

Zenith Markets PLC

AML Policy

January 2025

tradgrip

1. Introduction

- 1.1 Zenith Markets PLC owns and operates the brand “TradGrip” (www.tradgrip.com) and is registered in Comoros Union, with registration IBC number HT00324011, authorized and regulated by the MWALI International Services Authority (hereinafter the “MISA”) with a brokerage license number BFX2024031 and registered office address at Bonovo Road-Fomboni Island of Mohéli- Comoros Union (hereinafter the “Company”, “we”, “us”). The Company is required to comply with the applicable legal framework for the prevention and suppression of money laundering and terrorist financing.
- 1.2 The Company promotes high standards of both business and personal conduct. This AML Policy provides the procedures to identify potential risks of the Company under the applicable AML/CFT framework, as well as the appropriate measures and procedures to minimize these risks.
- 1.3 Additionally, the Policy sets the procedures for implementing “Know Your Customer” (KYC) principles, conducting due diligence on new and existing customers and transactions, assigning responsibility for reporting suspicious transactions, and consolidating the relevant compliance policies, rules, and regulations that impact the Company’s operations.
- 1.4 We provide below the procedures and controls in place to detect, prevent, and communicate information regarding money laundering and terrorist financing activities, as well as to establish processes for preventing, detecting, and reporting suspicious activities. Our procedures and controls provided below are based on a risk-based approach, considering the money laundering and terrorist financing risks associated with each potential or existing client or business relationship.
- 1.5 Lastly, we outline the relevant Know Your Client (KYC) procedures for identifying and verifying the client's identity and address during the account opening and on an ongoing basis.

2. Definitions

- 2.1 “*Money Laundering*” shall mean the process of concealing or disguising the existence, source, movement, destination, or illegal application of illicitly derived funds or property for the purposes of making those funds appear legitimate. Anti-Money Laundering (AML) refers to procedures, regulations, and laws designed to prevent attempts to disguise illegally obtained funds. The money laundering offence may be committed by:
 - a) Any person knowing that any monetary instrument or property represents, involves, or relates to, the proceeds of any unlawful activity, transacts or attempts to transact said monetary instruments or property.
 - b) Any person knowing that any monetary instrument or property involves the proceeds of any unlawful activity, performs or fails to perform any act as a result of which he facilitates the offence of money laundering referred to in paragraph (a) above.
 - c) Any person knowing that any monetary instrument or property is required under the applicable framework to be disclosed and filed with the MISA Department of Anti-Money Laundering (DAML), fails to do so.

3. General Principles

- 3.1 The Company takes all reasonable measures to ensure that all trading accounts maintained are not used for the purpose of holding assets obtained as the result of or for facilitating the commission of any criminal activity or for any purpose contrary to applicable laws and regulations. In this respect, the Company maintains policies and procedures to identify and avoid any transactions associated with AML/CFT and thus to ensure compliance with the requirements of the applicable legal framework.
- 3.2 The Company regularly reviews and updates the policies, procedures and manuals related to AML/CFT to ensure consistency with its business model, product and service offering and any regulatory updates. In case of new emerging technologies, the Company ensures that its internal systems and controls remain up to date and consistent with the new innovative standards.
- 3.3 The Company will remain vigilant in preventing involvement in or misuse of money laundering activities and will not knowingly accept assets or engage in business relationships if there is reasonable suspicion that the assets may have been obtained illegally or are the proceeds of criminal activity.
- 3.4 The Company maintains policies and procedures for the AML/CFT employee training.
- 3.5 The Company established procedures to obtain appropriate evidence of client identity and maintain adequate records in this respect. The Company identifies and verifies the identity of all its clients and does not open or maintain any trading accounts unless it is satisfied with this requirement.
- 3.6 The Company's Board of Directors has the ultimate responsibility for the effectiveness of the Company's AML/CFT framework.
- 3.7 Senior management is responsible for the development of sound risk management programs and for keeping the Board adequately informed about these programs and their effectiveness.
- 3.8 The Company pays attention to all complex, unusual, or large business transactions, or unusual patterns of transactions, and to insignificant but periodic transactions, that have no apparent economic or lawful purpose.
- 3.9 The Company will observe and implement procedures aimed at monitoring client and account activity in order to adequately identify indicators relating to transactions and patterns, source of funds and wealth, and geographical risk, in line with the FATF recommendations/international standards on combating money laundering and the financing of terrorism & proliferation.
- 3.10 The Company collects information/documentation and data for the construction of its clients' economic profile. Transactions executed by the clients are compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the client and the data and information kept for the client's economic profile. Significant deviations are investigated, and the findings are recorded in the respective client's file.

3.11 The Company maintains records for client transactions which are safely stored for five (5) years from the transaction date. With respect to closed accounts, the records of client identification, account files, and business correspondence are preserved and safely stored for at least (5) five years from the date the relevant business or transaction was completed, or the termination of the business relationship. The Company will ensure that client information and transaction records are available to authorities upon request.

3.12 This Policy is updated once needed to ensure our consistent compliance with the applicable legal framework.

4. Application of the Risk-Based Approach (RBA)

4.1 The Company applies appropriate measures and procedures, on a risk-based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher.

4.2 In implementing the RBA, the Company follows a process to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. Where there are higher risks, the Company takes enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures are not applied whenever there is a suspicion of money laundering or terrorist financing. More specifically, the RBA:

- (a) identifies the specific threats posed to the Company by ML and TF and those areas of the Company's business with the greatest vulnerability;
- (b) assesses the likelihood of those threats occurring and the potential impact of them on the Company;
- (c) mitigates the likelihood of occurrence of identified threats and the potential for damage to be caused, primarily through the application of appropriate and effective policies, procedures and controls;
- (d) manages the residual risks arising from the threats and vulnerabilities that the Company has been unable to mitigate; and
- (e) allows the review and monitoring of those risks to identify whether there have been any changes in the threats posed to the Company which necessitate changes to its policies, procedures and controls.

4.3 Moreover, when determining and putting in place appropriate risk-based systems and controls, the Company considers the nature, size and complexity of its business and the type of ML and TF risk that it might reasonably face in identifying its ML and TF risk, the Company considers the risk posed by the following factors:

- a. Its client type, including any politically exposed persons;
- b. The types of designated services it provides;
- c. The methods by which it delivers designated services; and

- d. The jurisdictions where the beneficial owner resides, where the source of funds and wealth emanates and where the company operates.

4.4 The Company adopts reasonable criteria for assessing the risks in line with the applicable framework. The Company conducts periodic reviews to determine whether any adjustment should be made to its risk rating.

5. Client Due Diligence (“CDD”) Procedures

5.1 Timing of Application of the CDD:

The CDD applies before and during the establishment of a business relationship.

- When opening an account for, or otherwise establishing a business relationship with, a customer;
- Whenever doubts exist about the veracity or adequacy of previously obtained customer identification information;
- Whenever there is a suspicion of money laundering or terrorism financing involving the customer or the customer’s account.
- Whenever a transaction or linked transactions are carried above the threshold set by the applicable legal framework.

5.2 The Company follows a CDD procedure as follows:

- a. Identifies and verifies the identity of the applicant using reliable, independent sources, documents, data or information;
- b. Identifying and verifying the identity of the beneficial owner such that the Company is satisfied that knows who the beneficial owner is;
- c. Obtaining information on the purpose and intended nature of the business relationship;
- d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions throughout the course of the business relationship to ensure that the transactions in which the customer is engaged are consistent with the Company’s knowledge of the customer and his business and risk profile, including the source of funds.
- e. The Company ensures that all documents, data or information collected under the CDD process are kept relevant and up to date by undertaking reviews of existing records, following a risk-based approach.
- f. The Company ensures that employees remain up to date and aware of the AML/CFT risks and patterns and internal reporting obligations.
- g. Enhanced due diligence may be applied in cases where is justified by the associated risk or parameters set by the Company.
- h. Client due diligence (“CDD”) will be carried out with respect to any new or potential clients for the purposes of gathering information/documentation to identify and mitigate risks of money laundering, financing terrorism, and other illicit activities. Before accepting a new client, KYC and due diligence procedures are followed, by examining the following factors:

- i. Clients' identity;
- ii. Background and Sanctions checks;
- iii. Public or high-profile position (i.e. PEPs)
- iv. Linked account (s);
- v. Business activities;
- vi. Any other risk indicators.

5.3 The Company obtains, documents and regularly updates information in relation to the client's identity, address, source of funds, occupation, and expected business or transactional activity accompanied by documents verifying this information. Information collected will be verified by the collection of identification documentation, and via independent and reliable sources to confirm the veracity of the identifying information obtained.

5.4 Without limiting the generality of the aforesaid, the Company may, when establishing a business relationship obtain information on the purpose and nature of the business relationship and the source of funds and adequately identify and verify the client's identity and address. The Company maintains appropriate risk management systems to determine if a potential client or beneficial owner is a Politically Exposed Person ("PEP"), and if so, performs due diligence measures on a risk-sensitive basis; and

5.5 The Company utilize reasonable measures to verify and adequately document the identity of the client or account holder at the outset of a business relationship. This process includes, where appropriate:

- a) Taking reasonable measures to understand the identity of the client.
- b) Obtaining information on the purpose and intended nature of the business relationship, the source of funds, and the source of wealth, where applicable. And discontinuing the transaction if client documentation information is not forthcoming at the outset of the relationship
- c) Using enhanced due diligence procedures for high-risk clients or transactions or business relationships following the RBA.

5.6 The Company may use online software equipment or technology for the verification of its clients' identity or address.

6. Client Identification

6.1 The Company establishes, verifies and keeps appropriate records regarding the true identity of its clients as verified by official documents. The Company verifies the true identity of its clients who are physical persons and in the case of legal persons verifies their legal existence and organizational structure as well as the authority and identification of all persons purporting to act on their behalf.

6.2 The Company does not maintain or/and prohibits the opening of anonymous trading accounts or/and under fictitious names.

6.3 Documents and information that the Company will collect from physical and legal persons for due diligence purposes include but are not limited to the ones depicted in *Table I*:

Table I

Physical Persons	Legal Persons
Full name	Name of the corporate entity, identifier, and registration number.
Date of birth	Principal place of business and registered office.
Nationality	Contact details
A valid coloured scan ID or Passport or Driving License showing 4 edges and a photograph.	Information/Documentation on the beneficial owner and other information for establishing of the structural information of the corporate entity.
The residential address of the client accompanied by a recent up to three (3) months utility bill, telephone bills or bank statement.	Certified copies of the corporate documents including the Certificate of Incorporation or equivalent.
Information on the purpose and volume of the anticipated transactions, source of funds, etc.	<p>Evidence of the identity of all account signatories, details of their relationship with the company and if they are not employees, an explanation of the relationship.</p> <p>All are verified in accordance with the identification and verification of identity requirements of natural persons.</p>
Confirmation of whether the client is included in PEP lists, sanctions and/or other watchlists.	Identity information on the natural persons with significant control of the corporate entity. Satisfactory evidence of identity must be established for at least two directors, one of whom should, if applicable, be an executive director where different from account signatories. For publicly listed on a recognized stock exchange and not subject to effective control by a small group of individuals, identification and verification of the identity of shareholders is not required.

Information on the origin of funds and other information on the physical person's occupational background and supporting documentation in this respect.	Confirmation by way of company search and/or other commercial enquiries that the applicant company is in good standing and has not been, or is not in the process of being dissolved, struck off, wound up or terminated.
The Company also requests a description and nature of the business and the purpose of the account opening and the source of funds.	The Company also requests a description and nature of the business and the purpose of the account opening and the source of funds.

6.4 The Company may collect additional documents or request the completion of further verification procedures in order to satisfy its obligations, including those relating to the source of wealth and source of funds (e.g. bank statements, tax returns, or pay slips).

7. Reporting

7.1 The Company will promptly report suspicious/covered transactions relating to clients' trading accounts within the timeframe specified by the law or by the Supervising Authority.