ANTI MONEY LAUNDERING POLICY

MONEY LAUNDERING DEFINITION

Money laundering is the intricate process of converting funds derived from illicit activities, such as fraud, corruption, terrorism, and others, into alternative funds or investments that appear legitimate, thus concealing or distorting the true origin of the funds. This process can be categorized into three consecutive stages:

- Placement:

In this initial stage, funds are transformed into financial instruments such as checks, bank accounts, money transfers, or used to purchase high-value goods that can be resold. Additionally, funds can be physically deposited into banks or non-bank entities, such as currency exchangers. To avoid arousing suspicion, money launderers may opt to make multiple deposits instead of depositing the entire sum at once, known as "smurfing."

- Layering:

During this stage, funds are transferred or moved to other accounts and financial instruments. The objective is to obscure the funds' origin and disrupt any trace of multiple financial transactions, making it difficult to trace the flow of laundered money.

- Integration:

In the final stage, the funds are reintroduced into circulation as legitimate funds used to purchase goods and services.

INTRODUCTION

EMAR Markets (PTY) Ltd is authorized by the Financial Sector Conduct Authority (FSCA) in South Africa as a Financial Service Provider (FSP No. 53070) located at Ground Floor The Pavilion Building, CNR or Portswood and Dock Road, V&A Water Front Capetown, Western Cape 8001. As is customary among financial market service providers, the company, referred to as the "Company," strictly adheres to Anti-Money Laundering (AML) principles and actively prevents any actions that facilitate or aim to legalize illegally obtained funds. The AML policy's objective is to prevent criminals from utilizing the Company's services for money laundering, terrorist financing, or other illicit activities.

To fulfill this objective, the Company has implemented a stringent policy to detect and prevent any suspicious activities, promptly reporting them to the relevant regulatory bodies. Furthermore, the Company is prohibited from informing clients that law enforcement authorities have been notified. An intricate electronic system has been implemented to identify each client of the Company and perform comprehensive monitoring of all operations.

In line with the anti-money laundering efforts, the Company strictly prohibits the acceptance or disbursement of cash under any circumstances. The Company reserves the right to suspend any client transactions that may be deemed illegal or potentially linked to money laundering, as determined at the Company's discretion.

This Policy is communicated to all employees of the Company who manage, monitor, or have control over client transactions and are responsible for implementing the prescribed practices, measures, procedures, and controls outlined herein. Additionally, this Policy extends to all officers, appointed contractors, agents, as well as the products and services offered by the Company. All business units within the Company collaborate to create a cohesive effort in combating money laundering.

The appropriateness, effectiveness, and sufficiency of this Policy are subject to independent internal audits.

COMPANY PROCEDURES:

The Company ensures that it engages with authentic individuals or legal entities and carries out all necessary measures in accordance with applicable laws and regulations set by the relevant supervisory authorities. The fulfillment of this AML Policy within the Company involves the following:

- Implementation of a Know Your Customer (KYC) Policy and Customer Due Diligence (CDD).
- Continuous monitoring of client activities.
- Maintenance of comprehensive records.

The Company assesses and evaluates the risks it faces based on various criteria, including but not limited to the nature of the client, client behavior, initial communication with the client, as well as risks associated with the Company's services and securities. The Company maintains a structured Risk Assessment Framework to identify and manage AML/CFT risks.

Risks are assessed across four main categories:

- Client Risk – Nature of client, occupation, PEP status, corporate ownership structure.
- Geographic Risk – Jurisdiction of client residence or business, presence on FATF or local high-risk lists.
- Product/Service Risk – Leverage, payment methods, high-risk services.
- Transaction Risk – Size, frequency, and complexity of transactions compared to client profile.

Each client and transaction are rated Low, Medium, or High risk.

- 1 - 4 points: Low Risk - Standard CDD requirements.
- 5 - 7 points: Medium Risk - Additional verification and closer monitoring.
- 8 - 12 points: High Risk - EDD measures, senior management approval, and enhanced monitoring.

Risk ratings are reviewed annually and whenever material changes occur (e.g., new ownership, change of address, unusual transactions).

KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE

Due to the Company's commitment to AML and KYC policies, every client must complete the verification procedure before commencing any cooperation with the Company. The Company ensures the production of satisfactory evidence or takes other necessary measures to establish the identity of the client or counterparty. Additionally, the Company applies enhanced scrutiny to clients residing in countries identified by credible sources as having inadequate AML standards or posing a high risk of crime and corruption, as well as to beneficial owners residing in and sourcing funds from those countries.

The Company applies Enhanced Due Diligence (EDD) measures for clients and transactions that present a higher risk of money laundering or terrorist financing. EDD is required in the following cases:

- Clients from high-risk jurisdictions identified by FATF or local regulators.
- Politically Exposed Persons (PEPs), their family members, and close associates.
- Clients with complex ownership structures or unclear sources of wealth.
- Unusually large, complex, or frequent transactions without clear economic purpose.

EDD measures include:

- Obtaining additional documents verifying source of funds and source of wealth.
- Conducting background checks through reliable databases.
- Requiring senior management approval before establishing or continuing the business relationship.
- Increasing the frequency of ongoing monitoring and reviews.

PEPs are individuals who hold, or have held, prominent public positions, as well as their immediate family members and close associates.

The Company applies the following measures:

- Screening all clients against PEP databases at onboarding and periodically thereafter.
- Mandatory EDD for PEPs.
- Senior management approval before establishing a relationship with a PEP.
- Enhanced monitoring of all transactions involving PEPs.

Counter-Terrorist Financing (CTF).

The Company is equally committed to preventing terrorist financing (TF). In line with FATF recommendations, UN resolutions, and applicable domestic laws, the Company implements measures to:

- Prohibit the use of its services for financing terrorism or proliferation of weapons of mass destruction.
- Screen all clients and transactions against UN Sanctions, EU Consolidated Lists, OFAC SDN List, and other relevant government lists.
- Immediately freeze and report any funds or accounts linked to designated persons or entities.
- Ensure no business relationship is maintained with persons or organizations suspected of terrorism or associated with terrorist financing.

INDIVIDUAL CLIENTS

During the registration process, individual clients provide personal information, including full name, date and place of birth, residential address, phone number, city code, and any other information deemed necessary by the Company.

Individual clients are required to provide the following documents (in cases where documents are written in non-Latin characters, notarized translation into English is necessary) to fulfill the KYC requirements and verify the provided information:

Identity verification can be established through:

- Valid passport.
- National ID card.
- Driver's license.
- Any other government-issued identification documents.

The provided documents should include the client's full name, date of birth, photo, citizenship, and, if applicable, confirmation of document validity (issue and/or expiry date) and the holder's signature.

These documents must be valid at the time of submission and for at least thirty (30) days from the submission date.

For identification procedures and CDD requirements, proof of identity is considered satisfactory if:

- It can be reasonably established that the client is the person they claim to be.
- The person examining the evidence is satisfied, following the procedures outlined in the relevant legislation and regulations, that the client is indeed the person they claim to be.

To verify the current residential address, one of the following documents shall be provided:

- A recent utility bill (gas, water, electricity), telephone bill, or internet bill.
- Bank statement.
- Credit card statement.
- Tax clearance or tax return, social security policy or insurance policy, police character certificate, affidavit, certificate of residence, or residence permit (if these documents contain the current residential address and the client's name).
- Valid passport, national ID card, or driver's license that includes the current residential address and the client's name (where specifically allowed in certain countries/regions).
- Any other government-issued document that includes the current residential address and the client's name.

The utility bill, bank statement, and credit card statement should not be older than six (6) months from the submission date. There is no prescribed time frame for the other documents, but they must be current.

When certification is required, the documents should be certified by one of the following authorities:

- An Apostille.
- A judge.
- A magistrate.
- A notary public.
- A barrister-at-law.
- A solicitor.
- An attorney-at-law.
- A commissioner of oaths.

If applicable (e.g., for ID or driver's license), both sides of the submitted document should be provided. The document image must be a high-resolution color photo or scan copy without blurs, light reflections, or shadows. All four edges of the document should be visible, and all information must be clearly readable without any watermarks or similar obstructions.

For each account, the Company shall also make reasonable efforts, before settling the initial transaction, to obtain the following information to the extent it is applicable:

- Occupation of the client.
- The client's investment objective and other relevant information regarding their financial situation and needs.
- Annual income, assets, or net worth.
- Any other information deemed necessary by the Company for account opening.

CORPORATE CLIENTS

In the case of an applicant company listed on a recognized or approved stock exchange, or where independent evidence confirms that the applicant is a wholly owned subsidiary or under the control of such a company, further identity verification steps are generally not required. For unquoted companies where none of the principal directors or shareholders already hold an account with the Company, the following documents are required to fulfill the KYC requirements:

- Copies of the Certificate of Registration/Certificate of Incorporation.
- Copies of the Memorandum and Articles of Association, Partnership Agreement, or similar documents, as applicable.
- Copies of the By-Laws and the latest General Information Sheet, which lists the names of directors/partners, principal stockholders, secondary licenses, and other relevant information.
- Extract from the Commercial Register or equivalent document, demonstrating the registration of corporate acts, amendments, and the current legal status of the entity, such as a Certificate of Good Standing.
- Copy of the Certificate of Incumbency issued no older than 3 months from the filing date.
- Information about the beneficial owners (BOs) of the company is obtained from independent and reliable sources.
- KYC documents of all Directors, Shareholders, Beneficial Owners, and Officers of the legal entity, where applicable.
- Appropriate Board of Directors' resolutions and signed application forms for account opening, identifying authorized signatories or principal officers of the corporation, their authorities, and specimen signatures.
- Evidence of the registered address and actual place of business of the legal entity.
- Latest audited financial statements, if applicable.
- Additional information about the nature of the client's business, such as a description and nature of the business, date of business commencement, products or services provided, and principal place of business, as requested by the Company.

This procedure is conducted to establish the client's identity and enable the Company to understand their financial transactions and provide the best online trading services.

ADDITIONAL PROVISIONS

If, during the business relationship, the client fails or refuses to provide the required verification data and information within a reasonable timeframe, the Company reserves the right to terminate the business relationship and close all client accounts.

Customer Due Diligence for both individual and corporate clients should be updated or amended promptly following any changes. This includes changes in residential or business addresses, new identification cards, new passports, additional business information, new business securities/ventures, and similar updates. The Company may request a letter or document confirming the changes made.

During the verification process and document review for new clients, the Company reserves the right to apply additional requirements and procedures for client identification. Such procedures are determined at the sole discretion of the Company and may vary based on factors such as the client's country of residence, client profile, and other considerations. The Company may request the client to provide a source of funds, source of wealth documents, proof of funds being deposited in a manner determined appropriate by the Company, and any other necessary documents to complete the verification process.

GOVERNANCE & RESPONSIBILITIES

Board of Directors

- Approves the AML/CTF policy and ensures resources are available.
- Reviews compliance reports and audit results periodically.

Compliance Department

- Oversees daily AML/CTF compliance.
- Coordinates with regulators and law enforcement when required.

Money Laundering Reporting Officer (MLRO)

- Designated Officer: Compliance Officer, Darius van Graan CO No: 7731
- Responsibilities:
  - Primary point of contact with regulators and FIUs.
  - Receives and reviews internal suspicious transaction reports.
  - Decides on escalation to authorities.
  - Maintains a confidential log of all STR/SAR reports.
  - Submits annual AML/CTF compliance reports to the Board.

Employees

- Must adhere to AML/CTF procedures at all times.
- Required to report any suspicious transactions immediately to the MLRO.
- Prohibited from tipping-off clients.
- Non-compliance will result in disciplinary action, up to and including termination.

MONITORING CLIENT ACTIVITIES

In addition to gathering client information, the Company maintains continuous monitoring of all client activities to detect and prevent any suspicious transactions. Suspicious transactions are those that deviate from a client's legitimate business activities or their typical transaction history, as identified through client activity monitoring. The Company has implemented a comprehensive system, including both automated and manual processes, to prevent the utilization of its services by individuals involved in criminal activities.

The Company reserves the right to suspend any client operation that is deemed illegal or may be associated with money laundering, as determined by its staff. All employees must remain vigilant for unusual or suspicious activity, including but not limited to:

- Transactions inconsistent with client's stated profile.
- Sudden large deposits or withdrawals without economic justification.
- Use of multiple accounts or third-party accounts.

Suspicious Transactions Reporting

When suspicion arises, staff must immediately escalate the matter to the Company's Money Laundering Reporting Officer (MLRO).

The MLRO maintains an Internal STR/SAR Register recording:

- Date of report
- Reporting staff member
- Nature of suspicion
- Action taken

The MLRO is responsible for:

- Reviewing the report and conducting an internal investigation.
- Filing a Suspicious Transaction Report (STR) to the relevant authority within the statutory timeline.
- Maintaining a confidential register of all internal and external STRs/SARs.

External reports to the FIU must be filed within the statutory deadline (typically 24–72 hours depending on jurisdiction). Employees are prohibited from informing clients when a report has been made ("tipping off").

Copies of reports are retained for **7 years**.

The ongoing monitoring of client accounts and transactions is essential in effectively managing the risk of money laundering.

DEPOSIT AND WITHDRAWAL REQUIREMENTS

All client operations related to depositing and withdrawing funds must adhere to the following requirements:

- For bank transfers or transfers from a bank card, the name provided during registration must match the account or card owner's name. Withdrawals can only be made to the same bank and account/card used for the initial deposit.
- When using electronic payment systems, funds can be withdrawn from the trading account only to the system and account used for the deposit.
- Suppose the account was credited using a method that cannot be used for fund withdrawals. In that case, the funds may be withdrawn to the client's bank account or another approved method, provided that the Company can verify the account owner's identity.
- If the account has been credited with funds from multiple payment methods, withdrawals shall be made proportionally based on the size of each deposit. Any profits earned can be transferred to any account from which the deposits were made, if such transfers are feasible.
- In cases where the account was credited using various payment methods, including bank cards, the Company will process withdrawal requests to the bank card(s) until the total amount of the initial deposit using the bank card(s) has been withdrawn. Afterward, clients can request withdrawals and withdraw any earned profits via alternative payment methods.
- Deposits and withdrawals to third-party bank accounts, bank cards, electronic wallets, or any other payment accounts are strictly prohibited.

RECORD KEEPING

The Company is committed to maintaining comprehensive records in accordance with the requirements of the AML Policy. This includes the retention of all documents obtained for the purpose of client identification, as well as information related to each transaction and other client-related information as mandated by applicable AML laws and regulations.

The following document retention periods will be adhered to:

- All documents related to the opening of client accounts and records of their transactions, including client identification records, will be securely stored and maintained for a period of seven (7) years from the dates of the transactions.
- For closed accounts, records pertaining to client identification, account files, and business correspondence will be preserved and securely stored for a minimum of seven (7) years from the date of account closure.

By maintaining these records, the Company ensures compliance with regulatory obligations and facilitates the effective monitoring and review of client activities.

Training & Independent Audit:

- All relevant employees receive mandatory AML training at onboarding and annually thereafter. Training covers KYC/CDD, EDD, identifying suspicious activity, and reporting obligations.
- Training attendance is documented and monitored.
- The AML Policy and controls are subject to independent audit at least once every 12–18 months to test effectiveness and compliance with applicable laws.
- Audit findings are reported to senior management and corrective actions are tracked to completion.

CONFIDENTIALITY & STAFF OBLIGATIONS

Employees are strictly prohibited from informing a client or third party that a suspicious transaction has been reported (“tipping off”).

Breach of confidentiality is grounds for disciplinary action and may result in criminal liability.

All staff must maintain professionalism and impartiality when handling AML/CTF matters.