GCMTRADING



GCMT SA PTY LTD

ANTI MONEY LAUNDERING POLICY

TABLE OF CONTENTS

Policy Statement. 3

Scope. 3

Regulatory Requirements 4

AML Compliance Committee 4

Identification Requirements (Client) 5

Enhanced Identification Requirements (Client). 5

Customer Account Funding and Withdrawal Policy 5

Verifying Information. 6

Customers Who Refuse to Provide Information. 6

Checking the Office of Foreign Assets Control ("OFAC") List 7

Controls, Monitoring and Reporting 7

Suspicious Activity 8

Investigation. 10

Recordkeeping. 10

Training. 10

Testing of the Policy. 11

Notice to Clients 11

Administration. 11

Policy Statement

In compliance with The Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA 2002), the Prevention of Corruption Act 2002 (POCA 2002) and the Prevention of Terrorism Act 2002 (POTA 2002), GCMT GROUP LTD (SA) ("Global Capital Markets Limited") have adopted an Anti-Money Laundering (AML) compliance policy ("Policy"). For avoidance of doubt, and the purposes of this agreement and policy, any statement in the text below referring to GCMT GROUP LTD. is also referring to CMTrading as the owner of this site and any reference made to CMTrading herein, will also refer at the same time to **GCMT SOUTH AFRICA (PTY) LTD,** trading as CMTrading and to our subsidiary company, CMT Processing Limited, our appointed Independent Representative and Distributor. The business address of CMT Processing Limited is: Triton Quarters, 2nd Floor, Office 202, Parallel Road to New Port Limassol, No.22, 3045 Limassol, Cyprus.

Scope

This policy applies to all GCMT SOUTH AFRICA (PTY) LTD Trading as CMTrading as well as all its subsidiaries, officers, employees, appointed producers and products and services offered by CMTrading. All business units and locations within CMTrading will cooperate to create a cohesive effort in the fight against money laundering. Each business unit and location has implemented risk-based procedures reasonably expected to prevent, detect, and cause the reporting of transactions required under the FIAMLA. All efforts exerted will be documented and retained in accordance with the FIAMLA. The AML Compliance Committee is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Committee.

It is the policy of CMTrading to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. CMTrading is committed to AML compliance in accordance with applicable law and requires its officers, employees, and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes. For the purposes of the Policy, money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

Generally, money laundering occurs in three stages. Cash first enters the financial Anti-Money Laundering Policy system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's cheques, and/or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Regulatory Requirements

GCMT SA PTY LTD.'s Anti-Money Laundering policy complies with all the statutory and regulatory requirements for money laundering control and combatting of terror financing as stated in the following statues and their corresponding Regulations, Exemptions and Guidance notes:

- Prevention of Organised Crime Act, 121 of 1998 ("POCA")
- Financial Intelligence Centre Act, 38 of 2001 ("FICA"); and
- Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 ("POCDATARA") FICA is South Africa's ("SA") primary anti-money laundering legislation and SA is a member of the Financial Action Task Force ("FATF").

GCMT SA PTY LTD applies standards applicable in accordance with FATF's 40 Recommendations and is fully committed to maintaining high levels of integrity, professionalism, and ethical behavior.

AML Compliance Committee

The AML Compliance Committee, with full responsibility for the Policy, shall be comprised of the Company shareholders, Corporate Attorney and the Head of Compliance. The Head of Compliance shall also hold the title Chief AML Officer and shall have authority to sign as such. The duties of the AML Compliance Committee with respect to the Policy shall include, but are not limited to, the design and implementation of as well as updating the Policy as required; dissemination of information to officers, employees and appointed producers of GCMT SA PTY LTD, training of officers, employees and appointed producers; monitoring the compliance of GCMT SA PTY LTD operating units and appointed producers, maintaining necessary and appropriate records, filing of SARs when warranted; and independent testing of the operation of the Policy.

Each GCMT SA PTY LTD business unit shall appoint a contact person to interact directly with the AML Compliance Committee to assist the Committee with investigations, monitoring and as otherwise requested.

Identification Requirements (Client)

GCMT SA PTY LTD has adopted a Customer Identification Program (CIP). GCMT SA PTY LTD will provide notice that they will seek identification Anti-Money Laundering Policy information; collect certain minimum customer identification information from each customer, record such information and the verification methods and results; and compare customer identification information with OFAC.

Enhanced Identification Requirements (Client)

Means the reasonable steps taken by the organisation to establish and verify the identity of a client that is party to a High-Risk ML/TF transaction, which steps are more stringent than a Quick Due Diligence and a Standard Due Diligence.

As part of its client onboarding process, the organisation will determine whether a single transaction, or a transaction to be concluded pursuant to a new or an existing business relationship, must be classified as a ML/TF High-Risk transaction.

ML/TF High-Risk transactions are those transactions that have been identified by the organisation as more likely to be exploited for money laundering or the financing of terrorism purposes.

A ML/TF High-Risk transaction, is any transaction where:

- A product or service that has been previously identified by the organisation as a ML/TF High-Risk product or service, forms part of that transaction, or
- A client or client representative who is party to that transaction, has been identified by the organisation as a ML/TF High-Risk person.

The organisation will perform Enhanced Client Due Diligence procedures on all prospective and existing clients that are party to a ML/TF High-Risk transaction.

Customer Account Funding and Withdrawal Policy

Consistent with this AML Policy, GCMT SA PTY LTD has the following policy regarding the deposit and withdrawal of funds from customer trading accounts:

- A customer may have more than one trading account with GCMT SA PTY LTD. *However*, each trading account may have only one beneficiary/owner.
- Only the account beneficiary/owner may deposit or withdraw funds to or from the trading account.
- Funds may be deposited by Credit or Debit Card, Wire Transfer, E-Money and Cryptocurrencies. Upon withdrawal of funds from the trading account, the funds will be sent to the same method by which they were deposited, or to a verified method owned by the trading account beneficiary/owner.
- The account beneficiary/owner must be the verified owner of any method used to deposit or withdraw funds from a customer trading account.

Verifying Information

Based on the risk, and to the extent reasonable and practicable, GCMT SA PTY LTD will ensure that it has a reasonable belief of the true identity of its customers. In verifying customer identity, appointed producers shall review photo identification. GCMT SA PTY LTD shall not attempt to determine whether the document that the customer has provided for identification has been validly issued. For verification purposes, GCMT SA PTY LTD shall rely on a government-issued identification to establish a customer's identity. GCMT SA PTY LTD, however, will analyze the information provided to determine if there are any logical inconsistencies in the information obtained. GCMT SA PTY LTD will document its verification, including all identifying information provided by the customer, the methods used and results of the verification, including but not limited to sign-off by the appointed producer of matching photo identification.

Customers Who Refuse to Provide Information

If a customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the appointed agent shall notify their Manager. The GCMT SA PTY LTD Manager will decline the application and notify the AML Compliance Committee. A Suspicious Activity Report (SAR) must be completed and forwarded to the Compliance Officer for filing with the relevant Authorities.

Checking the Office of Foreign Assets Control ("Ofac") List

For all (1) new applications received and on an ongoing basis, (2) disbursements (3) new producers appointed or (4) new employees, Global Capital Markets Limited will check to ensure that a person or entity does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. Global Capital Markets Limited may contract with verified external Government sources to secure accuracy in the checks. Global Capital Markets Limited will also review existing policyholders, personnel, and employees against these lists on a periodic basis. The frequency of the reviews will be documented and retained. In the event of a match to the SDN List or other OFAC List, the business unit will conduct a review of the Anti-Money Laundering Policy circumstances where such match has been identified. If the business unit is unable to confirm that the match is a false positive, the AML Committee shall be notified.

Controls, Monitoring and Reporting

The control, monitoring and reporting measures, as contained in the Financial Intelligence Centre Act, 38 of 2001, ("the FIC Act"), as amended, are based on three basic principles of money laundering detection and investigation, i.e. that:

- intermediaries in the financial system must know with whom they are doing business;
- the paper trail of transactions through the financial system must be preserved;
- possible money laundering transactions must be brought to the attention of the Financial Intelligence Centre ("the Centre") and the investigating authorities.

The Compliance Officer has a responsibility to report suspicious and unusual transactions to the Financial Intelligence Centre: It is the responsibility of management to ensure that:

- All employees can identify suspicious and unusual transactions, and;
- Know how to report these transactions;
- Identification and verification of suppliers by applicable employees as required by FICA are complied with.
- Records of the identification and verification documents are kept as required by FICA, by the employees who are required to comply with this requirement.

• Employees receive training to enable them to comply with the legislation and the internal rules applicable to them.

• The FICA Risk Management and Compliance Programme is made available to all employees. Any employee who knows or ought reasonably to have known or suspected that:

• the business has received or is about to receive the proceeds of unlawful activities or property that is connected to an offence relating to the financing of terrorist and related activities.

• a transaction to which the business is party facilitated the transfer of the proceeds of unlawful activities or property connected to an offence relating to the financing of terrorist and related activities; or has no apparent business or lawful purpose; is conducted for the purpose of avoiding giving rise to a reporting duty under this Act; or may be relevant to the investigation of an evasion or attempted evasion of duty to pay any tax.

• the business has been used in any way for money laundering purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities.

Non-compliance with AML/CFT requirements is a very serious offence and could result in dismissal or contract termination. Failure by any employee to adhere to any of the requirements and obligations contained herein shall result in disciplinary action being taken against the relevant employee in terms of disciplinary action.

Suspicious Activity

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as "red flags." If a red flag is detected, additional due diligence will be performed before proceeding with accepting the client. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee. Examples of red flags are:

• The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspect identification or business documents.

• The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business strategy.

• The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

• Upon request, the customer refuses to identify or fails to indicate any legiti mate source for his or her funds and other assets.

• The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

• The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

• The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

• The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

• The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.

• The customer engages in transactions involving cash or cash equivalents or other Anti-Money Laundering Policy monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

• For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

• The customer is from, or has accounts in, a country identified as a non co-operative country or territory by the Financial Action Task Force.

• The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

• The customer's account shows numerous currencies or cashier's check transactions aggregating to significant sums.

• The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

• The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.

• The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.

• The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- Attempt to borrow maximum cash value of a single premium policy soon after purchase.

If the appointed producer:

- Exhibits a dramatic or unexpected increase in sales (particularly of single premium contracts) as defined in the Anti-Money Laundering Policy;
- Has consistently high activity in single premium contracts more than company averages;
- Exhibits a sudden change in lifestyle;
- Requests client documentation be delivered to the agent;

Investigation

Upon notification to the AML Compliance Committee of a match to the OFAC SDN List or possible suspicious activity, an investigation will be commenced to determine if a report should be made to appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrants it, a recommendation will be made to the AML Compliance Committee to file a blocked asset and/or a SAR with the appropriate law enforcement or regulatory agency. The AML Compliance Committee is responsible for any notice or filing with law enforcement or regulatory agency. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know.

Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing with the person or persons subject of such, or any other person, including members of the officer's, employee's, or appointed agent's family.

Recordkeeping

The AML Compliance Committee will be responsible to ensure that AML records are maintained properly and that SARs and Blocked Property Reports are filed as required. Global Capital Markets Limited will maintain AML records for at least five years.

Training

Global Capital Markets Limited shall provide AML training to its officers, employees, and appointed personnel to ensure awareness of requirements under the FICA Act with FICA section 43. Training takes place as follows:

- Every employee shall receive training on FICA to enable them to comply with the provisions of the act and create an awareness of the internal rules/Risk Management and Compliance Programme applicable to them.
- Global Capital Markets Limited internal rules policy clearly documents money laundering and its requirements and is freely available to all staff members.
- Changes in legislation will be communicated as and when required.

The training will include, at a minimum: how to identify red flags and signs of money laundering; what roles the officers, employees and appointed producers have in the Global Capital Markets Limited compliance efforts and how to perform such duties and responsibilities; what to do once a red flag or suspicious activity is detected; Global Capital Markets Limited record retention policy; and the disciplinary conse- quences for non-compliance with the Act and this Policy. In addition, each affected area will provide enhanced training in accordance with the procedures developed in each area for officers and employees reasonably expected to handle money, requests, or processing that may bring them into contact with information designated above. Training will be conducted on an annual basis. The AML Compliance Committee will determine the ongoing training requirements and ensure written procedures are updated to reflect any changes required in such training. Global Capital Markets Limited will maintain records to document that training has occurred as per the Anit-Money Laundering Policy/FICA Risk Management and Compliance Programme.

Testing Of The Policy

The testing of the Policy may be conducted by an outside independent third party annually. Any findings will be reported to the AML Compliance Committee, SFG Audit Committee and Senior Management for appropriate action.

Notice To Clients

Global Capital Markets Limited will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law.

Administration

The AML Compliance Committee is responsible for the administration, revision, interpretation, and application of this Policy. The Policy will be reviewed annually and revised as needed.

CMTRADING

GCMT SOUTH AFRICA PTY LTD Trading as CMTRADING Registration No. 2013/045335/07 A juristic representative and agent of BLACKSTONE MARKETING PTY LTD
Registration No. 2010/010099/07 (FSP No. 38782).

Registered Office:
14th Floor, Sandton City Towers,
158 5th Street, Sandton,
Johannesburg, 2196, South Africa

Email:
support@cmtrading.com

RISK WARNING:

Trading Foreign Exchange (Forex) and Contracts for Differences (CFD's) is highly speculative, carries a high level of risk and may not be suitable for all investors. You may sustain a loss of some, or all, of your invested capital. Therefore, you should not speculate with capital that you cannot afford to lose. You should be aware of all the risks associated with trading on margin.