
MAKE CAPITAL
TRUST PROFESSIONALS

MAKE CAPITAL
TRUST PROFESSIONALS

ANTI-MONEY LAUNDERING POLICY

JANUARY 2024

MAKE CAPITAL
TRUST PROFESSIONALS

INTRODUCTION

Make Capital Market (PTY) Ltd is registered in South Africa, with company registration number 2022/526501/07 and regulated by the Financial Sector Conduct Authority (FSCA) with license number 53179 operating under the trading name Make Capital (hereinafter "The Company").

The Company has implemented policies, controls and procedures in line with the Financial Intelligence Centre Act, No 38 of 2001 (The FIC Act) together with the Prevention of Organised Crime Act, 1998 (POCA), the Prevention and Combatting of Corrupt Activities Act, 2004 (PRECCA) and the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (POCDATARA) under the guidance on how to comply with these requirements. The phrase "money laundering" covers all procedures to conceal the origins of criminal proceeds so that they appear to originate from a legitimate source. The Company aims to detect, manage and mitigate the risks associated with money laundering and the financing of terrorism. The Company has introduced strict policy aimed on the detection, risk prevention or mitigation in respect of any suspicious activities performed by Clients.

The Company is required to constantly monitor its level of exposure to the risk of money laundering and the financing of terrorism.

The Company believes that if it knows its Clients well and understands their instructions thoroughly, it will be better placed to assess risks and spot suspicious activities.

CLIENT ACCEPTANCE POLICY

Effective Client Due Diligence ("CDD") measures are essential to the management of money laundering and terrorist financing risk. CDD means identifying the Client and verifying their true identity on the basis of documents, data or information both at the moment of starting a business relationship with Client and on an ongoing basis. The Client identification and verification procedures require, first, the collection of data and, second, attempts to verify that data.

During the account registration process an individual Client provides the following identification information to the Company:

- Client's full name;
- Client's date of birth;
- Country of residence/location of Client;
- Mobile telephone number and e-mail.

During the account registration process a corporate Client provides the following identification information to the Company as a minimum:

- Full company name;
- Registration number and date;
- Country of registration/incorporation;
- Registered address;
- Mobile telephone number and e-mail.
- Names of Directors
- Names of Shareholders up to the ultimate beneficial owners (UBOs).

Appropriate documents for verifying the identity of Client include, but are not limited to, the following:

- For an individual Client: A high resolution scanned copy or photo of pages of a passport or any other national ID, or a current valid driving licence (where the Financial institution is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence) indicating family name and name(s), date and place of birth, passport number,issue and expiry dates, country of issue and Client's signature and a clear, non-edited selfie.

- For a corporate Client: a high-resolution copy of documents showing the existence of the entity, such as Certificate of Incorporation, and, where applicable, Certificate of Change of Name, Certificate of Good Standing, Articles of incorporation, a government issued business license (if applicable), etc.

To verify proof of address of the Client the Company requires one of the following to be provided, in the same correct name of the Client:

- A high-resolution copy of a utility bill (fixed-line phone, water, electricity) issued within the last 3 months;
- A copy of a tax or rates bill from a local authority;
- A copy of a bank statement (for a current account, deposit account or credit card account);
- A copy of a bank reference letter.

The information and documents will be automatically verified by the Company's electronic system or 3rd party identity verification software or by the Company's staff. The Client's information is verified against electronic databases for confirmation of identity details and legal status such as criminal record, political associations, sanctions lists etc.

The 3rd party system that is used by the company for verification purposes fulfills the below conditions:

1. Is registered with the Data Protection Commissioner in the country from which it operates, for the purposes of safety or the personal data and

2. Electronic databases provide access to information that refers to both current and previous situations that indicate that the person actually exists and include positive information (at least full name, address and date of birth of the Client) as well as negative information (eg committing offenses such as identity theft, inclusion in files of deceased persons, inclusion in lists of sanctions and restrictive

measures by the Council of the European Union, Interpol and the Security Council UN).

3. Uses multiple sources of information which update in real-time as well as present alerts whenever information in the system regarding a verified client, will change (eg. A previously verified client has now been added to a sanctions list)

4. Provide details as to what kind of information was researched and resulted in either validation or invalidation of the client's verification

5. Allows the Company to keep records of the information that was verified as well as the verification results

6. electronic databases contain a wide range of sources, with information from various time intervals, updated to real-time update and send notifications trigger alerts when important data is differentiated.

7. has established transparent procedures that allow to the Company to identify what information has been searched for, which ones are their effects and their importance in relation to the degree certainty as to the identity of the Client.

Potential sanctions matches are reviewed by the responsible persons and if the matches are found to be accurate and true the Client gets rejected.

When making a funds deposit or funds withdrawal via credit/debit card which is not 3D Secure, a Client is required to provide a scanned copy or photo of the credit/debit card (front and back side). The front side of credit/debit card should show the cardholder's full name, the expiry date and the first six and the last four digits of the card number (the rest of the digits may be covered). The copy or scan of the reverse side of credit/debit card should show the cardholder's signature, but the CVC2/CVV2 code must be masked. If an existing Client either refuses to provide the information described above or if a Client has intentionally provided misleading information, the Company, after considering the risks involved, will consider closing any of the existing Client's accounts.

The Regulations measures require further research and identification of Clients who may pose a potentially high risk of money laundering/terrorism financing. If the Company has assessed that the business relationship with a Client poses a high risk, it will apply the following additional measures:

- Obtaining the information relating to the source of the funds or the wealth of the Client will be required (this will be done via e-mail, Client Portal ticketing system or phone);
- Seek further information from the Client or from Company's own research and third-party sources in order to clarify or update the Client's information, obtain any further or additional information, clarify the nature and purpose of the Client's transactions with Company.

When obtaining information to verify the Client's statements about source of funds or wealth, the Company's staff will most often ask for and scrutinize details of the person's employment status or business/occupation. The Company's staff will ask for whatever additional data or proof of that employment/occupation that may be deemed necessary in the situation, particularly the appropriate

confirming documents (employment agreements, bank statements, letter from employer or business, financial statements etc.).

The Company will conduct ongoing Client due diligence and account monitoring for all business relationships with Clients. It particularly involves regularly reviewing and refreshing Company's view of what its Clients are doing, the level of risk they pose, and whether anything is inconsistent with information or beliefs previously held about the Client. It can also include anything that appears to be a material change in the nature or purpose of the Client's business relationship with Company.

REFUND POLICY

The Company's Refund Policy is an integral part of the Client Agreement and can be found on the Company's website at https://makecapitalmarket.com The Refund Policy contains all the relevant information regarding payments to and from the Company and measures taken prevent money laundering and terrorist financing.

PERSONNEL

AML Compliance Officer

The Company shall appoint an AML Compliance Officer, who will be fully responsible for the Company's AML and CFT program and report to the Board of the Company or a committee thereof any material breaches of the internal AML policy and procedures and of the Regulations, codes and standards of good practice.

AML Compliance Officer's responsibilities include:

- Ensuring the Company's compliance with the requirements of the Regulations;
- Establishing and maintaining internal AML program;
- Establishing an audit function to test its anti-money laundering and combating the financing of terrorism procedures and systems;
- Training employees to recognize suspicious transactions;
- Receiving and investigating internal suspicious activity and transaction reports from staff and making reports to the FIU where appropriate;
- Ensuring that proper AML records are kept;
- Obtaining and updating international findings concerning countries with inadequate AML systems, laws or measures.

Employees

All Company employees, managers and directors must be aware of this policy.

Employees, managers and directors who are engaged in AML related duties must be suitably vetted. This

includes a criminal check done at the time of employment and monitoring during employment. Any violation of this policy or an AML program must be reported in confidence to the AML Compliance Officer, unless the violation implicates the AML Compliance Officer, in which case the employee must report the violation to the Board of Directors.

Employees who work in areas that are susceptible to money laundering or financing terrorism schemes must be trained in how to comply with this policy or the AML program. This includes knowing how to be alert to money laundering and terrorism financing risks and what to do once the risks are identified.

Employee Training Program

The Company provides AML training to employees who will be dealing with Clients or will be involved in any AML checking, verification or monitoring processes. The Company may conduct its training internally or hire external third-party consultants.

Each person employed within the Company is assigned a supervisor who teaches him or her in relation to all policies, procedures, Client documentation forms and requirements, forex markets, trading platforms, etc.

The Company's AML training program is aimed to ensure its employees receive appropriate training level with regards to any possible AML/TF risks.

Content of training

The Company's AML and risk awareness training includes the following content:

- The Company's commitment to the prevention, detection and reporting of ML and TF crimes.
- Examples of ML and TF that have been detected in similar organisations, to create an awareness of the potential ML and TF risks which may be faced by the Company's employees
- Well known or recognised typologies, especially where made available by the FATF or AML Supervisors.
- The consequences of ML and TF for the Company, including potential legal liability.
- The responsibilities of the Company under the AML Act and Regulations.
- Those particular responsibilities of employees as identified in this AML Policy, and how employees are expected to follow the Company's AML procedures.
- How to identify and report unusual activity that may be a suspicious transaction or attempted transaction.
- The rules that apply against unlawful disclosure of suspicious transactions ("tipping off").