AML POLICY

VERSION 1.0

SPECTRA GLOBAL LTD

AN INVESTMENT DEALER (FULL-SERVICE DEALER EXCLUDING UNDERWRITING) LICENCE AND GLOBAL BUSINESS COMPANY LICENSED BY THE FSC

Spectra Global Ltd. (the “Company” or “SGL”) holds a Global Business License (“GBL”) issued by the FSC on 29 June 2023 as well as an Investment Dealer (Full Service Dealer excluding Underwriting) license (the “ID License”) granted by the FSC on 29 June 2023.

An investment dealer has an affirmative duty to act in the best interests of its clients and to make full and fair disclosure of all material facts to the exclusion of any contrary interest. Generally, facts are “material” if a reasonable investor would consider them to be important. The duty of addressing and disclosing conflicts of interest is an ongoing process and as the nature of an investment dealer's business changes, so does the relationship with its clients.

The Company will be both acting as an intermediary in the execution of securities transactions for clients and will also be dealing on its own account, that is trade in securities as principal with the intention of reselling these securities to the public. The Company will be offering Online Trading of various derivatives and other financial instruments on a non-deliverable basis only and the Company will not be engaged in the physical delivery of any instruments or its underlying.

1. **Legislative Framework:**

- The legislative requirements and framework for a Company holding a Global Business Licence and an Investment Dealer Licence in Mauritius are set out in the Securities Act 2005 and the Securities (licensing) Rules 2007
- Income Tax Act 1995 as amended by Finance Acts and complemented by Regulations
- Companies Act 2001 as amended by Finance Acts and complemented by Regulations
- Financial Intelligence and Anti Money Laundering Act 2002 as complemented by the FIAML Regulations 2018
- Prevention of Terrorism Act 2002 as complemented by Regulations
- Mutual Assistance in Criminal and Related Matters Act 2003 as amended by the relevant Finance Acts
- Banking Act 2004 as complemented by the relevant Codes and Regulations
- Financial Reporting Act 2004 as amended by Finance Acts
- Securities Act 2005 as complemented by Regulations, including The Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008
- The Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008
- Financial Services Act 2007 as complemented by Guidelines, Codes and Circular Letters
- Insolvency Act 2009
- The Data Protection Act 2017 as complemented by Regulations
- The Finance (Miscellaneous Provisions) Act 2018
- The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
- The Anti-Money Laundering and Combating of the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019
- The Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2020
- FSC Guide to Fitness and Propriety
- Guidelines on The Implementation of Targeted Financial Sanctions under The United Nations (Financial Prohibitions, Arms Embargo And Travel Ban) Sanctions Act 2019 issued on 25 August 2020 by the National Sanctions Secretariat
- FSC Communique on the Guidelines on The Implementation of Targeted Financial Sanctions under The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 issued on 25 August 2020
- FSC Anti-Money Laundering and Combatting the Financing of Terrorism Handbook 2020, updated on 31 March 2021 and last revisited in September 2022
- The Securities (Amendment) Act 2021

- Financial Crimes Commission Act 2023
- The Finance (Miscellaneous Provisions) Act 2024
- The Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2024.

2. Anti-Money Laundering and Combatting Financing of Terrorism (AML/CFT)

2.1. The Board of the Company has adopted an AML/CFT Framework to combat money laundering and financing of terrorism as per the requirements of the FIAMLA, FIAMLR 2018, the FSC Handbook and other relevant guidelines/circulars issued by the FSC.

2.2. The Board has put the following into operation:

- Programs for assessing risk relating to money laundering and financing of terrorism.
- The formulation of a control policy that will cover issues of timing, degree of control, areas to be controlled, responsibilities and follow-up.
- Monitoring programs in relation to complex, unusual or large transactions.
- Enhanced due diligence procedures with respect to persons and business relations and transactions carrying high risk, and high-risk countries in accordance with section 17H of the FIAMLA, and with persons established in jurisdictions that do not have adequate systems in place against money laundering and financing of terrorism.
- Providing employees, including the Money Laundering Reporting Officer, from time to time with training in the recognition and handling of suspicious transactions.
- Making employees aware of the procedures under the FIAMLR 2018, the FSC Handbook and any other relevant policies, guidelines/circulars; and
- Establishing and maintaining a manual of compliance procedures in relation to anti-money laundering.

2.3. The Board should ensure compliance with the requirements of FIAMLA and FIAMLR 2018 and the following forms part of the AML/CFT framework adopted by the Company:

i. The Board is responsible for managing the Company effectively and is in the best position to understand and evaluate all potential risks to the financial institution, including those of money laundering and financing of terrorism. The Board must therefore take ownership of, and responsibility for, the business risk assessments and ensure that they remain up-to-date and relevant. On the basis of its business risk assessment, the Board must establish a formal strategy to counter money laundering and financing of terrorism. Where the Company forms part of a group operating outside Mauritius, that strategy may protect both its global reputation and its Mauritius business. The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for countering money laundering and financing of terrorism, and, in particular, responsibilities of the Compliance Officer ("CO") and Money Laundering Reporting Officer ("MLRO").

ii. The Company has established and maintains an effective policy, for which responsibility shall be taken by the Board, and such policy shall include provision as to the extent and frequency of compliance reviews. The Board should take a risk-based approach when defining its compliance review policy and ensure that those areas deemed to pose the greatest risk to the firm are reviewed more frequently.

iii. The Board must consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance at a minimum annually, or whenever material changes to the Company occur. Where, as a result of its review, changes to the compliance

arrangements or review policy are required, the Board must ensure that the Company makes those changes in a timely manner.

iv. The Company has appointed a CO. In addition to appointing a CO, an independent audit function to test the money laundering and financing of terrorism policies, procedures and controls of the Fund/ Company should be maintained.

v. The Board must ensure that the compliance review policy takes into account the size, nature and complexity of the business of the financial institution, including the risks identified in the business risk assessments. The policy must include a requirement for sample testing of the effectiveness and adequacy of the financial institution's policies, procedures and controls.

vi. The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for the money laundering and financing of terrorism, and, in particular, the responsibilities of the MLRO and CO.

vii. According to the FSC Handbook, the board or senior management of the Company must establish documented systems and controls which:

a) Undertake risk assessments of its business and its customers.
b) Determine the true identity of customers and any beneficial owners and controllers.
c) Determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship.
d) Require identification information to be accurate and relevant.
e) Require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to transactions which are complex, both large and unusual, or an unusual pattern of transactions which have no apparent economic or lawful purpose.
f) Compare the expected activity of a customer against the actual activity.
g) Apply increased vigilance to transactions and relationships posing higher risks of money laundering and financing of terrorism.
h) Ensure adequate resources are given to the CO to enable the standards within the FSC Handbook to be adequately implemented and periodically monitored and tested.
i) Ensure procedures are established and maintained which allows the MLRO and the Deputy MLRO to have access to all relevant information, which may be of assistance to them in considering a suspicious transaction report ("STRs");

3. Prevention of Money Laundering and Terrorist Financing

3.1. The legislative framework has been set by the FIAMLA, followed by the FIAMLR 2018 which are effective since 01 October 2018.

3.2. In April 2012, the Code on Prevention of Money Laundering and Terrorist Financing issued by the FSC in 2012 (the "FSC Code") came into effect and the same was updated on 25 May 2017. However, the FSC has, on 06 November 2020, by way of a Circular Letter referenced as CL061120, repealed the FSC Code until the issuance of any additional enforceable Anti Money Laundering/Combatting Terrorist Financing (AML/CFT) requirements.

3.3. However, the repeal of the FSC Code will not, inter alia, affect any obligations or liability incurred thereunder, nor will it affect anything done or suffered under the repealed FSC Code.

3.4. The FSC has reserved itself the right to take any regulatory or disciplinary actions for any breaches of the said code which have occurred on or before 06 November 2020.

3.5. In addition, the FSC issued its new FSC Handbook on 13 January 2020 to provide guidance to financial institutions on the anti-money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction framework. The FSC Handbook is a supplement to the FSC Code. Although the FSC Handbook does not aim to prescribe an exhaustive list of recommended AML/CFT practices, it shall assist financial institutions in shaping their systems of internal controls on areas such as risk-based approach, customer due diligence measures, electronic identification and verification, monitoring of transactions whether automated or manually, screening and training of staff, to name a few. The FSC would take the FSC Handbook guidance into account when assessing the level of compliance with the FIAMLA and FIAMLR 2018 while conducting onsite visits.

3.6. The Company is required under its GBL to adopt, enforce and re-assess on an annual basis, its anti-money laundering and combating of financing of terrorism framework.

4. Money Laundering

4.1. The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source. Illegal arms sales, smuggling, and the activities of organized crime, including for example drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to “legitimize” the ill-gotten gains through money laundering.

4.2. Put simply, money laundering involves the channelling of proceeds of illegal activity into the stream of commerce and finance in order to disguise the nature, location, source, ownership or control of such proceeds.

5. Money Laundering Cycle

5.1. Money laundering is not a single act but is in fact a process that is accomplished in basic steps. These steps can be taken at the same time in the course of a single transaction, but they can also appear in separable forms one by one as well. The steps are:

i. **Placement**
This is the first stage in the washing cycle or the initial point of entry of “dirty money” into the legitimate financial system. This can be done by breaking large amounts of cash into less conspicuous, smaller amounts that are then deposited into a bank account.

ii. **Structuring/Layering**
This is the deliberate creation of complex transactions to hide the criminal origin of the money. It is typically designed to confuse law enforcement who would be forced to commit more resources to follow a more complex paper trail. The laundered might simply wire funds through a series of accounts.

iii. **Integration**
This is the ultimate introduction of money into the legitimate financial system where the criminal believes it would no longer be possible or easy to associate with the underlying criminal offence.

6. Policy

6.1. In view of the above, summarized below is the Company's "Anti-Money Laundering Policy" based on the provisions contained in the Mauritius AML laws and applicable regulations, and guidelines issued by the FSC in this regard.

6.2. The Company shall not accept funds in cash or third-party cheques from clients. It is the policy of the Company to seek to prevent the misuse of the funds it manages, as well as preventing the use of its personnel and facilities for the purpose of money laundering and terrorist financing. The Company has adopted and enforced policies, procedures and controls with the objective of detecting and deterring the occurrence of money laundering, terrorist financing and other illegal activity.

6.3. Anti-money laundering ("AML") compliance is the responsibility of every employee (as applicable). Therefore, any employee (as applicable) detecting any suspicious activity is required to immediately report such activity to the MLRO/DMLRO under the FIAMLR 2018. The employee (as applicable) making such a report should not discuss the suspicious activity or the report with the client in question or with any other person that may jeopardise further investigation of the matter by law enforcement authorities.

6.4. The MLRO is responsible for ensuring that the Company complies with the applicable AML laws and regulations.

6.5. The MLRO/DMLRO will review any reports of suspicious activity which have been observed and reported by employees (as applicable) and report to the FIU where appropriate.

7. Client Acceptance Policy and Procedures

7.1. All persons sourcing clients on behalf of the Company shall be required to adhere to the requirements specified herein below that are aimed to identify the types of clients that are likely to pose a higher than the average risk of money laundering or terrorist financing.

7.2. The Client Acceptance Policy and Procedures adopted by the Company can be found in the AML/ CFT Framework adopted by the Company.

8. Screening

8.1. Screening covers Sanctions, PEPs and Adverse Media on the customers, Associated Parties, beneficial owners ("BO") and all parties identified in the organisational and control structure. The Company shall ensure that its customers, connected parties of customers and all natural persons appointed to act on behalf of customers are screened through World Check and Internet Check for the purpose of determining if there are any money laundering and terrorism financing risks in relation to the customers.

8.2. All new customers and their Associated Parties (including B.O., Immediate, Intermediate and Ultimate owners) must be screened upfront through World Check and Internet Check, prior to onboarding. Existing customers must also be screened continuously. It is the Company's responsibility to ensure that ongoing screening is carried out on its applicants for business.

8.3. The PEP Policy adopted by the Company can be found in the AML/ CFT Framework adopted by the Company.

9. Sanctions Screening

9.1. Sanctions are measures imposed by governments across the world in response to a variety of international issues including terrorism and nuclear weapons proliferation. Sanctions make it an offence to do business with persons or entities listed in such sanctions and in some cases, the assets of sanctioned individuals/entities are subject to an asset freeze. Sanctions lists are local and/or international lists of persons and entities with whom a business relationship may not be established and their assets, where applicable are to be frozen.

9.2. World check compliance screening is performed via LSEG (a.k.a Refinitiv) and Infinitix. The screening software encompasses the following list: the Office of Foreign Assets Control (OFAC), United Nations Security Council (UNSC) and European Union (EU).

9.3. Sanctions screening of all customers and where possible suppliers against applicable local and international sanctions and PEP lists shall be conducted. Where sanctions screening identifies a potential match, the result must be properly investigated in order to determine whether it is a positive match. In the event that the match is positive, it must be reported to the CO for further investigation.

9.4. The Targeted Financial Sanctions Policy adopted by the Company can be found in the AML/ CFT Framework adopted by the Company.

10. Ongoing monitoring of existing clients

10.1 The frequency of the ongoing monitoring of the end clients shall be on a risk- based approach. For example, low risk will be reviewed every 3 years, medium risk will be reviewed every 2 years and high risk will be reviewed every year.

10.2 This implies:

(a) Screening of clients (Refinitiv and Infinitix – a new software which has just been acquired by the MC) to be done by the MC on behalf of the Company;

(b) Handling of Adverse Media / compliance reports;

(c) Verifying source of funds / wealth, where applicable;

(d) Ensuring that documents, data, or information collected are kept up to date and relevant by undertaking reviews of existing records;

(e) Obtaining information on the reasons for intended or performed transactions / scrutiny of transactions undertaken throughout the course of the relationship, by way of review of bank

statements or otherwise, to ensure that the transactions are consistent with its knowledge of the customer and the business and risk profile of the customer;

(f) obtaining the approval of the Board to continue the business relationship;

(g) Reviewing the risk assessments of the customers on a risk basis.

10.3 Where the Company is unable to satisfactorily apply enhanced due diligence measures as per its internal procedures or where the Company has discovered that the customer has provided false or stolen identification documentation or information, it shall terminate the business relationship with the customer and where applicable, file a suspicious transaction report as required. The Company shall adopt its Internal Procedures Manual which elaborates on Internal and External Reporting Procedures in this regard.

11 Ongoing monitoring of PEP

11.1 Once a business relationship has been established with a PEP, ongoing monitoring must be conducted on all related transactions to ensure that they are in line with the customer's source of funds and wealth and original account mandate. This can be achieved by requesting additional information to understand the purpose of a transaction verifying the provenance of the source of funds and where required, to request for evidentiary documents such as agreements, invoices, bank statements, etc.

11.2 Furthermore, quarterly World Check and Internet Check must be conducted on the PEP and evidence of such screening kept on record.

11.3 Annual reviews must be conducted on all customers identified as PEPs and approved by Board / Senior Management.

11.4 The following information and documentation must be reviewed/reconfirmed/updated when conducting an annual review of a PEP investor:

- All KYC information.
- The relevance of the EDD conducted initially includes reconfirmation of the customer's source of funds and source of wealth; and
- Where adverse information such as ongoing litigation or regulatory proceedings were noted as part of the onboarding information, further checks must be undertaken to ascertain any outcomes or obtain updated information.

11.5 Information obtained from the customer may be compared against additional independent sources in order to verify the accuracy of the information. The formal decision and reasons to either maintain or terminate the PEP relationship must be documented.

11.6 Factors to consider in establishing/maintaining/terminating a customer relationship with a PEP

11.7 The following are factors, which should be considered in deciding whether to establish/ maintain/terminate a customer relationship with a PEP:

- Funding of the account is the Company's account in line with the customer's source of funds and wealth and original account mandate.
- Is there a history of suspicious or unexplained transactions.
- Is the customer responsive to requests for up-to-date information.

11.8 There should be a detailed consideration of the rationale for establishing, maintaining, or terminating the business relationship with the PEP. – The ultimate decision to onboard a PEP is reserved for senior management.

[Note – where a customer has been accepted and the said customer or its beneficial owner or its associate or its family member is subsequently found to be or subsequently becomes a PEP, appropriate EDD and Company Board's approval should be obtained as per the above in order to continue such business relationships.]

12 Connected persons that are PEPs

12.1 'Connected persons' will include underlying principals such as beneficial owners and controllers.

12.2 The Company must apply appropriate EDD measures on a risk-sensitive basis where an applicant for business or customer (or any connected person, such as a beneficial owner or controller) is a PEP, and must ensure that they operate adequate policies, procedures and controls to comply with this requirement.

12.3 The Company must:

a) Develop and document a clear policy on the acceptance of business relationships or one-off transactions with such persons and ensure that this is adequately communicated.
b) obtain and document the approval of senior management prior to establishing relationships with such persons.
c) Where such persons are discovered to be so only after a relationship has commenced, thoroughly reviewed the relationship and obtained senior management approval for its continuance; and
d) Apply EDD measures to establish the source of funds and source of wealth of such persons.

13 Steps for EDD measures:

13.1 The company :

a) **Will identify** the type of high-risk clients or situations, such as PEPs, clients from high-risk jurisdictions, or those involved in suspicious or unusual activities.
b) **Must obtain** senior management approval before establishing or continuing such relationships.
c) **Will collect** comprehensive KYC information, verify the source of funds and source of wealth, and understand the purpose of the transaction..
d) **May request** other relevant documents in addition to the source of wealth and source of fund depending on the type of risk or situation

13.2Supporting document may include:

Individuals	Corporate
6 months' bank statements: ▪ Whereby it shows sufficient incoming and outgoing funds (Salary, investments etc.) ***(Duly translated in English or French where applicable).***	**Either one of the followings:** ▪ Latest financial statements (audited where applicable) ▪ Management Accounts ▪ 6 months' bank statements ▪ Annual Report
Duly filled and Signed Declaration of Source of Funds & Source of Wealth Form	Duly filled and Signed Declaration of Source of Funds & Source of Wealth Form
Either one of the followings: ▪ Updated and Signed CV - Showing qualifications (education) and detailed work experience. ▪ Letter of Employment from Employer. ***(In cases where the client did not provide his employment details on the Application Form).***	

e) **Will verify** the documents provided and conduct adverse media and sanctions screening using independent sources. (example worldcheck, Refinitiv)
f) **Will assess and document** the client's risk profile based on the findings, and where applicable, record the client in the PEP register etc.
g) **Will conduct** ongoing monitoring to ensure transactions remain consistent with the client's risk profile and declared financial background**.**
h) **Will file** a Suspicious Transaction Report (STR) with the MLRO and relevant authorities if suspicious activity is identified.

14 Targeted Financial Sanctions

14.1 In order to ensure that employees (if applicable) are of the required standard of competence, which will depend on the role of the employee, the Company gives consideration to screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions, prior to, or at the time of, recruitment.

14.2 The Company also carries out periodic ongoing of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

14.3 Section 23(1) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (the "UN Act") provides that subject to the said Act, no person shall deal with the funds or other assets of a designated party or listed party, including:

a) All funds or other assets that are owned or controlled by the designated party or listed party, and not just those that can be tied to –
   I. A particular terrorist act, plot or threat.
   II. A particular act, plot or threat of proliferation.
b) Those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by the designated party or listed party.
c) Funds or other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by the designated party of the listed party, and
d) Funds or other assets of a party acting on behalf of, or at the direction of, the designated party or listed party.

14.4 In addition, section 23(2) of the UN Act provides that where a prohibition is in force, nothing shall prevent any interest which may accrue, or other earnings due, on the accounts held by a listed party, or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the prohibition, provided that any such interest, earnings and payments continue to be subject to the prohibition.

15 Appointment of Compliance Officer (CO), Money Laundering Reporting Officer (MLRO) and Deputy MLRO (DMLRO)

15.1 Compliance Officer

Regulations 22 (1) of the FIAMLR 2018, requires that the Company designates a CO at the senior management level for undertaking the day-to-day oversight of the AML Program for combating anti-money laundering and terrorism financing.

Currently, Mr. Tariq Caramtali has been appointed as the Company's CO and as per Regulation 22(3) of FIAMLR 2018, his responsibilities will entail the following:

I. Ensuring continued compliance with the requirements of the FIAMLA and FIAML Regulations 2018 subject to the ongoing oversight of the Board of the Company.
II. Undertaking day-to-day oversight of the AML Program
III. Regular reporting, including reporting of non-compliance to the Board of the Company; and
IV. Contributing to designing, implementing and maintaining the Company's compliance manual, policies and procedures and system for combating ML/TF.

15.2 MLRO/ DMLRO

Further, Regulation 26 of the FIAMLR 2018 requires the Company to appoint a MLRO and a DMLRO to whom all internal report of suspicious transactions must be made. In that respect, Ms. Ranjana Gujadhur has been appointed to act as the MLRO and Mr. Tariq Caramtali as the DMLRO.

According to Regulation 26(4) of the FIAMLR 2018, the MLRO and DMLRO must be:

a) Be sufficiently senior in the organisation of the financial institution or have sufficient experience and authority; and
b) Have a right of direct access to the board of directors of the financial institution and have sufficient time and resources to effectively discharge his functions.

The MLRO/ DMLRO is the person who is nominated to ultimately receive internal disclosures and who considers any report to determine whether an external disclosure is required.

The responsibilities of the MLRO will normally include, as stated in the FIAMLR 2018:

- Undertaking a review of all internal disclosures in the light of all available relevant information and determining whether or not such internal disclosures have substance and require an external disclosure to be made to the FIU.
- Maintaining all related records.
- Giving guidance on how to avoid tipping off the customer if any disclosure is made.
- Liaising with the FIU and if required the FSC and participating in any other third-party enquiries in relation to money laundering or terrorist financing prevention, detection, investigation or compliance; and providing reports and other information to senior management.

The MLRO shall provide a quarterly report on the above to the Board and the Company is required under its FSC licence to re-assess on an annual basis its anti-money laundering and combating the financing of terrorism framework.

In the absence of the MLRO, the DMLRO is expected to fulfil the duties described above. The DMLRO should be of similar status and experience to the MLRO.

16 Know Your Clients

16.1 The Financial Intelligence and Anti-Money Laundering Act 2002 (the "FIAMLA") and the Financial Intelligence and Anti-Money Laundering Regulations 2018 (the "FIAML Regulations") obligate the Company to perform thorough due diligence on its clients. The FSC has also issued an Anti-Money Laundering and Combatting the Financing of Terrorism Handbook 2020 which was updated in September 2022 to guide reporting persons on anti-money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction. By having effective systems and controls in place and having sound due diligence measures, the Company will be able to prevent and detect money laundering and terrorist financing.

16.2 To ensure compliance with the applicable Anti-Money Laundering legislation, the Company and its Administrator in Mauritius shall require a detailed verification of a prospective Client's identity and the source of payment for each transaction during the initial transaction and also on an ongoing basis. The Company has developed a risk-based due diligence approach for client acceptance. This involves the identification and verification of the clients. CDD is the process used to identify, verify, and understand the clients. The Clients

shall also be screened on risk intelligence databases and against the UN Sanctions list. The Company will require detailed verification of a client and its owners' identities before any transaction can be executed. This becomes more important in the event (i) a payment is received from an account in the name of a person or persons other than the Client, or (ii) appears that the Client is acting on behalf of some other person. Verification of the identity of the Client or the person on whose account such amount is being received is required. For the list of the documents to be required on Clients, reference is to be made to the Company's Policies and Procedures Manual.

16.3 The type of due diligence measure to be applied to a client will depend on the risk such client represents to the Company. For example, simplified due diligence may be applied where risk is low, but the simplified CDD measures shall be commensurate with the lower risk factors and in accordance with any guidelines issued by the FSC, Financial Intelligence Unit (the "FIU") or any other supervisory authority. It shall be ensured that the low risk identified is in accordance of the national risk assessment (the identification, assessment and understanding of the national money laundering and terrorist financing risks by the Minister of Financial Services and Good Governance as per section 19D (1) of the FIAMLA) or any risk assessment by the regulator whichever is recently issued. It is to be noted that simplified due diligence measures cannot be applied where there is a suspicion of money laundering or for a high-risk business relationship.

16.4 Enhanced due diligence measures shall be applied where the business relationship is high-risk.

17 Audit

17.1 (1) The Firm will commission regular reviews and assessments of the effectiveness of its money laundering policies, procedures, systems and controls, and its compliance with them, and will specifically cover the following:

(a) Sample testing of compliance with the Firm's CDD arrangements;

(b) An analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced;

(c) A review of the nature and frequency of the dialogue between the Board of Directors and the MLRO.

(2) Such reviews will be carried out by the Group's Compliance Department at least annually.

18 Red Flags

18.1 Red flags that signal possible money laundering or terrorist financing include but are not limited to:

- The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the Company's AML policies (particularly concerning 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 suspicious 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 or investment 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 legitimate 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, or asks for exemptions from the Company's policies relating to the deposit of cash.
- 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-cooperative country or territory by the FATF.
- 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 currency 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 a 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 Company, 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 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 to avoid the Company'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, Regulations 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.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose; or
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

19 Reporting of Suspicious Transactions

19.1 In accordance with the FIAML Regulations, the Company will appoint a Money Laundering Reporting Officer (the "MLRO").

19.2 The duties of the MLRO will include receiving and evaluating internal Suspicious Transactions Reports ("STRs") and, where appropriate, filing these STRs with the FIU within 5 working days from the date of the suspicious transaction has been found. In order to allow the MLRO to discharge his/her responsibilities, the Company must ensure that, at all times, the MLRO has unrestricted access to all records, and resources, and has the cooperation of the Board and client administrators as necessary for the performance of his/her functions. Detailed duties of the MLRO have been mentioned in the Policies and Procedures Manual.

And therefore:

- You ("the Client") will be under obligation to provide all necessary documents as required by the Company.
- You hereby agree and undertake to provide us with all the information we require as part of our CDD procedures.
- You hereby further authorize us or any of our agent(s) to investigate your identity, credit standing and/or any current and past investment activity, and in connection with such investigations, to contact such banks, brokers and other related parties as we shall deem appropriate and necessary.
- Without prejudice to the Terms herein, you agree that Spectra Global Ltd shall be held harmless against any loss arising as a result of any delay or failure to process any application or transaction if all such documentation as has been requested by us has not been provided by you.
- We hereby reserve the right to make necessary amendments, corrections and/or deletions to any details, particulars and information provided by the clients at our sole discretion on the company's trading platform PROVIDED THAT the said details.
- Particulars and/or information contained on the application form therein are incorrect, missing and/or unnecessary after a comparison is made with the clients' KYC documentation.

For further AML enquiries please contact us at support@sgfx.com