

ANTI-MONEY LAUNDERING POLICY

Earn
Online Broker

August 2025

1. Scope of the Policy

Money Laundering is the participation in any transaction that seeks to conceal or disguise the nature or the origin of funds derived from the illegal activities. Money laundering involves not only the proceeds of drugs trafficking, but funds related to other illegal activities, including fraud, corruption, organized crime, terrorism and many other crimes. Generally, the money laundering consists of three stages:

- Placement: introduction of cash originating from illegal / criminal activities into financial or non-financial institutions.
- Layering: separating the proceeds of criminal activities from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.
- Integration: placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

This Policy is developed and periodically updated by the Risk Management/Compliance and Anti-Money Laundering Officer of Top Markets Solutions Ltd (“the Company”), operating under the trade name Earn, based on the general principles set up by the Board of Directors of the Company in relation to the prevention of money laundering and terrorist financing.

The Policy applies to all employees of the Company and aims to setup key roles and responsibilities for the staff members as well as to ensure compliance with the following legislation:

- The Prevention and Suppression of Money Laundering and Terrorist Financing Laws No. 188(I)/2007 of 2007-2019 and amending law N.22(I) 2021 (the Law)
- Directive (EU) 2018/843 of 30 May 2018 amending Directive (EU) 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 purposes of money laundering or terrorist financing
- Directive DI144-2007-08 OF 2012, Directive DI144-2007-08(A) of 2016 and Directive DI144-2007-08(B) OF 2016, Directive RAD157/2019 as updated by RAD 125/2020 of the Cyprus Securities and Exchange Commission for the Prevention of Money Laundering and Terrorist Financing (the AML Directive)
- Any other Directives, Circulars and Guidelines issued by the Cyprus Securities and Exchange Commission (CySEC), the Unit of Combating Money Laundering (MOKAS), the recommendations of the Financial Action Task Force (the “FATF Recommendations”), ESA’s Guidelines and any other authority entrusted with the task of combating Money Laundering.

The Company has established principles and procedures to prevent money laundering and combat terrorism financing, in accordance with the risk profile of its products, services, clients and geographic locations.

All amendments and/or changes of current version of the Policy must be approved by the Company’s Board of Directors.

2. Clients ‘acceptance policy

Inadequate understanding of the client's profile and purpose of investment activity may expose the Company to a number of risks. In order to minimize such risks, the Company has developed the Client Acceptance Policy.

3. Risk-based Approach

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. This approach will enable the Company to assign to its clients the following risk categories:

- High risk clients
- Medium risk clients
- Low risk categories

4. Dynamic Risk Management

Risk Management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Client's activities change as well as the services and financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

5. Know Your Client Procedures

The prime method for preventing money laundering is by carrying out "Know Your Client" procedures. With thorough knowledge of clients, counterparties and the origin of client's funds, unusual or suspicious behaviour can be identified, including false identities, unusual transactions, changing behaviour or other indicators where laundering may be occurring.

The Company performs the obligatory identification of each Client and verification of identity of each Client and, where applicable, its beneficial owners before the establishment of a business relationship or the carrying out of the transaction.

5.1 Establishment of Identification for Individual Customers

The identity will be established to the Company's satisfaction by reference to official identity papers or such other evidence as may be appropriate under the circumstances including, without limitation: full name; date of birth; origin; marital status; name of wife/husband, if married; name of parents; complete address, including phone number and city code; occupation; information on the earnings and his/her financial situation.

Identification documents must be valid at the time of the establishment of the business relationship.

Evidence of the potential client's identity should be in the form of a true copy or a copy of:

- a) Passport or National ID card if the potential client does not have a passport
- b) Proof of residence - this document can be in the form of a utility bill (electricity, water or landline telephone bill, home internet bill), local authority tax bill, a confirmation letter issued by the municipality, bank statement or other equivalent document showing the potential client's full name (cannot be wife/ husband/ other family member's name) and should be dated within the last 6 months. Provided that there is a reasonable explanation, a proof of residence issued in the name of the potential client's parent (mother/father) or spouse can be accepted, however, additional documents to establish the relationship, such as, birth certificate, marriage certificate, should be received.

Depending on the country of origin the Company may request additional documents and will be considered on a case-by-case basis following a risk-based approach by the AMLCO and directors.

The Company applies enhanced customer identification and due diligence procedures in respect of the clients that pose a high level of risk for money laundering or terrorist financing and are classified by the Company as high risk according to Clients Acceptance Policy.

The Company will follow the following measures in order to verify the identity of non face to face clients:

- 1) Where possible, direct and personal contact with the potential client is established. The staff member of the Company or its remote organizational units, who has met with the client in person and verified his identity, confirms a face-to-face meeting in the client's profile in the CRM software;
- 2) Telephone contact with the client at his residence or office, before the establishment of a business relationship or the occasional transaction, on a telephone number which has been provided by the potential client;
- 3) Contact with the client through email at an email address provided by the potential client.

The Company may also apply the following additional verification methods:

- a) The first payment of the operations is carried out through an account opened in the customer's name with a credit institution operating and licensed in a Member State or in a third country, which imposes requirements on combating money laundering equivalent to those of the EU Directive;
- b) Video Call with the potential client. It is provided that a potential customer, whose identity was verified hereunder cannot deposit an amount over €2.000 per annum, irrespective of the number of accounts that he keeps with the Company, unless an additional measure as per above paragraph is taken in order to verify his identity. In such case the Company monitors both the amount of the client's deposit and the risk for money laundering or terrorist financing, as well warns the client appropriately and in due time for the above procedure in order to obtain the client's express consent prior to its commencement;
- c) Requiring for identification documents to be provided in the form of certified true copies of the originals. Certification can be made by:
 - a third party, such as, accountant or a lawyer, provided that additional measures/procedures are applied as per the paragraph **Reliance on third parties for client identification and due diligence purposes** of this Policy;
 - a competent authority or person that, pursuant to the relevant provisions of the laws of their country, is responsible to certify the authenticity of documents or information.

6. Ongoing Monitoring

The Company performs reviews of existing records and examine clients' transactions and activities undertaken throughout the course of the business relationship, to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, the business and risk profile, including where necessary, ascertaining the source and origin of the funds credited to accounts.

The Company ensures that the clients' identification records remain completely updated with all relevant identification data and information throughout the business relationship. The Company examines and checks, on a regular basis, the validity and adequacy of the clients' identification data and information it maintains, especially those concerning high risk clients.

7. Reporting of Suspicious Transactions to MOKAS

Suspicious Transactions

Suspicious transactions are transactions or other activities that have no apparent lawful purpose or is not the sort in which a particular client would normally be expected to engage in, and the Company knows of no reasonable explanation for the transaction or activity after examining the available facts, including the background and possible purpose of the transaction or activity. The Company, in cases where there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, reports, through the AMLCO its suspicion to MOKAS.

8. Record Keeping

The Company must maintain records of:

- Client identification documents obtained;
- Any additional documents/information obtained during the relationship;
- All World-Check and Accuity World Compliance Reports performed for the client, as well as all results for the screening on sanctions' lists;
- Details of all relevant business transactions carried out for clients for a period of five (5) years after the end of the business relationship with their customer or after the date of an occasional transaction.

This information may be used as evidence in any subsequent investigation by the authorities. The records kept provide audit trail evidence during any subsequent investigation. In practice, the business units of the Company will be routinely making records of work carried out for clients in the course of normal business and these records should be archived.