ATFX
A GLOBAL LEADER IN ONLINE TRADING

Anti-Money Laundering and Counter-Terrorism Financing Policy

AT GLOBAL MARKETS INTL LTD

TABLE OF CONTENTS

1. Overview

1.1 This Anti-Money Laundering and Counter-Terrorism Policy Manual (the "Manual") has been designed to ensure that AT Global Markets Intl. Ltd. ("ATG" or "the Company") complies with all the relevant laws and regulations under which it is governed and regulated which include the following amongst others:

1.1.1 Financial Services Act 2007;
1.1.2 Code on The Prevention of Money Laundering & Terrorist Financing 2012;
1.1.3 Financial Intelligence and Anti-Money Laundering Act 2002;
1.1.4 Securities Act 2005; and
1.1.5 The relevant acts, guidelines and regulations under the laws of Mauritius.

1.2 The Company aims to prevent, detect and not knowingly facilitate money laundering and terrorism financing activities. The management of the Company places extremely high importance on assisting in discovering any money laundering scheme. It is the policy of the Company and its affiliates to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

2. Definitions

2.1 **"Transaction"** means any deposit, withdrawal, exchange or transfer of funds.

2.2 "Money laundering" is the conversion of criminal monetary proceeds into clean money, so that it may be used as if it was legitimately acquired funds. It can also be seen as the need to change the form of the proceeds in order to shrink the huge volumes of cash generated by criminal activity. These proceeds include those derived from a variety of criminal activities including tax evasion, terrorism, sale of drugs, corruption, theft, etc.

2.3 Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's cheques, 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.

3. Risk-Based Approach

3.1 The possibility of being used to assist with money laundering and terrorist financing poses many risks to ATG, including civil action against the group as a whole and as an individual partner and damage to reputation leading to loss of business.

3.2 These risks must be identified, assessed and mitigated, which are done for all business risks facing by the Company. The Company believes that if it knows its client well and understands its requirements thoroughly, it will be better placed to assess risks and spot suspicious activities. The

risk-based approach means that ATG focuses its resources on the areas of greatest risk. This approach is more efficient and effective use of resources proportionate to the risks faced. It minimized compliance costs and burdens on clients and there is greater flexibility to respond to emerging risks as laundering and terrorist financing methods change.

4. Conflict of Interests

4.1 The Company shall designate an Anti-Money Laundering Program Compliance Officer ("AML Compliance Officer"), who is qualified in terms of experience, knowledge and training and to whom any internal report of suspicious transactions must be made. The AML Compliance Officer 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/CFT policy and procedures, and of the AML/CFT laws, codes and standards of good practice.

4.2 The duties of the AML Compliance Officer will include monitoring the Company's compliance with AML/CFT obligations, overseeing communication and AML/CFT training for employees. The AML Compliance Officer will also ensure that proper AML records are kept. When warranted, the AML Compliance Officer, will ensure Suspicious Transactions Reports ("STR") are duly filed. The AML Compliance Officer will also be responsible for ensuring that the Company has adequate customer identification and verification program in place at all times and in accordance with requirements of the law. The AML Compliance Officer shall also prepare reports on an annual basis and such other periodic reports as necessary to the Board of the Company or a committee thereof dealing with:

4.2.1 the adequacy/shortcomings of internal controls and other AML/CFT;

4.2.2 procedures implemented; recommendations to remedy the deficiencies identified above;

4.2.3 the number of internal reports made by staff; and

4.2.4 the number of reports made to the Financial Intelligence Unit.

4.3 The Company and the AML Compliance Officer shall ensure that the employees are properly trained and are fully aware of the Company's AML/CFT policies and procedures. The Company will also perform criminal and disciplinary checks on all employees before they are hired. The Company will develop on-going employee training under the supervision of the AML Compliance Officer.

5. Suspicious Transactions Reports ("STRs")

5.1 Internal suspicious transaction reports will not to be disclosed to anybody other than to the AML Compliance Officer. The AML Compliance Officer making an STR is protected from civil, criminal or disciplinary action in respect of any information contained in the report, unless the information was disclosed in bad faith. The AML Compliance Officer is obliged to keep records in a form that will allow a transaction to be completely reconstructed at any time by the authorities. All STR records are to be kept for a period of at least seven years.

5.2 The AML/CFT Compliance Officer and the Company's employees must not alert the customer on the fact that a potentially suspicious transaction is being investigated so as not to breach the offence of unlawful disclosure of an STR.

6. Customer Due Diligence ("CDD")

6.1 Effective Customer Due Diligence "know your customer" ("CDD") measures are essential to the management of money laundering and terrorist financing risk. CDD is identifying the client and verifying their true identity on the basis of documents, data or information obtained from a reliable and independent source both at the moment of starting a business relationship and on an ongoing basis. Identification of a client is getting to know a client's identifying details, such as their name and address, financial status and the capacity in which he/she is entering into the business relationship with the Company. Verification is obtaining evidence which is satisfactory to the Company and which supports the claim of identity. The Company will:

6.1.1 collect certain identification information from each customer who opens an account;

6.1.2 utilize risk-based measures to verify the identity of each customer who opens an account;

6.1.3 record customer identification information and the verification methods and results; and

6.1.4 conduct a risk profiling of the customer as per Appendix 1.

6.2 Prior to opening of account, the Company collect the following information:

6.2.1 For all accounts, if applicable, for any person, entity or organization opening a new account and whose name is indicated on the account:

(1) Name, incorporation number, legal status, date and country of incorporation or registration (for an entity other than an individual);

(2) Date and place of birth (for an individual);

(3) Occupation, public position held and where appropriate, the name of the employer (for an individual) or Anti-Money Laundering and Counter-Terrorism Financing Policy;

(4) A current address, which will be residential (for an individual) or registered office address and principal place of business (where different from the registered office), for an entity other than an individual;

(5) Passport number and country of issuance, identification card number and country of issuance of any other government issued document evidencing nationality or residence and bearing a photograph or other similar safeguard e.g. national identity cards, current valid passports or current valid driving licences; and

(6) The identity of underlying principles (including beneficial owners, controllers, directors or equivalent) with ultimate effective control over the capital or assets of an entity other than an individual in addition to evidence that any person who purports to act on behalf of the legal person is duly authorized and identify that person.

6.2.2 Where the underlying principals are not individuals, the Company shall investigate further to establish the identity of the natural persons ultimately owning or controlling the business. When opening an account for a foreign business or enterprise that does not have identification number, the Company will request alternative government-approved documentation certifying the existence of the business or enterprise.

6.3 Customers who refuse to provide information

6.3.1 If a potential or existing customer either refuses to provide the information described above or such information appears to have intentionally provided misleading information, the Company shall not open a new account and, after considering the risks involved, will consider closing any open account(s) of an existing customer.

6.4 Verifying information

6.4.1 Based on the risk, and to the extent reasonable and practicable, the Company will ensure that it has a reasonable belief that it knows the true identity of its customers by using risk-based procedures to verify and document the accuracy of the information received about the customers. In verifying the customer's identity, the Company will analyse any logical inconsistencies in the information obtained. Customer's identity must be verified when:

(1) Establishing a business relationship with a new client;

(2) The Company suspects money laundering or terrorist financing; and

(3) The Company has doubts about the veracity or adequacy of documents, data or information previously obtained for the purpose of CDD.

6.4.2 Where verification of identity is conducted after the establishment of the business relationship, verification will be completed as soon as is practicable after the business relationship has been established.

6.5 Methods of verification

6.5.1 The Company will verify customer identity through documentary evidence and non-documentary evidence (electronic verification). The Company will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, the Company will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. It may also use such non-documentary means, after using documentary evidence, if still uncertain about whether the true identity of the customer is known.

6.5.2 In analysing the verification information, the Company will consider whether there is a logical consistency among the identifying information provided, such as the customer's name, date of birth, street address and telephone number.

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

(1) For an individual: a current government issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; and

(2) For a person other than individuals, documents showing the existence of the entity, such as Certificate of Incorporation, Articles of incorporation, a government issued business license (if applicable), etc.

6.5.4 The Company will not be required to take steps to determine whether the document that the customer has provided for identity verification has been validly issued and it may rely on government-issued identification as verification of a customer's identity. If, however, it appears that the document shows some obvious form of fraud, the Company will consider that factor in determining whether it can form a reasonable belief that it knows.

6.5.5 The Company will use the following non-documentary methods of verifying identity:

(1) Contacting a customer;

(2) Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from Internet and/or other sources;

(3) Checking references with other financial institutions; or

(4) Obtaining a financial statement.

6.5.6 Non-documentary methods of verification will be used in the following situations:

(1) When the Company is unfamiliar with the documents the customer presents for identification verification;
(2) When there are other circumstances that increase the risk that the Company will be unable to verify the true identity of the customer through documentary means.

6.6 Lack of verification

6.6.1 Should the Company reasonably believe that the true identity of a customer cannot be established, it will do any or a combination of the following:
(1) Not proceed with or terminate any business with the customer;
(2) File a STR in accordance with applicable laws and regulations.

7. Enhanced Due Diligence ("EDD")

7.1 The regulatory measures require further research and identification of clients who may pose a high risk of money laundering to better assess the risks they pose.

7.2 If the Company has assessed that the business relationship or occasional transaction is a high-risk relationship, based on the customer's individual risk status, that is, the nature of the customer, the business relationship, its location, or any other specificity of the business relationship, it will apply EDD measures. By way of non-exhaustive examples, circumstances when EDD will be applied are:

7.2.1 If the Company establishes a business relationship with a customer from a country that has insufficient anti-money laundering and countering financing of terrorism systems or measures in place; or

7.2.2 If a customer seeks to conduct, through ATG, a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose.

7.3 The Company may in all circumstances consider that the level of risk involved is such that enhanced due diligence should apply to a particular situation.

7.4 In addition to CDD, the following enhanced requirements under EDD will apply:

7.4.1 Information relating to the source of the funds or the source of wealth of the customer will be required.

7.4.2 Carrying out more frequent and extensive ongoing monitoring on the customer and comparison with provided lists of terrorists and other criminals within openly accessible media sources (World-Check, internet) will be conducted.

7.4.3 Seek further information from the customer or from the Company's own research and third-party sources in order to clarify or update the customer's information, obtain any further or additional information, clarify the nature and purpose of the customer's transactions with the Company.

7.5 If suspicious information is found indicating possible money laundering or terrorist financing activity, the AML Compliance Officer shall file a STR in accordance with applicable law and regulations.

8. Politically Exposed Person ("PEP")

8.1 Politically exposed person are individuals who are or have been entrusted with prominent public functions, including government heads, senior politicians, judicial or military officials, important political party officials including their family members or close associates of the politically exposed person.

8.2 The Company will review public information, including information available on the Internet or in databases, to determine whether any account holders, who conduct transactions in amounts over 10,000 USD (or equivalent), are individuals who are or who have been entrusted with prominent public functions, their family members or close associates ("PEPs") If information indicating that an account holder may be a PEP is found, and upon taking additional reasonable steps to verify this information, it is determined that the individual is, in fact, a PEP the Company will:

8.2.1 Take enhanced due diligence measures to establish the source of funds and source of wealth of the PEP.

8.2.2 Conduct enhanced ongoing monitoring of the business relationships involving the PEP.

8.2.3 Establish or continue the business relationship only with senior management approvals. If suspicious information is found indicating possible money laundering or terrorist financing activity, the AML Compliance Officer shall file an STR in accordance with the applicable laws and regulations.

9. Monitoring Accounts for Suspicious Transactions

9.1 The Company will monitor a sufficient amount of account activity to permit the identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "red flags" identified below. The Company will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. The Company will closely monitor any transaction of over USD 20,000 (or equivalent) for identification of any suspicious activity.

9.2 The AML Compliance Officer will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious transactions to the appropriate authorities, when necessary. Examples of suspicious transactions, behaviours or activities that should raise a "red flag" and cause further inquiry. These "red flags" may alert the employees of the Company to possible suspicious activity. Some examples of "red flags" that could cause further investigation include:

9.2.1 Customers who wish to maintain a number of trustee or client accounts that do not appear consistent with the type of business, including transactions involving nominee names.

9.2.2 Matching withdrawals with deposits by different ways on the same or previous day.

9.2.3 Exposure or abuse of transfers without completing trading operations on the trading account.

9.2.4 Revelation of unusual nature of operations that do not have obvious economic substance or obvious legal purpose.

9.2.5 Customers who give conflicting information to different staff members.

9.2.6 Large cash withdrawals from a previously inactive account, or from an account which has just received an unexpected large credit from abroad.

9.2.7 A customer exhibits an unusual level of concern for secrecy, particularly with regard to the customer's identity, type of business or source of assets.

9.2.8 A corporate customer lacks general knowledge of its own industry.

9.2.9 A customer is unconcerned with the risks, commissions or other costs associated with trading.

9.2.10 Revelation of circumstances implying that the operations are performed for the purpose of money laundering or financing terrorism.

9.3 **Responding to red flags and suspicious activity**

9.3.1 When a member of the Company detects any "red flag", he must file an incident report without delay to the AML Compliance Officer. He may also be required to investigate the activity further under the direction of the AML Compliance Officer. This may include gathering additional information internally or from third party sources, classifying the account as a high risk account, placing the account under heightened supervisory review, which includes, but is not limited to, depending on the situation, turning the account over to the AML Compliance Officer for review of all orders prior to entry, daily review of all trading activity, review of all money transfer requests, review of all deposits, contacting the authorities, freezing the account, or filing a STR. The Company shall not inform anyone outside of law enforcement or other competent authorities about a STR.

10. Record Keeping

10.1 When transferring funds, the Company will record in its database at least the following information:

10.1.1 The execution date of the transmittal order;

10.1.2 The name and address of the recipient;

10.1.3 The amount of the transmittal order;

10.1.4 The identity of the recipient's financial institution, and;

10.1.5 The account number of the recipient.

10.2 For each transmittal order that the Company accepts, it will retain in its files any payment instructions received from the transmitter with the transmitter's order and any form relating to the transmittal of funds that is completed by the person placing the transmittal. With regards to the STR Maintenance and Confidentiality, all employees of the Company shall be aware of to whom and in what format their suspicions must be reported. They will also receive training from the AML Compliance Officer upon, and during the course of, their employment.

10.3 The AML Compliance Officer shall hold AML records, STRs and supporting documentation confidential and ensure that STRs are filed as required. This information will not be communicated to anyone other than law enforcement or other competent authorities. Once an internal suspicion report is made to the AML Compliance Officer or an STR has been submitted to the FIU, no employee of the Company shall warn or inform the owner of any funds of any report or any action that is to be taken in respect of any transaction concerning such funds. When an STR has been

made to the FIU with respect to a particular customer, the Company shall ensure that due care is taken during subsequent enquiries so as not to alert the customer about the disclosure. Appropriate measures shall be taken by the Company to ensure that the offence of tipping off is not committed.