ANTI-MONEY LAUNDERING POLICY

Promax Trading Limited

December 2024

Table of Contents

Anti-Money Laundering Policy

Introduction

Promax Trading Limited (the "Company") is incorporated in Saint Lucia in accordance with the International Business Company's Act Cap 12.14 (IBC Act) with the organizational and legal form of a limited liability company as an international business company (hereinafter referred to as "IBC"), with registration number 2024-00683 and having its registered address at Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia. The Company operates under the fully owned domain https://www.promaxtrading.com/.

The Business activities of the Company are in particular but not exclusively, commercial, financial, lending, borrowing, trade, services activities, Forex brokerage, and managed accounts services in currency Contract for Difference agreements, namely precious metals, Contract for Difference agreements, index Contract for Difference agreements, and any other contract for difference agreements entered into, but does not include (a) shares and stock in the share capital of the company; (b) any instrument creating or acknowledging indebtedness, in particular, debentures, debenture stock, loan stock, bonds and notes; and (c) bonds and other instruments creating or acknowledging indebtedness issued by or on behalf of any participating Government and excluding any security as defined by The Securities Act CAP 12.18 of the revised laws of Saint Lucia or any 'securities' as defined by The Securities Act CAP 12.18 of the revised Laws of Saint Lucia, do not require a particular license and can be carried out by the Company in accordance with its Articles of Association and Memorandum (Articles of Association). The Company shall not carry out on any named financial service in or from any jurisdiction in which a license for that named financial service is required.

The Company aims to prohibit, detect and actively pursue the prevention of money laundering, terrorism financing, and all other predicate offences and vows to comply with all related laws, rules, and regulations with full attention and no compromises with any of the abovementioned illegal activities.

The Company recognizes the critical importance of Anti-Money Laundering ("AML") and Counter-Terrorism Financing ("CTF") and is dedicated to implementing and adhering to the highest international AML and CTF standards, while fully complying with the laws of Saint Lucia.

Purpose of the Policy

This AML Policy aims to provide clear guidance and transparency regarding the procedures and protocols followed by the Company to detect and prevent Money Laundering (ML) and Terrorism Financing (TF) activities, in full compliance with the applicable laws of Saint Lucia. This AML policy applies to all Company officers, employees, introducing brokers, affiliated entities, as well as the products and services offered. All company's employees are required to perform their duties in accordance with the principles outlined in this Policy. The Company is committed to taking all necessary steps to ensure compliance with its obligations, and any employee who fails to adhere to these policies and procedures will be subject to strict disciplinary actions.

Legal Framework

The Company is required to adhere with the provisions of the applicable laws relating to the prevention of ML and TF. The main objective of those laws is to define and criminalize the activities related to ML and TF. Legal entities carrying on financial and other business activities must establish and maintain certain policies and procedures to safeguard their business from being used for the purposes of ML.

For the purposes of this AML policy the applicable Legal Framework of the Company is comprised inter alia of the following:

- International Business Companies Act - Cap.12.14.
- Money Services Business Act - Cap 12.22.
- Anti-Terrorism Act 2 - Cap. 3.16.
- Money Laundering Prevention Act - Cap. 12.20.
- Proceeds of Crime Act – Cap.3.04.

- UN Sanctions (Counter-Proliferation Financing) Act.
- The Financial Services Regulatory Authority Act.
- Any other legislation which addresses matters related to AML and CFT or any other legislative act of Saint Lucia currently in force repealing, amending or complementing the above-mentioned legislations.
- Any other acts, rules, recommendations or regulations adopted by the Financial Intelligence Authority (FIA), the Financial Action Task Force (FATF), and the Caribbean Financial Action Task Force (CFATF).

Money Laundering and Terrorism Financing

Money laundering includes all procedures to conceal the origins of criminal proceeds so that they appear to originate from a legitimate source.

For this Policy, ML is also taken to encompass activities related to TF, including handling, or possessing funds to be used for terrorist purposes as well as proceeds from terrorism.

The Company is alert of the risk of its clients, counterparties and others laundering money in any of its possible forms. The Company or its client does not have to be a party to money laundering for a reporting obligation to arise.

Stages of **Money Laundering**

There are three stages of money laundering:

1. **Placement:** The physical disposal of cash proceeds. In the case of many serious crimes (e.g. drug trafficking) the proceeds take the form of cash which the criminal wishes to place in the legitimate business system. Placement may be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of the criminal, his advisers, and their network.

Typically, it may include:

- placing cash on deposit at a bank (often intermingled with a legitimate credit to obscure the audit trail), thus converting cash into a readily recoverable debt;

- physically moving cash between jurisdictions;
- making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting cash into debt;
- purchasing high value goods for personal use or expensive presents to reward existing or potential colleagues with cash;
- purchasing the services of high value individuals with cash;
- purchasing negotiable assets in one-off transactions; or
- placing cash in the client account of a professional intermediary.

2. **Layering:** This is the separating of the proceeds of crime from their source by creating sometimes complex layers of transactions designed to mask their origin and hamper the investigation, reconstruction and tracing of the proceeds; for example, by international wire transfers using nominees or "shell companies", by moving in and out of investment schemes or by repaying credit from the direct or indirect proceeds of crime.

3. **Integration:** This is the placing of the laundered proceeds back into the economy as apparently legitimate business funds, for example, by realizing property or legitimate business assets, redeeming shares or units in collective investment schemes acquired with criminal proceeds, switching between forms of investment, or by surrendering paid up insurance policies.

Money Laundering Relevant Offences:

A **money laundering** offence is committed by:

a. concealing or transferring proceeds of criminal conduct;
b. arranging with another to retain the proceeds of criminal conduct;
c. acquisition, possession or use of proceeds of criminal conduct.

Tipping Off

It is an offence for anyone who knows, suspects or has reasonable grounds to suspect that a disclosure has been made, or that the authorities are acting or are proposing to act

in connection with an investigation into money laundering, to prejudice an investigation by so informing the person who is the subject of a suspicion, or any third party of the disclosure, action or proposed action.

Prejudicing the Investigation

It is an offence to cause or permit to be falsified or conceal or destroy or otherwise dispose of information which is likely to be material to an investigation into money laundering.

Failure to Disclose

It is an offence if a person fails to report a suspicious transaction relating to money laundering within seven days from the date the transaction was deemed to be suspicious.

Terrorism Financing

Terrorist financing is the raising and processing of legal or illegal funds by any means, directly or indirectly, with the intention to use such funds or knowing that they will be used in whole or in part to support the activities of a terrorist or a terrorist group by any means. A terrorist, or terrorist group, is one that has the purpose to facilitate or carry out any terrorist action or activity. The intent and knowledge are enough to prove the offence of TF.

TF offences should extend to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: to carry out a terrorist act(s); or by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts).

TF offences should include financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

It is also a TF offence to:

a. attempt to commit the TF offence;

b. participate as an accomplice in a TF offence or attempted offence;

c. organise or direct others to commit a TF offence or attempted offence; and

d. contribute to the commission of one or more TF offence(s) or attempted offence(s), by a group of persons acting with a common purpose.

Procedures in Place

The Company's adopted legal provisions implement procedures and processes designed to ensure compliance with the relevant laws concerning ML and TF.

These procedures are aligned with the guidelines and measures set forth by the competent authorities in Saint Lucia.

The Company maintains transaction records for a period of seven years from the date the transaction was conducted. Additionally, the Company keeps a record detailing the nature of the evidence used to identify or verify an individual's identity.

Construction of Client economic Profile

The Company is committed to ensuring that it is dealing with a legitimate individual and, as such, will obtain sufficient evidence to verify the person's identity. The Company will take all reasonable measures to confirm the identity of any individual wishing to open an account, establish a business relationship, or engage in a significant one-off transaction or a series of connected transactions.

In this regard, the Company has established a clear procedure for verifying the identity of its clients. The identity of a prospective client should be established prior to the establishment of a business relationship with the Company and prior to the execution of any transaction or the provision of any service whatsoever. If the Company is unable to identify and verify a client, it will not proceed with any transactions through a bank account, establish a business relationship, or complete the transaction. Depending on the circumstances, the Company may terminate the business relationship and consider

submitting a suspicious transaction report to the relevant competent authority regarding the client.

The documents and information required to be collected before the establishment of a new business relationship between the Company and a client shall include the purpose and the reasons for requesting this business relationship, the company account transactions, the origin of the incoming funds and the destinations of the outgoing funds, the clients' wealth and the estimated annual income and a detailed description of the Company's business activities. In order to have a complete economic profile the Company also obtains basic information such as the company name, country of incorporation, and head office address, personal information relating to the Company's Beneficial Owners, Company Directors and Company Shareholders.

The Company strictly prohibits any client, whether retail, professional, eligible, or institutional, from engaging in a business relationship that involves the use of anonymous accounts or passbooks.

Risk Assessment Process

The risk assessment process within the AML framework is designed to identify, assess, and mitigate risks related to ML and TF. This process enables the Company to implement appropriate controls and ensure compliance with AML regulations. The AML risk assessment process involves the following steps:

1. Identify Risks

- Understand Business Operations: Evaluate the Company's products, services, customers, geographic exposure, and delivery channels to identify areas vulnerable to money laundering.
- Review Regulatory Guidance: Consider AML-related regulatory requirements, FATF recommendations, and the risks arising from Saint Lucia regulations.
- Analyze Data: Use internal and external data sources to identify risk patterns and trends, such as high-risk customer types, transaction anomalies, or geographic risks.

2. Assess and Categorize Risks

- Risk Factors

- Customer Risk: Analyze customer profiles (e.g., PEPs, high-net-worth individuals) and their activities for inherent risks.
- Geographic Risk: Assess jurisdictions involved in customer transactions, including sanctioned or high-risk countries.
- Product/Service Risk: Evaluate risks associated with specific products or services offered, such as private banking or cryptocurrencies.
- Channel Risk: Identify risks in how products or services are delivered, such as online or non-face-to-face interactions.

3. Evaluate Controls

- Assess Existing Controls: Evaluate the adequacy of existing AML policies, procedures, and technologies in mitigating identified risks.
- Identify Gaps: Identify areas where controls are insufficient or outdated, such as outdated customer due diligence (CDD) or weak transaction monitoring systems.
- Stress-Test Controls: Simulate scenarios to test the effectiveness of AML controls against high-risk activities.

4. Mitigate Risks

- Enhanced Due Diligence (EDD): Implement stronger controls for high-risk customers, transactions, or regions (e.g., more frequent reviews or stricter identity verification).
- Transaction Monitoring: Develop robust systems to flag suspicious activities or unusual transaction patterns.
- Training and Awareness: Ensure employees understand AML risks and are trained to recognize and report red flags.

5. Monitor and Review

- Continuous Monitoring: Use real-time transaction monitoring systems to detect and respond to suspicious activities promptly.
- Periodic Risk Assessment: Reassess risks periodically to reflect changes in customer behavior, regulatory requirements, or business operations.
- Review: Update policies and controls based on risk assessment findings, regulatory changes, or feedback from audits and investigations.

6. Document and Report

- Risk Assessment Report: Document the risk assessment findings, including identified risks, mitigation measures, and residual risks.

- Regulatory Reporting: Provide risk assessment results to regulators or other stakeholders as required by law.
- Audit Trail: Maintain comprehensive records to demonstrate compliance and facilitate audits or inspections.

7. Risk Assessment Tools

- **Risk Assessment Tools:** Software to automate customer risk scoring, transaction monitoring, and geographic risk analysis.
- **AML Models and Metrics:** Use key risk indicators (KRIs) and key performance indicators (KPIs) to track and evaluate the effectiveness of the AML framework.

This process is crucial as it ensures the Company proactively manages money laundering risks, upholds regulatory compliance, and protects its reputation.

Know Your Customer (KYC) Process

The Know Your Customer (KYC) process is a vital component of the Anti-Money Laundering (AML) framework, involving procedures that financial institutions and regulated entities follow to verify the identity of their customers. The primary goal is to prevent identity theft, financial fraud, money laundering, and terrorist financing.

During the KYC process, the Company identifies potential clients and evaluates the associated risks based on the client's economic profile and risk categorization. The Customer Identification procedure is essential for gathering key information about the customer (such as name, address, date of birth, and contact details) and verifying their identity using valid documentation, such as government-issued identification.

Documentation Required for KYC

The specific requirements may differ depending on the jurisdiction and the type of customer (individual or corporate), but common documentation typically includes:

For Individuals:

1. **Proof of Identity:**
   - Passport
   - National ID card
   - Driver's license
   - Social security card (if applicable)

2. **Proof of Address:**
   - Utility bill (electricity, water, or gas) issued within the last 3 months
   - Bank statement or credit card statement
   - Rental agreement or property ownership documents

3. **Additional Documentation (for Enhanced Due Diligence):**
   - Source of funds declaration
   - Employment verification or income proof
   - Letter from a bank or other reference.

For Businesses (Corporate KYC):

1. **Business Registration and Ownership:**
   - Certificate of incorporation or registration
   - Articles of association or partnership agreement
   - Business license.

2. **Proof of Address:**
   - Utility bills or bank statements in the company's name.

3. **Identity Proof for Key Individuals:**
   - Directors, shareholders with significant control (owning 25% or more), and authorized signatories must provide proof of identity and address.

4. **Tax Information:**
   - Taxpayer Identification Number (TIN) or equivalent documentation.

5. **Financial Records (if required):**
   - Recent financial statements or bank account details.

6. **Ultimate Beneficial Owner (UBO) Details:**
   - For identifying and verifying individuals who own or control the company.

7. **Additional Information (for Enhanced Due Diligence):**
   - Source of funds and business activity details.
   - International trade documentation (for import/export businesses).

KYC Compliance and Record Keeping

The Company must maintain records of KYC documentation for 5 years from the end of the relationship or occasional transaction.

Ultimate Beneficial Owner

A ‘Beneficial Owner’ means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted.

The Company takes appropriate measures to verify the identity of the beneficial owner, ensuring it is confident in knowing who the beneficial owner is. For legal entities and arrangements, this includes financial institutions taking reasonable steps to understand the ownership and control structure of the customer.

Customer Due Diligence (CDD)

Customer Due Diligence (CDD) is the process of verifying the identity of the client. To confirm a client's identity, independent and reliable information is required. The Company gathers information regarding the purpose and intended nature of the business relationship and performs ongoing due diligence to ensure that the transactions conducted align with the Company's understanding of the customer, their business, and risk profile. This includes, when necessary, verifying the source of funds.

The Company determines the extend of the CDD measures on a risk-based approach considering the type of customer, the nature of the business relationship, and the transaction involved.

Customer Due Diligence must be applied when there is doubt about veracity or adequacy of previously obtained customer identification data, or when identifying and verifying the identity of customers:

- On the establishment of the business relationship,

- When carrying out occasional transactions above $25,000.00 or that are wire transfers on funds transfers,
- When there is suspicious activity transaction,
- When there is a suspicion of money laundering or terrorist financing.

Simplified Due Diligence (SDD)

The Company may apply Simplified Due Diligence (SDD) when a client is assessed to present a low level of risk. In such cases, the Company implements less stringent identification and verification measures compared to standard or enhanced due diligence. However, SDD does not exempt the client from the fundamental CDD requirements.

The Company ensures adequate monitoring of transactions and business relationships to detect any unusual or suspicious activities.

Enhanced Due Diligence (EDD)

When the Company is dealing with natural persons or legal entities identified as high risk for ML or TF and classified as high risk based on the client's economic profile and the risk assessment conducted, the Company applies enhanced due diligence.

EDD is applied for clients with higher risks and includes:

- Additional verification of identity
- Detailed information to understand the source of funds
- More frequent monitoring of transactions
- Require documentation to verify the source of funds, particularly for large or unusual transactions.

The Company shall always apply enhanced client identification and due diligence procedures for the following clients, who are considered high-risk:

- Cross-frontier correspondent
- Non-face-to-face Clients

- Account in names of companies whose shares are in bearer form
- Trust accounts
- Client accounts' in the name of a third person
- Politically Exposed Persons accounts
- Clients from countries which inadequately apply FATF's recommendations

Additional customer risk factors include:

- The business relationship is conducted in unusual circumstances
- Clients are residents in geographical areas of higher risk
- Legal persons or arrangements that are personal asset-holding vehicles
- Companies that have nominee shareholders or shares in bearer
- Businesses that are cash incentive
- The ownership structure of a legal entity appears unusual or excessively complex given the nature of the company's business.

Product, service, transaction or delivery channel risk factor:

- Private banking
- Products or transactions that might favour anonymity
- Non-face-to-face business relationships or transactions, without certain safeguards such as electronic signatures
- Payment received from unknown or un-associated third parties
- New products and new business practices including new delivery mechanism and the use of new or developing technologies for both new and pre-existing products.

The Company maintains comprehensive records of all due diligence measures undertaken, including risk assessments and the rationale for the risk category assigned to each client.

The Company ensures that appropriate due diligence measures are in place to identify and verify a customer's identity using reliable, independent source documents, data, or information. Additionally, the Company conducts ongoing due diligence throughout the

business relationship, closely monitoring and scrutinizing transactions to ensure they align with the Company's knowledge of the customer, their business, risk profile, and, when necessary, the source of funds.

Screening of Clients

The screening process involves checking clients against various risk-related lists and databases to identify potential risks. The Company screens all clients against national and international sanctions lists and employs automated systems to ensure regular screening against updated sanctions. Additionally, the Company conducts reviews and rescreens existing clients in accordance with new watchlist updates, as per current regulations.

Politically Exposed Persons

The Company documents and has in place specific policies and procedures to identify and manage Politically Exposed Persons (PEPs). It ensures that transactions involving PEPs are authorized by senior management, determines the source of funds and source of wealth for PEPs, and conducts ongoing EDD on all accounts held by PEPs.

The Company employs automated systems to regularly screen clients against updated sanctions and PEP lists. It periodically reviews and updates its screening criteria to maintain compliance with the latest regulations. Additionally, the Company conducts ongoing reviews and rescreens existing clients in accordance with updates to the watchlist, ensuring alignment with current regulatory requirements.

Ongoing Monitoring Process of Clients Transactions and Activities

The Company monitors clients' activities based on their economic profiles, enabling employees to identify transactions that deviate from typical account behavior or appear complex, unusual, or lacking a clear economic purpose or legitimate explanation. Continuous monitoring of clients' accounts and transactions is a crucial component in effectively managing the risks of money laundering (ML) and terrorist financing (TF).

The Compliance/AML Officer is responsible for maintaining and enhancing the Company's ongoing monitoring process. The Internal Auditor will review the Company's procedures related to this monitoring process at least once a year.

The monitoring process is based on risk assessment categories and the estimated transaction volume for each client. Employees conduct reviews of client transactions at least once a week, or as requested by the Company's Compliance/AML Officer, and report their findings to the Compliance/AML Officer. Additionally, responsible employees provide daily records of clients' incoming and outgoing money transfers to the Compliance/AML Officer.

The Compliance/AML Officer monitors and ensures, on a frequent basis, that the actual amount of funds deposited by clients is consistent with the amount of funds indicated at account opening, as well as with the economic profile of the client.

Additionally, all employees must remain vigilant in identifying and reporting any activity or client behavior that appears inconsistent with the previously obtained information about the client and their business. Employees are required to notify their supervisor, who will then inform the Compliance/AML Officer. If the supervisor is unavailable, the employee should report the matter to the General Manager or an Executive Director.

The procedures and frequency of monitoring clients' accounts and examining clients' transactions are based on the level of risk associated with them, including:

a) The identification of high-risk clients and facilitate enhanced monitoring of accounts and transactions, as deemed necessary,
b) The identification of unusual or suspicious transactions that are inconsistent with the economic profile of the client for the purposes of further investigation.
    a. When an unusual or suspicious transaction is identified, the person identified the suspicious transaction is responsible to submit an internal suspicious report to the Compliance/AML Officer.
    b. The Compliance/AML Officer proceeds with investigation of unusual or suspicious transactions and the results of the investigations are recorded in a separate memo and kept in the file of the clients concerned.

c) The ascertainment of the source and origin of the funds credited to accounts.

d) The use of appropriate and proportionate IT systems, including:

- adequate automated electronic management information systems which will be capable of supplying the Board of Directors and the Compliance/AML Officer, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of client accounts and transactions based on the assessed risk for ML or TF purposes, in view of the nature, scale and complexity of the Company's business and the nature and range of the investment services undertaken in the course of that business
- automated electronic management information systems to extract data and information that is missing regarding the client identification and the construction of a client's economic profile
- for all accounts, automated electronic management information systems to monitor the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g. high risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the client, the country of his origin, the source of the funds, the type of transaction or any other risk factors. The Company pays particular attention to transactions exceeding the abovementioned limits, which may indicate that a client might be involved in unusual or suspicious activities.

e) The monitoring of accounts and transactions in relation to specific types of transactions and the economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship. Furthermore, the monitoring covers clients who do not have a contact with the Company as well as dormant accounts exhibiting unexpected movements.

f) The Company checks the adequacy of the data and information of the Client's identity and economic profile, whenever one of the following events or incidents occurs:

- a material change in the client's legal status and situation, such as change of directors/secretary, registered shareholders, registered office, etc.
- a material change in the way and the rules the client's account operates, such as a change in the persons authorised to operate the account and the application for the opening of new account.

Internal Reporting Procedures

The Company has implemented and maintains internal reporting procedures to ensure that all employees know who to contact if they suspect that someone within the organization or a customer is involved in illegal activities, including money laundering (ML). This system ensures that the organization handles such concerns in a structured and organized manner, in compliance with relevant anti-money laundering (AML) and counter-terrorism financing (CFT) regulations.

Reporting Suspicious Activities

The Company has established a clear protocol for employees to report any suspicious activities directly to the designated AML Compliance Officer. Additionally, it fosters an environment where employees are encouraged to raise concerns without fear of retaliation.

The Company will report any suspicious transaction or business activity when there is a reasonable suspicion that it involves the proceeds of money laundering (ML) or terrorist financing (TF), regardless of the transaction amount. The external reporting process involves filing a Suspicious Activity Report (SAR) with the relevant authorities, as required by law. The Company ensures that reports are submitted promptly and accurately, including a clear documentation of the reasons for suspicion.

Furthermore, the Company will terminate an account when its purpose or background is unclear, complying with the instructions of the competent authorities and facilitating any necessary inspections of transaction records.

Transactions exceeding $25,000

When a person enters into a transaction with the Company or engages in any other business activity exceeding $25,000.00 must fill out a source of fund declaration in the prescribed form. It will be considered an offence if a person knowingly makes a false declaration regarding the source of funds.

Training and Awareness

The Company takes appropriate measures to ensure that its employees are fully informed about the relevant laws in Saint Lucia regarding AML and CFT, as well as the procedures and policies established by the Company.

To achieve this, the Company conducts regular training for all employees on AML/CFT policies, including KYC and CDD procedures. The training ensures that employees understand the significance of their role and responsibilities in identifying and reporting suspicious transactions and related activities. Additionally, the Company provides ongoing education through refresher courses and newsletters, keeping employees updated on regulatory changes and emerging risks within the brokerage sector.

Compliance and Review

The Company conducts regular internal audits of its AML/CFT procedures to evaluate the effectiveness of the measures in place. Based on audit findings, regulatory updates, and the evolving risk landscape, the Company reviews and revises its policies and procedures as needed.

Additionally, the Company ensures that senior management is actively involved in overseeing AML/CFT compliance efforts, including the allocation of resources for training and ongoing monitoring.

Legal Obligations of the Company

The Company reserves the right to refuse to process a transfer of funds at any stage if it believes it to be connected in any way to criminal activities or money laundering.

Third party or anonymous payments shall not be accepted. If the Company is not satisfied of who the sender of the money is, it reserves the right to reject the money and return it to the remitter less any transfer fees or other charges, the Company further reserves the right to terminate any account held with it with immediate effect. It may require the submission of additional documentation as required under applicable AML obligations or any similar applicable regulations.

The Company is prohibited from accepting any client business if the funds are sourced from criminal activities or if the nature of the account transactions is illegal in any manner whatsoever.

The Company is obliged to report all suspicious transactions and is prohibited from informing the client that they have been reported for suspicious transactions and account activity. Account misuse may result in criminal prosecution.

The Company may terminate its business relationship with the client either with, or without notice, for a series of severe reasons, deriving from Regulatory Obligations, including taking measures against ML and extending (but, not limited to) breach of the client agreement and terms and conditions, bad faith, attempt to commit fraud, etc.

Additional Information

Any personal information collected relating to a client such as name, address, date of birth and contact details will remain confidential with Promax Trading Limited strictly for business purposes. Other information such as client transactions, copies of passports and proof of addresses will remain confidential and only shared between our account services and compliance departments. Such information will be maintained either physically or electronically with strict access requirements. The Company may share

client information with internal departments or affiliate offices who conduct marketing, back-office and customer service functions to accomplish normal business operations. Every employee at Promax Trading Limited has signed a Confidentiality Agreement, therefore, client information is required to be kept confidential.

The Company is dedicated to continuously improving this policy. It will be reviewed and updated regularly, at a minimum every six months, to ensure its effectiveness.

The Company reserves the right to review and/or amend its Anti-Money Laundering Policy at its sole discretion, whenever it deems fit or appropriate without notice to the client.

If you have any further questions regarding our Anti-Money Laundering Policy or our Privacy Policy, please contact us at https://www.promaxtrading.com/.

Document owned by: Promax Trading Limited