name or logo of the issuer. It must normally have been issued within the preceding six months, unless the Company specifies a shorter period or accepts another reliable source of address verification.
- 5.2.2. Acceptable documents may include:
- a bank or regulated financial institution statement or letter;
 - a utility bill for electricity, water, gas, fixed line telephone or fixed internet service;
 - a tax statement, tax bill or other correspondence issued by a governmental or local authority;
 - a residence certificate or other official government issued document; or
 - another independent and reliable document accepted by the Company.
- 5.2.3. Mobile phone bills, screenshots, envelopes, handwritten documents and documents issued in another person's name are not normally accepted. A payslip is not normally accepted as standalone proof of residential address because it is not generally an independent source of address verification. The Company may request clarification or further evidence where the declared address, document details, IP location or other information is inconsistent.

5.3. Document Quality and Language

- 5.3.1. Documents must be genuine, unaltered, in colour where requested, and submitted with all edges and information visible. The Company may request a certified copy, an original document, an apostille or legalisation, or a translation into English by an acceptable



translator. Documents and information must remain accurate and up to date throughout the relationship.

6. VERIFICATION REQUIREMENTS FOR LEGAL PERSONS

- 6.1. For a company, partnership, trust, foundation or other legal person or legal arrangement, the Company may require documents and information including:
- constitutional and incorporation documents and current registry extracts or certificates;
 - registered office, principal place of business, legal form, registration number and nature of activities;
 - details of directors, partners, trustees, protectors, beneficiaries, authorised representatives and other persons exercising control, as applicable;
 - a board resolution, power of attorney or other evidence authorising the opening and operation of the account;
 - an ownership and control structure and documents identifying the ultimate beneficial owner or owners;
 - identity and address evidence for relevant natural persons;
 - evidence of regulatory status, where applicable; and
 - financial statements, management accounts, tax information, bank statements, source of funds or source of wealth evidence, where required.
- 6.2. A beneficial owner is ultimately a natural person who owns or controls the client, directly or indirectly, or on whose behalf a transaction or activity is carried out. The Company applies the applicable statutory ownership threshold and also considers control through other means. Where no natural person is identified after reasonable measures, the Company will apply the measures required by law in relation to the relevant senior managing official and will retain records of the steps taken.

7. RISK BASED AND ENHANCED DUE DILIGENCE

- 7.1. The Company assesses money laundering and terrorist financing risk at onboarding and throughout the relationship. Enhanced due diligence may be applied where higher risk is identified, including in relation to politically exposed persons, higher risk countries, complex or unusual ownership structures, adverse information, sanctions exposure, unusual or large transactions, non face to face risks, or inconsistencies in the information provided.
- 7.2. Enhanced measures may include obtaining additional information or documents, establishing source of funds and source of wealth in greater detail, verifying information through additional independent sources, obtaining senior management approval, and applying increased or more frequent monitoring. The Company may decline or terminate a relationship where the risk is outside its risk appetite or where required due diligence cannot be completed.

8. POLITICALLY EXPOSED PERSONS AND SANCTIONS

- 8.1. The Company screens clients and relevant connected persons for politically exposed person status, sanctions and other financial crime risk indicators. Politically exposed persons, their family members and known close associates are not automatically prohibited from



becoming clients, but are subject to the measures required by applicable law, including appropriate approval and enhanced monitoring.

- 8.2. The Company will not establish or maintain a relationship or process a transaction where doing so would breach applicable financial sanctions or other legal restrictions. Screening may be repeated on an ongoing basis and following relevant changes.

9. SOURCE OF FUNDS AND SOURCE OF WEALTH

- 9.1. The Company may request information and supporting evidence concerning the origin of money used to fund an account and, where appropriate, how the client or beneficial owner accumulated their overall wealth. The information and evidence required will depend on the circumstances and risk and may include bank statements, payslips, audited financial statements, tax documents, contracts, sale agreements, inheritance documents or other reliable evidence.
- 9.2. No single monetary threshold limits the Company's right or obligation to request this information. Requests may arise at onboarding or at any time during the relationship, including where activity changes, a transaction is unusually large or complex, or information is inconsistent with the client's known profile.

10. DEPOSITS AND WITHDRAWALS

- 10.1. The following general principles apply to account funding and withdrawals:
- cash deposits and cash withdrawals are not accepted;
 - third party payments are not accepted;
 - the name of the payment account holder should correspond to the name of the VSMarkets client;
 - the Company may require evidence that the payment method or bank account belongs to the client;
 - withdrawals will normally be returned to the original funding source or to a verified payment account held in the client's name, subject to legal, technical and risk based requirements; and
 - the Company may reject, return, delay or request further information about a payment where ownership cannot be verified or where the transaction raises legal, regulatory, fraud or financial crime concerns.
- 10.2. The Company may apply different return routes where the original method cannot receive funds or where another route is required by law, payment scheme rules or risk management considerations. Any alternative destination must be appropriately verified.

11. ONGOING MONITORING AND UPDATING OF INFORMATION

- 11.1. The Company monitors the business relationship and scrutinises transactions and account activity to assess whether they are consistent with its knowledge of the client, the client's business and risk profile, and, where necessary, source of funds and source of wealth. Monitoring may be automated, manual or both.
- 11.2. Clients must promptly notify the Company of changes to their name, address, contact details, tax residence, occupation or business, ownership or control, authorised persons,



financial profile, source of funds, source of wealth or other information previously provided. The Company may periodically request updated documents or require reverification.

12. UNUSUAL OR SUSPICIOUS ACTIVITY

- 12.1. The Company maintains procedures for identifying, reviewing and, where legally required, reporting knowledge or suspicion of money laundering, terrorist financing or other relevant criminal activity to the competent authorities. The Company may refuse, suspend or delay a transaction, restrict an account, decline an application or terminate a relationship where permitted or required.
- 12.2. The Company may be prohibited by law from informing a client that a report has been made or that an investigation or review is taking place.

13. RECORD KEEPING AND PERSONAL DATA

- 13.1. The Company retains identification and verification material, account files, correspondence, transaction records and the results of relevant analyses for the period required by applicable law and for longer where lawfully required by a competent authority or necessary for legal proceedings.
- 13.2. Personal data is processed for compliance with legal and regulatory obligations, fraud prevention, risk management and the establishment, exercise or defence of legal claims, as applicable. Further information about how the Company processes personal data and about data protection rights is available in the Company's Privacy Notice.

14. CLIENT RESPONSIBILITIES

- 14.1. Applicants and clients must provide complete, accurate and current information and authentic documents, respond promptly to reasonable requests, and must not use the Company's services for unlawful purposes. Submission of documents does not guarantee acceptance of an application or transaction.
- 14.2. If the Company cannot apply the customer due diligence measures required by law or is not satisfied with the information or evidence provided, it may be unable to open or maintain the account or to carry out a transaction.

15. POLICY STATUS AND REVIEW

- 15.1. This Policy is provided as a summary for information and transparency. It should be read together with the Client Agreement, Privacy Notice and other applicable client disclosures. If there is any inconsistency, mandatory law and regulatory requirements prevail.
- 15.2. The Company reviews this Policy periodically and may amend it to reflect changes in law, regulation, guidance, products, services, systems or risk. The current version will be made available through the Company's usual communication or publication channels.

16. CONTACT

- 16.1. Questions concerning account verification requirements may be submitted to the Company through its official client support channels. The Company will never ask a client to send account passwords, full payment card security codes or other authentication credentials.