Anti-Money Laundering Policies

Aron Broker Ltd (Mauritius)

Effective Date: July 2024

Contents

ACKNOWLEDGMENT

The present document has been prepared after thorough review by the Board of Directors and Senior Management.
The document should be read in conjunction with:

- The Anti-Money Laundering and Countering the Financing of Terrorism Handbook, 2020, Updated on 21 September 2022;
- The Financial Intelligence and Anti-Money Laundering (FIAML) Regulations 2018;
- The Financial Intelligence and Anti-Money Laundering Act (FIAMLA) 2002;
- The Anti-Money Laundering and Combating the Financing of Terrorism (Miscellaneous Provisions) Act 2020;
- The Guidelines on the Implementation of Targeted Financial Sanctions Under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 on 25 August 2020;
- The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019;
- The FIU, Guidance Note 4 on Suspicious Transaction Report on 21 January 2014 (updated November 2020).

Application and Responsibility

- The contents of this Manual apply to all employees, including but not limited to the directors, authorized individuals, managers, executives and interns of Aron Brokers Ltd (collectively EMPLOYEES), whether employed full time or part time.
- It is the responsibility of all EMPLOYEES to read, understand and observe all the rules and procedures applicable to them, both in letter and in spirit. Failure to comply with the rules and procedures contained herein will constitute serious misconduct.
- The overall responsibility of information dissemination and ensuring compliance lies with the Compliance Officer.
- If you become aware of a violation of this manual, if you are instructed by your superior to act in contravention of this manual, or if you find yourself inadvertently in contravention of this manual, you must not hesitate to report such contravention to the Compliance Officer.
- This is the first edition of the AML/CFT/GRC Operations Manual (herein referred to as, the Manual). The Manual shall be reviewed annually and at the point of a material change in the AML/CFT legal requirements as prescribed under the Financial Intelligence and Anti-Money Laundering Act (FIAMLA), FIAML Regulations, the FSC AML/CFT Handbook, amongst others. The same shall be updated on a regular basis and the latest version control applies. Should the changes required be substantial, the Compliance Officer shall request the senior management to call a meeting with the Board and review the Manual in its entirety and make the necessary revisions.

Aron Brokers Ltd. shall be referred to as “the Company or Aron Broker”, throughout the Manual.

PART I – GOVERNANCE, RISK AND COMPLIANCE (GRC)

1. Introduction

1.1. Why Governance, Risk and Compliance

- Compliance with regulatory requirements, prudential norms and industry best practices enhances the efficiency and reputation of Aron Brokers Ltd (the Company), boosts investor confidence and helps the management to fulfil stakeholder's expectations of integrity.
- Compliance with laws, rules and standards also covers matters such as observing proper standard of market conduct, ethical business practices, managing conflicts of interest, and fair treatment of clients and stakeholders. Compliance needs to be integrated into the culture of a company and shall have to be reinforced by a close alignment of values, processes and rewards. A holistic approach to compliance ensures that the benefits of compliance far exceed the related costs.

1.2. Risk of Non-Compliance

- The compliance risk is defined as the risk of impairment to the Company business model, reputation and financial condition (resulting) from a failure to meet laws, regulations, internal standards and policies, and expectations of key stakeholders such as clients, employees and society as a whole.
- Failure to comply with the FIAML Regulations 2018 and the FIAMLA may result in a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years, according to the FIAMLA Section 32A of 2002, and Regulation 33 of the FIAML 5 Regulations 2018.

2. GRC at Aron Brokers Ltd

- At the Company, we place the highest priority on complying with rules and regulations required by the authorities.
- The commitment for compliance starts at the highest levels of the firm. Our core principles of governance and compliance are to:
    - Maintain a compliance function: The role of the compliance function is to identify, asses, advice on, monitor and report on the Company's compliance with regulatory requirements and the appropriateness, effectiveness and integrity of its supervisory procedures.
    - Act in a professional and ethical manner for the benefit of clients and always put client's interest first; communicate with clients and others in a clear and fair manner.
    - Act with independence and objectivity; avoid relationships that may impair or appear to impair our independence and objectivity.
    - Uphold the rules governing capital markets transparency and disclosure requirements and comply with letter and spirit of laws and regulations; Develop a business culture that values and promotes not only compliance with the letter of the law, but also a high ethical and investor-protected standard.

3. Responsibilities of the Board of Directors for GRC

- The Governing Board is responsible for overseeing the management of the Company's governance and compliance. The Board should approve the Company's GRC policy, including a formal document establishing a permanent and effective compliance function. At least once every year, the Board should assess the extent to which the Company is managing its compliance risk effectively.
- The Board clearly understands that compliance policies will not be effective unless the Board promulgates the values of honesty and integrity throughout the Company. Accordingly, the Board has committed to ensure that appropriate policies are in place to manage the compliance, and employees are made aware of these policies and the modes of implementation.
- The Board and Senior Management shall review and approve all policies, procedures, controls and manuals, prior to be put in use. The policies, procedures, controls and manuals shall have the Board approval date in it.
- The Board will oversee the implementation of the policies and ensure that compliance issues are resolved effectively and expeditiously by Senior Management with the assistance of the compliance function.
- The Company must ensure that the training provided to officers and employees is comprehensive and ongoing and that the officers and employees are aware of ML and TF, the associated risks and vulnerabilities of the Company, and their corresponding obligations.
- As part of compliance arrangements, the Company is responsible for appointing a Compliance Officer (CO) who is responsible for the implementation and ongoing compliance of the Company with internal programmes, controls and accordance with the requirements of the FIAMLA and FIAML Regulations 2018.
- In Addition to appointing a CO, an independent audit function to test the ML and TF policies, procedures and controls of the Company should be maintained.

4. Responsibilities of Directors for GRC

- To design, establish and maintain a compliance function and related policies and procedures, keeping in mind the prevalent regulatory practices of the region where the company operates and the strategic moral and ethical obligations of the firm to its stakeholders.
- To designate a suitable person who has the appropriate competence, to have the day-to-day responsibilities for the firm's compliance with regulatory requirements.
- To identify and assess on an ongoing basis the new or changed compliance requirements applicable to the company by any regulatory authorities; and take steps to modify existing policies and procedures to comply with the new or changed requirements.
- To provide compliance advice and support in relation to new business initiatives and ensure that a robust compliance infrastructure is implemented for any new initiatives that are undertaken.

5. Money Laundering & Terrorism Financing (ML & TF), and Responsibilities of the MLRO

- The appointment of a MLRO will be assigned in accordance with Regulations 26(1) of FIAML Regulations 2018.
- It is imperative that every financial institution appoints an appropriate MLRO who must be of sufficiently senior status and not below the rank of Manager.
- The MLRO officer or the Alternate/Deputy MRLO (DMLRO) must make sure that all sources of funds are supported by the relevant documents. It is very important that the MLRO adopt the policy of Know Your Client (KYC) framework as outlined in the Manual.
- The MLRO must ensure that the clients are running according to the business plan. Any change in business activity must be addressed to the clients.
- A proper CDD must be made to each client. Relevant online sources as well as reports provided by the authorities must be checked to ascertain if the client is risky either by virtue of Politically Exposed Person (PEP) status or has the name listed as terrorist, as listed by the US. In the case of a former PEP, it is incumbent on the MLRO to ensure that procedures are followed for enhanced due diligence and monitoring.
- Countries with deficiencies in their AML regime will need enhanced due diligence.
- Any suspicious transaction must be reported to the Board and the Financial Intelligence Unit (FIU) using the appropriate forms found in the Manual.
- It is important to note that the Board has given the MLRO the freedom to make his or her decision and without influence, pressure or fear of repercussions if the senior colleagues disagree with his / her decision.
- The MLRO shall exercise his reasonable judgement in deciding whether certain Client's DD documentation should be acceptable to the Company, subject to the laws and practices of the Client's jurisdiction.
- Important Aspects Loita Management Services Limited (LMS) has a Compliance Due Diligence agreement with the Company. Therefore, the MLRO and Compliance Officer are LMS's employees.

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

- To undertake 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;
- To maintain all related records.
- To give guidance on how to avoid tipping off the client if any disclosure is made.
- To liaise 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.
- To provide reports and other information to the Board, if any cases encountered; and to produce in an annual basis (initially) the MLRO Report and submit the same to the Board.

6. Responsibilities of the Compliance Officer (CO)

- To ensure effective management of the company's compliance function.

- To advise management, during the inception of new business processes, of the underlying integrity and compliance implications of these processes.
- To ensure corporate-wide communication of the compliance policy and its implementation and to report to the directors on the management the Company's compliance risk.
- To act as a central repository of all information on rules, codes and business practices and ensure dissemination to all appropriate people in the organization.
- To establish detailed written compliance procedures that should be followed by all staff members.
- To ensure that the compliance policies and procedures are observed and breaches, if any, are remedied immediately and disciplinary actions, if required, are taken against the personnel responsible for the breach.
- To regularly report to the Board on compliance issues (if any cases encountered) and to make an informed judgment on the effectiveness corporate-wide compliance policy.
- To produce in an annual basis (initially) a Compliance Report and submit the same to the Board.
- To report promptly to the Board, of any material compliance failures (e.g., failures that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation).
- To liaise with the Finance Officer to ensure accuracy of financial recording and compliance with established accounting standards (IFRS);
- To ensure that all requests and instructions of regulators are complied with in a timely and accurate manner.
- To ensure that day to day compliance monitoring and administration are carried out to specified standards.
- To ensure that all registrations with the FSC and other regulatory authorities are current and up to date.
- To work with the legal advisors and ensure that valid agreements with contracting parties or counterparties are put in place for new business initiatives.
- To update compliance manuals and procedures.
- To arrange training and development of staff on regulatory responsibilities.

7. Independent Compliance audit

The FIAML Regulations 2018 requires the audit process to be carried out independently. The audit functions should be independent of, and separate to the executive team dealing with the Company's Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) processes. The auditor must not have been involved in the development of the risk assessment, or the establishment, implementation, or maintenance of the Company's AML / CFT program. An independent audit function shall be appointed by the Company, in order to test the ML and TF policies, procedures and controls that should be maintained.

7.1. Independent Compliance Audit Frequency

Independent compliance audit shall be conducted Annually and/or when there has been a major change in the AML / CFT risk assessment, policies, or procedures.

7.2. Independent Compliance Audit Depth

The appointed Independent Audit Function shall:

- Evaluate how the Company adheres to rules, regulations and laws.
- Cover the adequacy and effectiveness of the Company's policies, systems, controls, and procedures relating to AML/CFT. This is done by having a detailed plan covering access to information and relevant staff, testing of the effectiveness of existing procedures and controls and any automated systems in use by the Company, random selection of transactions/files for review and record-keeping.
- Verify if the AML/CFT program adopted by the Company is adequate and effective; and
- Advise on any changes that may be required.

The Independent Audit shall test compliance in the following areas:

- AML / CFT policies and procedures.
- Internal risk assessment.
- Risk assessment on the use of third-party service providers (Outsourcing).
- Compliance Officer function and effectiveness.
- MLRO function and effectiveness.
- Implementation and effectiveness of mitigating controls, including customer due diligence and enhanced measures.
- AML / CFT training.
- Record keeping obligations.
- Targeted Financial Sanctions (TFS);
- Suspicious transaction monitoring and reporting; and
- Technological reliance and effectiveness.

8. Internal Due Diligence and Training

8.1. Screening

As part of the process of hiring staff members, the Company must ensure that the same are screened against the required numerous Sanctions, PEP, Criminal related lists as well as adverse media results, prior to finalizing the hiring process. This is conducted to assist in the prevention and detection of financial crime, as well as to ensure that the Company is compliant with the existing regulations.

Screening of existing Staff Members and the Company's Stakeholders in general should also be conducted periodically as part of the Company's Business Risk Assessment (BRA).

- Screening for PEPs & PEPs by Association
    - Potential Employees are screened against the PEP list to verify if any positive hit is
    - triggered.
    - It shall be determined whether the potential employee is a PEP or PEP by association.
    - The Compliance shall conduct an EDD Assessment, including a recommendation, and submit it to the Board/Senior Management in such cases.

- Board/Senior Management shall decide whether to proceed or not with the hiring process.

- Screening against Sanctions Lists
  - Potential Employees are screened against Sanctions lists, as required by the Commission.
  - In the event that a positive hit is triggered by the screening process, an EDD Assessment shall be conducted and submitted to the Board/Senior Management.
  - Potential Employee job application shall not be carried forward and further action shall be taken as per required by law / regulations / the Commission.

- Screening against Crime Related Lists
  - Potential Employees are screened against criminal related lists;
  - In the event that a positive hit is triggered by the screening process, an EDD Assessment shall be conducted and submitted to the Board/Senior Management;
  - Potential Employee job application shall not be carried forward and further action shall be taken as per required by law/regulations/ the commission.

- Screening for Adverse Media Results
  - Potential Employees are screened against several internet articles that have been made available to the public, in order to find any related adverse media results;
  - In the event that a positive hit is triggered by the screening process, the compliance shall verify the gravity of the results and give its feedback and recommendation to the Board/Senior Management on the EDD Assessment Report.

8.2. Training

While there is no single or definitive way to conduct training, the critical requirement is that training is adequate and relevant to those being trained and that the content of the training reflects good practice.

Training shall be carried out to meet the requirements of FIAML Regulations 2018, if new legislation or significant changes to this Handbook are introduced, or where there have been significant technological developments within the Company or with the introduction of new products, services or practices.

The guiding principle of all AML and CFT training should be to encourage and ensure that directors, officers and employees, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the financial institution against the risks of ML and TF.

The Company shall keep records containing information and data regarding the attended trainings.

- Scope, Content and Methodology of training
  - In accordance with Regulation 22(1)(c) of FIAML Regulations 2018, the ongoing training provided by the Company shall cover:

- The FIAMLA, FIAML Regulations 2018, any AML / CFT Code issued by the FSC and this Handbook;
- The implications of non-compliance by employees to requirements of FIAMLA, FIAML Regulations 2018, any AML / CFT Code issued by the FSC and this Handbook; and
- The Company's policies, procedures and controls for the purposes of foreseeing, preventing and detecting ML and TF.

- New and existing employees, officers, Board members and Senior Management must have a good understanding of the Company's business activities, functions and its AML / CFT policies and procedures.
- Staff Members (including Senior Management) shall attend AML / CFT related training and acquire the equivalent of 10 hours (minimum) of CPDs per Year.
- In-house training covering the Company's AML / CFT Policies and procedures.
- In-house training, on how to use the Company's compliance due diligence software, shall be provided to all relevant staff members.
- New employees and existing employees shall be given graded tests pertaining to the in-house training. The grades will impact on the employees' Annual Reviews at the end of the Financial Year.
- Staff members shall be required to provide a report / summary to Senior Management and CO, of the attended courses, webinars, seminars and trainings. The evaluation of the reports shall form part of the Annual Reviews and impact the result of the same.
- The Company's staff members shall receive a training program and shall be requested to attend certain trainings, seminars, webinars or courses.
- The Company shall ensure that the ongoing training provided to directors, officers and employees also covers, to a minimum:
    - The requirements for the internal and external disclosing of suspicion.
    - The criminal and regulatory sanctions in place, both in respect of the liability of the Company and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of the Company.
    - The identity and responsibilities of the MLRO, CO and DMLRO.
    - Dealing with business relationships or occasional transactions subject to internal disclosure, including managing the risk of tipping off and handling questions from customers.
    - Those aspects of the Company's business deemed to pose the greatest ML and TF risks, together with the principal vulnerabilities of the products and services offered by the Company, including any new products, services or delivery channels and any technological developments.
    - New developments in ML and TF, including information on current techniques, methods, trends and typologies.
    - The Company's policies, procedures and controls surrounding risk and risk awareness, particularly in relation to the application of CDD measures and the management of high risk and existing business relationships.

- The identification and examination of unusual transactions or activity outside of that expected for a client.
- The nature of terrorism funding and terrorist activity in order that employees are alert to transactions or activity that might be terrorist- related.
- The vulnerabilities of the Company to financial misuse by PEPs, including the effective identification of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs;
- UN, EU and other sanctions and the Company's controls to identify and handle natural persons, legal persons and other entities subject to sanction; and
- Interruption or stop of the performance of a CDD process and file a STR, if the Company reasonably believes that the performing it will tip off the client or potential client.

- The Board and senior management shall receive adequate training to ensure they have the knowledge to assess the adequacy and effectiveness of policies, procedures and controls to counter the risk of ML and TF. The additional training provided to the Board and Senior Management must include, at least, a clear explanation and understanding of:
  - Offences and penalties arising for non-reporting or for assisting money launderers or those involved in terrorist financing.
  - Requirements for CDD including verification of identity and retention of records; and
  - In particular, the application of the Company's risk-based strategy and procedures.
- Ongoing professional development, including participating in professional associations and conferences, is vital for MLROs / DMLROs. In addition, MLROs and DMLROs should receive in depth training on all aspects of the prevention and detection of ML/TF, including, but not limited to:
  - AML / CFT legislative and regulatory requirements.
  - The international standards and requirements on which the Mauritius' strategy is based, namely the FATF 40 Recommendations and ML / TF typology reports that are relevant to their business.
  - The identification and management of ML / TF risk
  - The design and implementation of internal systems of AML / CFT control.
  - The design and implementation of AML / CFT compliance testing and monitoring programs.
  - The identification and handling of suspicious activity and arrangements and suspicious attempted activity and arrangements.
  - The money laundering and terrorist financing vulnerabilities of relevant services and products.
  - The handling and validation of internal disclosures.
  - The process of submitting an external disclosure.
  - Liaising with law enforcement agencies.
  - ML / TF trends and typologies; and

        - Managing the risk of tipping off.
    - The CO is responsible for ensuring continued compliance with the requirements of FIAMLA and FIAML Regulations 2018 and having an overall oversight of the program for combatting ML / TF amongst others - Regulation 22(3) of FIAML Regulations 2018.
    - The CO should receive in depth training on all aspects of the prevention and detection of ML / TF, including, but not limited to, addressing the monitoring and testing of compliance systems and controls (including details of the Company's policies and procedures) in place to prevent and detect ML / TF.

9. Cost of Compliance

- There is a cost to compliance which needs to be factored into the operations of the Company.
- Prior to the annual budget preparation, the Compliance Team should be consulted about their budget and expectations.
- The budget allocated to the project will directly correlate to the Company's risk exposure.
- If there are budget cutbacks, these need to be clearly explained and documented.

10. Conduct of Business Policies in Governance & Compliance

10.1. Client Restrictions

Aron Brokers Ltd must ensure that the business is conducted only with genuine and trustworthy clients

- Our procedures will ensure a check on the individual client's past experience and CDD
- And relevant KYC check.
- We will devise appropriate systems and controls that shall ensure that the financial status of the individual client and his/her credentials to qualify as a client are checked prior to being admitted as a client.

10.2. Responsible Conduct

As a registered company providing Global Business Services, including "Investment Dealer Licence (excluding underwriting)", it is our professional and ethical responsibility to conduct ourselves in the most responsible manner and with clients' best interests in mind.
The client's interest is paramount to the firm. We are responsible to safeguard our client's interest, to avoid conflict of interest situations, to communicate with the client in an honest and fair manner, deal fairly and objectively with the clients and treat all clients fairly and equally.

10.2. Conflict of Interest

- All clients shall be treated fairly. Any conflict of interest between the client and the firm shall be avoided.
- Client interests are paramount. All employees of our company including Managers should ensure that client interests supersede employees' interests in all aspects of client relationship, including (but not limited to) recommendations, advice or change in prior recommendations and actions.

- Where the conflict of interest is unavoidable such conflicts shall be managed in such a way that the client's interest has priority and is protected. If the conflict of interest is of a significant nature, the firm shall decline to act for the client.
- We must not act, or cause others to act, on material non-public information or knowledge that could affect the value of a publicly traded investment. Procedures shall be established to create effective information barriers ("Chinese walls") to prevent the disclosure and misuse of material non-public information.

10.3. Dealing with Clients' Money

Segregation of client money in a separate CLIENTS Bank account is important and money is to be monitored and documented.

11. Confidentiality

We will treat all information collected from its clients and employees for the purpose of carrying out its business or administrative functions as confidential.

11.1. Maintenance of Records

- We will review the advanced information and documentation management policies, procedures and standards of ISO 9001, ISO 154489 and ISO 27001 and implement where necessary.
- All records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of clients and beneficial owners, and records and the results of any analysis / assessment undertaken in accordance with the FIAMLA, all of which shall be maintained for a period of not less than 7 years.
- Adequate records will be maintained by the Firm for all transactions it undertakes, including but not limited to the following summation:

11.2. Detail Record keeping requirement

- Client verification, due diligence, client agreements, complaints and any other client-related documentation. A minimum period of 7 years from the date on which the business relationship ended.
- Financial statements and reports. Minimum period of 7 years from the date on which it was provided.
- All records and documents not mentioned in the preceding table shall be maintained for a minimum period of 7 years.
- Records on transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders, which shall be maintained for a period of 7 years after the completion of the transaction; and
- Copies of all suspicious transaction reports or other reports made to the FIU in accordance with the FIAMLA, including any accompanying documentation, which shall be determined for a period of at least 7 years from the date the report was made.
- All records shall be available for inspection by the FSC at all times during office hours.

- The joint authorisation of the CO and one Director shall be required before destruction of any record.
- The CO ensures that the compliance policies and procedures are observed properly and breaches if any are remedied immediately and disciplinary actions if required are taken against the personnel responsible for the breach.
- The CO ensures that all regulators' requests and instructions are complied with in a timely and accurate manner.
- The CO will ensure that compliance monitoring and administration is carried out strictly according to the compliance program.

The following information should be kept for every transaction carried out in the course of a business relationship or one-off transaction:

- The name and address of the client;
- If a monetary transaction, the kind of currency and the amount;
- If the transaction involves a client's account, the number, name or other identifier for the account;
- The date of the transaction;
- The details of the counterparty, including account details;
- The nature of the transaction; and
- The details of the transaction.

PART II – RISKS

1. Risk

Aron Brokers Ltd will ensure that the approved party / parties carrying out its controlled function:

- Act with integrity.
- Act with due skill, care and diligence;
- Observe proper standards of market conduct.
- Deal with the FSC and other regulators in an open and co-operative way; and
- Disclose appropriately any information of which the FSC would reasonably expect notice;
- Take reasonable steps to ensure that the regulated business of the company is organized so that it can be controlled effectively.
- Is of financial soundness;
- Reports to the Board;
- Is aware of emerging regulatory issues.

Compliance mode culture along with a values-led culture within the Company will together create a symbiotic relationship to a full Compliance Program. Implementation of appropriate Risk Controls will also be more effective built on Trust and not if the GRC Officer/Responsible is seen as an enforcer, opportunist or snitch. Personal Integrity forms part of the fundamental aspects of a good compliance model. The objective is the same - a successful company that observes the relevant codes of practice.
Reports regarding the Risk Classification, Expired or Missing KYC, PEPs, etc., are generated on a regular basis, in order to keep timely and updated information, which can be provided to the relevant stakeholders, and authorities at short notice.

2. Risk Based Approach

A risk-based approach requires us to assess the risks of how we might be involved in ML and TF, taking into account clients, countries or geographic areas, the products, services and transactions the clients offer or undertake, and the delivery channels by which those products, services and/or transactions are provided.
The following are procedural steps to manage the ML and TF risks, according to the FSC AML CFT Handbook 2020, Updated on 21 September 2022

2.1. Identifying the Risk

- Identifying the specific threats posed to the Company by ML and TF and those areas of the Company's business with the greatest vulnerability;
- A periodic review of clients' existing activities should be conducted using the necessary and available means;
- The Company and client's risk is reviewed whilst taking into account that the problem may also be considered as an opportunity.

Aron Brokers Ltd' MLRO and CO may have the further following queries:

- Are we tracking changes on beneficial owners over time?

- Are we completing our periodic screening using the CDD tools?
- Did we check the FSC recommended Sanctions and PEP lists and any other Public Records Data Sources?
- Are the financial transactions in accordance with the business plan and the contracts in place?
- Are transactions being thoroughly monitored?
- Is the risk related to Market Abuse?
- Is data destruction properly managed? Both physical and digital?
- Is training in place for both initial and knowledge update, to all staff members, to ensure that policies and procedures regarding ML and TF are being strictly followed?
- Are the policies read and understood by all staff members?
- Are the authority limits clear?
- Is the business plan verified against the business transactions / operations on a regular basis?
- If the above conflicts with the actual operations, are the necessary procedures in place to ensure updating of the business plan with the relevant submission to the authorities?

In the case of card-based products for Electronic Funds Transfer, the application of the ACI product –Proactive Risk Manager is in place.

2.2. Assessing the Risk

- Assessing the likelihood of those threats occurring and the potential impact of them on the Company.
- All changes to the activities from both the original activities and from the original business plan are to be reviewed and graded.
- The assessment of risk should be completed independently from the Senior Management of the client companies.
- The current legislation and the adherence to the same will form part of the compliance risk. Any mitigating factors will be considered when reviewing the risk profile.
- The problem or opportunity may be able to generate alternative solutions – these should be considered when assessing the risk.
- The client product needs to be reviewed for changes over a period of time and how this impact (if at all) the risk profile of the client.

2.3. Mitigating the Risk

Mitigating the likelihood of occurrence of identified threats and the potential for damage to be caused, primarily through the application of appropriate and effective policies, procedures and controls.

Examples of mitigating measures:

- The application of additional elements of enhanced due diligence;

- The introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions;
- The limitation of business relationships or transactions with natural persons or legal entities from the countries identified as high risk countries.
-

2.4. Managing the Risk

Managing the residual risks arising from the threats, and vulnerabilities that the Company has been unable to mitigate. The risk assessment of Clients is conducted using the Compliance Due Diligence (CDD) Software, Cleversoft KYC. The Cleversoft KYC sums up all risk factors (each one has an assigned risk rate/score) in order to provide us with the final Client's risk rate / score and classification. For further information on the CDD Software, Cleversoft KYC, and risk rating, please refer to the "Cleversoft KYC Manual / User Guide".

2.5. Reviewing and Monitoring the Risk

- Reviewing and monitoring those risks to identify whether there have been any changes in the threats posed to the Company which necessitate changes to its policies, procedures and controls.
- Once the risk has been assessed, the inherent risks reviewed, the mitigating factors considered, the residual risk is then at hand. An action plan is put in place for execution under the supervision of compliance. The follow-up and review should be at regular intervals depending on the nature of the transactions or business under review. The monitoring reviews should be documented.
- The client along with the business manager need to closely manage the associated risks and should be encouraged to work within the guidelines proposed.

Aron Brokers Ltd Compliance and Risk Officer will ask the following questions:

- Is pattern detection in place?
- Are there periodic BRAs, clients risk assessments (CRAs), third-party reliance risk assessments, etc., reviews which may further implicate the risks of Aron Brokers Ltd? And If so, are those periodic reviews being completed and properly documented?

2.6. Advising on the Risk

Evaluating alternatives and selecting a solution may be done by ensuring the staff members put forward the problems:

- Persistently and in pursuit of common goals;
- With rational persuasion, a consultative approach, a positive exchange and in collaboration with the departments concerned;
- The staff members should be encouraged to refrain from legitimization, pressure, ingratiation and personal or emotional appeals.

Market Efficiency need to be assessed against Social Justice

- The DOCUMENTATION on the Risk advice needs to be comprehensive and more specifically documented WHY the risk profile has increased / decreased or requires reporting. Emails, operational and Board minutes as well as bank transfers and

statements may all be used in the documentation trail. Formal Board minutes are not the only method of documentation.

- A business Conduct Committee may be established depending on the volume of high risk clients identified and who should work within the Policy Documents provided.

Aron Brokers Ltd' Compliance Officer will ask the following questions:

- Have the high-risk client reports been delivered to the Board?
- Have appropriate steps been taken to minimize the risk for the client and for Aron Brokers Ltd?

2.7. Reporting the Risk

- If the risk needs to be reported to the Board, has this been done properly and documented after following the above steps?
- Have the appropriate corrective measures been taken to monitor and contain the risk?

3. Business Risk Assessment (BRA)

- The Business Risk Assessment considers the extent of the Company's exposure to risk.
- Identifying areas where the Company's services could be exposed to the risks of ML and TF, and taking appropriate steps to ensure that any identified risks are managed and mitigated, are crucial aspects of a risk-based approach.
- Section 17(2) of the FIAMLA requires businesses to assess 6 key areas when undertaking the BRA, amongst other risk factors:
    - The nature, scale and complexity of the Company's activities;
    - The products and services provided by the Company;
    - The persons to whom and the manner in which the products and services are provided;
    - The nature, scale, complexity and location of the client's activities;
    - Reliance on third parties for elements of the customer due diligence process; and
    - Technological developments and reliance on the same.
- The Company shall record and document its risk assessment in order to be able to demonstrate its basis. The assessment shall be regularly reviewed and amended to keep it up to date.
- The BRA Policy and the BRA Report are set to be reviewed annually as part of the Company's operations, or when changes within the Company, as well as changes in the respective Regulations and Acts take place. The same shall be included in the Board Report, so that evidence that an appropriate review has taken place.
- The BRA Policy and the BRA Report shall address and cover the following not only the inherent risks of the Company, but the residual risks after applying mitigating controls of the latter.

4. Customer Risk Assessment (CRA)

- The CRA must be conducted before establishing a business relationship or carrying out transactions with or for, the client. This will allow us to verify the risk of ML / TF regarding our clients, transactions, etc., beforehand.
- This Assessment needs to be documented in order to be able to demonstrate its basis.

This risk assessment will let us determine the following:

- The extent of identification information to be sought;
- Any additional information that needs to be requested;
- How that information will be verified;
- The extent to which the relationship will be monitored on an ongoing basis.

It should be noted that the FSC has no objection to a financial institution having higher risk clients, provided that they have been adequately risk assessed and any mitigating factors documented. When the client is assessed as presenting a higher risk, Enhanced Due Diligence must be obtained.

A basic Risk Assessment will consist of the following processes:

- Collecting information;
- Assessing and evaluating;
- Determining initial risk rating;
- Collecting additional information and documentation;
- Assessing and evaluating additional information and documentation;
- Confirming risk rating;
- Conducting on-going due diligence.

The Customer Risk Assessments (including Third-party Service Providers) frequency shall be as follows:

- At least once, annually for higher risk customers / entities (or those that make part of a group structure where any entity is rated high risk);
- At least every 2 years, for Medium risk customers / entities (or those that make part of a group structure where any entity is rated medium risk);
- At least every 3 years, for Low risk customers / entities (or those that make part of a group structure where any entity is rated low risk);
- At the point of a material change in customer's profiles or circumstances, for example,
- establishing connections with a higher risk jurisdiction or engaging in a higher risk business.

Risk Assessment Factors Taken into Consideration:

- The nature, scale, complexity and location of the client's activity;
- The services / products provided by the client, and to whom the same is provided to;
- The involvement of third-parties in the client's activity;
- Location - Individuals, business entities or organizations that are located in any country or territory or doing business with a country or territory that is featured from time to time

on any Sanctions Lists or the list of Business from Sensitive Sources will automatically be rated as high risk;

- Political exposure of the Beneficial Owner or Beneficiary of the Corporate Client (Legal Arrangement / Legal Body / Entity);
- Commercial rationale for the relationship;
- The nature and value of assets concerned in the relationship;
- The Client's Source of Funds and where necessary the source of wealth;
- Powers of Attorney;
- Bearer Shares;
- Status of Litigation - Although the Company anticipates that most client relationships will not be litigious, it recognises that where litigation is pending, threatened or current, additional management attention and focus is warranted. As such, higher risk scores are associated with these litigation categories;
- Investments - Types and Asset Value.

Risk Factors taken into consideration when identifying the level of TF risk associated with a country or territory included:

- Is there information (for example, from law enforcement or credible and reliable open media sources) suggesting that a country or territory provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory?
- Is the country or territory subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the UN or the EU?
- Risk factors that the Company can consider when identifying the risk associated with the level of predicate offences to ML in a country or territory include:
    - Is there information from credible and reliable public sources about the level of predicate offences to ML in the country or territory, for example, corruption, organized crime, tax crime and serious fraud? Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the UN Office on Drugs and Crime World Drug Report.
    - Is there information from more than one credible and reliable source about the capacity of the country's or the territory's investigative judicial system effectively to investigate and prosecute these offences?

PART III – CUSTOMER DUE DILIGENCE (CDD)

1. Identification and Verification

A key element of the prevention of money laundering and combating the financing of terrorism the capability of the Company to identify its customers, and their beneficial owners, and then verify their identities.

Aron Brokers Ltd undertakes the following CDD measures:

- Identifying and verifying the identity of each applicant for business;
- Identifying and verifying the identity of individuals connected to the account or transaction, such
- as the customer's beneficial owner(s);
- Identify all natural persons who ultimately have a controlling ownership interest in the customer.
- Where there is doubt as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control of the legal person through other means as may be specified by relevant regulatory body or supervisory authority; and
- Where no natural person is identified, the identity of the natural person who holds the position of senior managing official;
- Obtaining information on the purpose and intended nature of the business relationship (the inability for employees to understand the commercial rationale for business relationship may result in the failure to identity non-commercial and therefore potential money laundering and
- financing of terrorism activity);
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions throughout the course of that relationship, to ensure that the transactions in which the client is engaged are consistent with Aron Brokers Ltd' knowledge of the customer and its business and risk profile (including the source of funds);
- Achieving each of the above measures by using reliable, independently sourced documents, data or information (this is intended through the use of commercial databases and public information); and
- Ensuring that all material collected under the CDD process is kept relevant and up to date (for example undertaking reactive reviews in response to trigger events, and by undertaking regular planned reviews of existing records at intervals determined by risk rating, with higher risk customers warranting more frequent reviews);
- Determining whether the applicant for the business is acting on behalf of a third-party. If that's
- the case, the it must keep a record setting out the following:
    - The identity of the third-party (and any beneficial owners or associated persons as required);
    - The proofs of identity required under Regulation 3 of the FIAML Regulations 2018; and

    - The relationship between the third-party and the applicant for business.
- Where Aron Brokers Ltd is unable to determine whether the applicant is acting for a third-party or not, make a Suspicious Transaction Report (STR), pursuant to Section 14 of the FIAMLA to the Financial Intelligence Unit (FIU).

Any person, who knowingly provides any false or misleading information to a reporting person in connection with CDD requirements or any guidelines issued under the FIAMLA, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 500,000 rupees and to imprisonment for a term not exceeding 5 years.
In order to start a business relationship and conduct a thorough and successful due diligence check on clients, the appropriate KYC complete documentation needs to be filed and kept up to date.

Necessary KYC documentation / data for Natural Persons

- Data
    - Legal Name (the full legal and any other names, including, marital name, former legal name or alias);
    - Sex;
    - Date of birth;
    - Place of birth;
    - Nationality;
    - Current residential address (PO Box addresses are not acceptable);
    - Permanent residential address (if different than above);
    - Any public position held and, where appropriate, nature of employment and name of employer;
    - Government issued personal identification number or other government issued unique identifier;
    - Tax Identification Number (if applicable/available).
- Documentation
    - Current valid Passport / National Identity Card (the document must incorporate photographic evidence of identity); or
    - Current valid Driving Licence (where the financial Institute is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence – the document must incorporate photographic evidence of identity);
    - A recent (within the last 3 months) utility bill issued to the individual by name – as Proof of current or permanent residential address; or
    - A recent bank / credit card statement; or
    - A recent bank Reference.

Necessary KYB documentation / data for Private companies, Partnerships, Sociétés, Foundations, Trusts and other legal persons

- Data
    - Legal status of body;

  - Legal name of body;
  - Any trading names;
  - Nature of business;
  - Date and country of incorporation / registration;
  - Official identification number (e.g. company number);
  - Registered office address;
  - Mailing address (if different);
  - Principal place of business / operations (if different);
  - Ownership and control structure;
  - The identity of all the natural persons who ultimately have an ownership interest;
  - For trusts, the identity of the settlor, the trustee, the beneficiaries or class of beneficiaries, and where applicable, the protector or the enforcer, and any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership;
  - Bank Account details;
  - Tax Identification Number (if applicable/available).
- Documentation
  - Certificate of Incorporation (or other appropriate certificate of registration or licensing);
  - Memorandum and Articles of Association (or equivalent);
  - UBO & Shareholder registry (or equivalent);
  - Director Registry (or equivalent);
  - Latest Audited Financial Statements (if available);
  - Annual report or equivalent (if available);
  - Partnership deed or equivalent;
  - Trust Deed or equivalent instrument;
  - Charter of Foundation;
  - Acte de Société.

Provision for actions to be taken in the event of incomplete CDD:

- After verifying the identity of the client and if there is no adverse information regarding the same, additional KYC is requested from the client so that the registering process may be finalised.
- The Registering process may not be completed before the full KYC is provided.
- In the event the client does not provide all the necessary KYC there will not be a business relationship with the client, or the client account shall be disabled (for old / existing accounts) until the complete KYC set has been provided.

Provisions for actions to be taken in the event the Beneficial Owner (BO) cannot be identified, where the client is a Private company, Partnership, Société, Foundation, Trust and other legal persons

- In case the client is a legal person, Aron Brokers Ltd shall identify and take reasonable measures to verify the identity of the BOs by obtaining information on the following:
  - The identity of all the natural persons who ultimately have a controlling ownership interest in the legal person;

- Where there is doubt under the above paragraph (a), as to whether the person with the controlling ownership interest is a BO or where no natural person exerts control through ownership interests, the identity of the natural person exercising control of the legal person through other means as maybe specified by relevant regulatory body or supervisory authority; and
- Where no natural person is identified under subparagraph (a) and (b), the identity of the natural person who holds the position of Senior Managing Official;
- In case none of the above can be determined, the on-boarding process shall not take place.

1.1. Procedures for Certification KYC Documentation

Where Aron Brokers Ltd relies upon verification of identity documentation that is not in an original form, the documentation must be appropriately certified as true copies of the original

Documentation

Where an employee of Aron Brokers Ltd meets an applicant for business or the principals thereof face-to-face and has access to original verification of identity documentation, he or she may take copies of the verification of identity documentation and certify them personally as true copies of the original documentation. In other cases, copies of the verification of identity documentation can be certified by a suitable person, such as an attorney, a lawyer, a notary, an actuary, an accountant or any other person holding a recognised professional qualification, director or secretary of a regulated financial institution in Mauritius or meets the FATF's standards, a member of the judiciary or a senior civil servant.

The certifier should sign the copy document and clearly indicate the date of certification, his or her name, address and position or capacity on it together with contact details to facilitate tracing of the certifier and, where available, any registration number with any professional body.

The above list of suitable certifiers is not intended to be exhaustive and Aron Brokers Ltd should exercise due caution when considering certified copy documents, especially where such documents originate from a country perceived to represent a high risk or from unregulated entities in any jurisdiction.

Where certified copy documents are accepted, it is Aron Brokers Ltd' responsibility to ensure that the certifier is appropriate. In all cases, Aron Brokers Ltd should also ensure that the clients' signature on the identification document matches the signature on the application form, mandate or another document.

1.2. Procedures for Electronic Identification and Verification Reliance

Where Aron Brokers Ltd adopts a system providing for the electronic verification of natural person identity, Aron Brokers Ltd shall test the reliance and effectiveness of the results provided by the system in place and report its results to the Board as part of the Annual BRA Report. The system shall be tested periodically as per stated on Aron Brokers Ltd' BRA Policy.

Aron Brokers Ltd shall take into consideration any additional risks posed by placing reliance on an electronic method or system.

1.3. Procedures for the Acquisition of a Block of Clients or a Business

In the event that Aron Brokers Ltd takes on a business which has established business relationships or a block of clients, Aron Brokers Ltd shall undertake sufficient enquiries to determine:

- Whether the business's CDD policies, procedures, controls and systems are in line with current AML / CFT legislative requirements; and
- The level and the appropriateness (having regard to risk) of identification data held in relation to the clients and business relationships which are to be acquired.

In deciding whether to acquire the business, Aron Brokers Ltd may rely on the identification data held where:

- The business relationships were established in jurisdictions that have equivalent AML / CFT legislation or meets the FATF Standards;
- The business' CDD policies, procedures and controls are in line with the AML / CFT legislative framework; and
- Aron Brokers Ltd has obtained identification data for each client acquired.

2. Simplified CDD

2.1. Situations on which Simplified CDD can be applied

- Where the risk of Money Laundering (ML) or Financing of Terrorism (TF) is lower;
- Where information on the identity of the applicant for the business is publicly available; or
- Where adequate checks and controls exist elsewhere in the national systems;
- Where there is a low level of risk, it shall be ensured that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment carried out, whichever is most recently issued.

2.2. Situations on which Simplified CDD must not be applied

- Where the Company knows, suspects or has reasonable grounds for knowing or suspecting that a customer or applicant for a business is engaged in ML/TF; or
- Where Transactions being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in Money Laundering; or
- Where there are other indicators of ML/TF risk.

2.3. Important Aspects

- The Company must document the decision of adopting the Simplified measures inrespect of a customer or applicant for a business. This must be done in a manner which explains
- the factors which it took into account and its reasons for adopting the measures in question; and
- Keep the relationship with the customer or applicant under review, and operate appropriate policies, procedures and controls for doing so;
- The Company must keep the client risk assessment up to date and review the appropriateness of CDD obtained even if Simplified CDD measures are adopted.

3. Enhanced Due Diligence (EDD)

3.1. Where to perform EDD

- A higher risk of ML/TF has been identified;
- Where through supervisory guidance a high risk of ML/TF financing has been identified;
- Where a client or an applicant is from a high-risk third country;
- Where business relations, and transactions and persons established in jurisdictions that do not have adequate systems in place to combat ML/TF;
- Where the client or the applicant is a PEP (Political Exposed Person);
- Where the individual or entity is named on a Sanctions List;
- Where it has been determined that the client has provided false or stolen identification documentation or information, and the reporting person proposes to continue to deal with that customer;
- In the event of unusual or suspicious activity.

Aron Brokers Ltd implemented EDD procedures with respect to high-risk persons, business relations and transactions and persons established in jurisdictions that do not have adequate systems in place to combat ML and TF.

3.2. EDD measures that may apply for higher risk business relationships

- Requesting additional information on the client (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating on a frequent basis the identification data of the customer and or the beneficial owner;
- Obtaining additional information on the intended nature of the business relationship and the source of funds / wealth;
- Obtaining information on the intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship where the client or applicant is classified as high risk;
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
- Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards;
- Any other measures a financial institution may undertake with relation to a high risk relationship.

Important Aspects

- In case the reporting person is unable to perform EDD where required under Section 12 of the FIAML Regulations 2018, the business relationship shall be terminated andan STR shall be filed according to Section 14 of the FIAMLA;
- The reporting person shall include the beneficiary of a life insurance policy as a relevant risk factor when determining whether EDD measures are required;

- Where a reporting person determines that the beneficiary who is a legal person or a legal arrangement presents a higher risk, the reporting person shall take EDD measures which shall include reasonable measures to identify and verify the identity of the BO of the beneficiary at the time of payout;
- Aron Brokers Ltd must keep and maintain customer relationship information with respect to all its clients as detailed in the CDD measures listed above. This includes scrutinizing the source of funds and the source of wealth, as described below:
    - Source of Funds (SOF)
        - The source of funds refers to the origin of the particular funds or assets, which are the subject of the business relationship between the Company and its client and the transactions the Company is required to undertake on the client's behalf. The Source of funds requirement refers to where the funds are coming from in order to fund the relationship or transaction. This does not refer to every payment going through the account; however, the Company must ensure it complies with the ongoing monitoring provisions.
            - The Source of Funds shall be required as follows:
                - When a Client (Natural Person) reaches / exceeds the total Transaction Amount of USD 10,000.00.
                - When a Client (Corporate / Entity / Trust / Legal Body) exceeds the total Transaction Amount of USD 25,000.00.
    - Source of Wealth
        - The source of wealth on the other hand, describes the origins of a customer's financial standing or total net worth, i.e. activities which have generated a customer's funds and property. A financial institution is required to hold sufficient information to establish the source of wealth and this information must be obtained for all higher risk customers (including higher risk domestic PEPs) and all foreign PEPs and all other relationships where the type of product or service being offered makes it appropriate to do so because of its risk profile.
            - The Source of Wealth shall be required as follows:
                - When a Client (Natural Person) reaches / exceeds the total Transaction Amount of USD 15,000.00;
                - When a Client (Corporate / Entity / Trust / Legal Body) exceeds the total Transaction Amount of USD 25,000.00.

4. Politically Exposed Persons (PEPs)

PEPs are individuals who are or who have been entrusted with prominent public functions (e.g. Heads of State or of Government, Senior Politicians, Senior Government, Judicial or Military Officials, Senior Executive of State-owned Corporations and important Political Party Officials) in foreign, domestic and international organisation PEP, as well as family members and close associates of such person.

Business relationships with PEPs pose a greater than normal money laundering risk to financial institutions, by virtue of the possibility for them to have benefitted from proceeds of corruption,

as well as the potential for PEPs (due to their offices and connections) to conceal the proceeds of corruption or other crimes.

4.1. Procedures Applicable to Foreign PEPs 27

- Put in place and maintain appropriate risk management systems to determine whether the client or beneficial owner is a PEP;
- Obtain Senior Management / Board of Directors approval before establishing or continuing, for existing clients, such business relationships;
- In the event of existing clients, Board of Directors / Senior Management shall decide whether the existing business relationship has to be terminated or not, according to the risk classification and all different aspects surrounding the risk classification of the PEP Client;
- Obtain similar approval from senior management in cases of family members or close associates of PEPs;
- Take reasonable measures to establish the source of wealth and the source of funds of clients and beneficial owners identified as PEPs; and Conduct enhanced ongoing monitoring on that relationship.

4.2. Procedures Applicable to Domestic PEPs or an International Organisation PEP

- Take reasonable measures to determine whether a client or the beneficial owner is such a person; and
- In cases when there is higher risk business relationship with a domestic PEP, adopt the measures in paragraphs on Point “4.1.”.

Important Aspects

- A reporting person shall apply the relevant requirements of paragraphs “4.1 and 4.2” to family members or close associates of all types of PEP, as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.
- A reporting Person shall, in relation to life insurance policies, at any time but before the time of payout, take reasonable measures to determine whether the beneficiaries or the beneficial owner of the beneficiary, are PEPs, provided that where higher risks are identified, the reporting person shall:
    - Inform senior management before the payout processed;
    - Conduct enhanced scrutiny on the whole business relationship with the policyholder; and
    - Consider making a suspicious transaction report.

4.3. Defining “Family Members”

- It means an individual who is related to a PEP either directly through consanguinity, or through marriage or similar civil forms of partnership; and
- It includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

4.4. Defining “Close Associates”

- It means an individual who is closely connected to a PEP, either socially or professionally; and
- It includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

5. Third-Party Reliance

5.1. Risk Assessment on third-parties

- When reliance is placed on a third party to introduce business or to perform CDD measures, the following may be considered:
    - Consider how reliance on third parties is prompted and agreed on;
    - Consider who these third parties are, including any reputational issues, the quality ofrelationships with such third parties and previous experiences;
    - Consider the extent and type of any reliance placed or to be placed on third parties;
    - Consider the extent of the information being provided by the third party and who hasactually met the same face-to-face (chains of information);
    - Consider any jurisdictional issues in connection with reliance placed on third parties;
    - Consider the results of any testing undertaken on the third party's procedures and theresponses to any previous requests for documentation;
    - Consider the extent of any outsourcing undertaken;
    - Consider the quality of the provider for any outsourced functions including any reputational issues, previous experiences with the provider, the results of any audits, assessments or inspections where the material generated as a result of outsourcing has been reviewed.

5.2. Procedures to be satisfied regarding reliance on third-parties

- There must have a signed agreement between the fund or its administrator and the relevant third party, in which the third party consents to being relied upon for these purposes and undertakes;
- Where reliance is placed on a third party for elements of CDD, the Company must ensure that the identification information sought from the third party is adequate andaccurate;
- The CDD information has to be submitted immediately upon onboarding, although the

documents can be provided upon request at a later date;

- The third party will provide, immediately upon request, relevant copies of identification data in accordance with Regulation 21(2)(b) of the FIAML Regulations 2018; and
- The quality of the third party's CDD measures is such that it can be relied upon;
- Where such reliance is permitted, the ultimate responsibility for CDD measures will remain with the financial institutions relying on the third party;
- Reliance may only be placed on third parties to carry out CDD measures in relation to the identification and verification of a client's identity and the establishment of the purpose and intended nature of the business relationship;
- Reliance may be placed on a third party that is part of the same financial group, where:
    - The group applies CDD and record keeping requirements and programs against ML/TF;

    - The implementation of those CDD and record-keeping requirements and program against money laundering and terrorism financing is supervised at a group level by a competent authority; and
    - Any higher country risk is adequately mitigated by the group's policies to combat money laundering and terrorism financing.
- Third parties may not be relied upon to carry out the ongoing monitoring of dealings with a client, including identifying the source of wealth or source of funds;
- A financial institution may not rely on a third party based in a high risk country.

The FSC recommends that regular assurance testing is carried out in respect of the third party arrangements, to ensure that the CDD documents can be retrieved without undue delay and that the documentation received is sufficient pursuant to section 17(2)(v) of the FIAMLA.

5.3. Third-Party Introducers

- Financial institution should subject third-party introducers to the full identification and verification CDD measures for identification and verification as provided under the FIAML Regulations 2018.
- In line with the third-party reliance obligations, when individual applicants, or applicants which are body corporate, are introduced to a financial institution by an introducer, the Company should:
    - Obtain and maintain documentary evidence that the introducer is regulated for the purposes of preventing money laundering and terrorist financing; and
    - Be satisfied that the procedures laid down by the introducer meet the requirements specified in the FIAMLA and FIAML Regulations 2018.

The Company's Board of Directors or equivalent Senior Management will ensure that periodic testing of the above arrangements is conducted, in order to ensure compliance with the current legislative framework with respect to the above provision.

6. Targeted Financial Sanctions (TFS)

6.1. Screening

- Clients and transactions are screened against the required sanctions lists in 2 different ways:
    - Using an automated screening tool;
    - Manually – this is done by accessing the publicly available lists, which can be downloaded from the UN, FIU or the NSSEC websites.
- Documentation to evidence that clients and transactions have been screened has to be kept;
- The focus should not only be on the names of persons and entities listed on UN sanctions lists, but also identify the persons and entities linked to them;
- Each incoming and outgoing transaction should similarly be screened for a potential match with sanctions lists. Screening should be focused at a point in the transaction where detection of sanctions risk is actionable – where a transaction can be stopped and funds frozen if required – and before a potential violation occurs.

6.2. Matches and Escalation

- An alert that is generated by a potential match might not, on its own, be an indication of sanctions risk. It should act as a trigger which can be confirmed or discounted with additional information gained through further investigation. Adequate records of these investigations have to be maintained.
- Senior management should be alerted before action taken when identifying a true match and or freezing assets, where it is appropriate.
- In the event that a true match is identified, the match and any associated asset freezing should be reported immediately to the NSSEC and the FSC. (The reporting template on Positive Match needs to be filed as an Appendix)
- An STR should be also filed to the FIU.

6.3. Freezing and Prohibition on dealing with funds and Assets

- It is required to immediately and without delay freeze the assets of designated persons. In other words, this means ceasing any dealings and securing the funds and other assets, including financial assets and economic resources, that are owned or controlled, directly or indirectly, by the persons or entities designated by the UNSC or the NSSEC. This also encompasses the freezing of funds, other financial assets and economic resources of persons or entities acting on behalf of, or at the direction of, those designated by the UNSC or NSSEC.
- New freezes are required to be implemented immediately, and without prior notice to the person.
- The account of any designated person identified as an existing client must not be closed, as this could result in funds or economic resources being made available to the designated person.
- The obligation to report and freeze extends to attempted as well as future transactions. Where a transaction is attempted and monies or other assets have been passed to a Licensee with a view to completing the transaction, these monies or assets must not be handed back to the entity if the transaction is aborted following a match; and
- The obligation to freeze covers funds and other assets e.g. non-cash assets such as wills, real estate deeds, boats, jewellery, corporate licenses etc. However, where assets are frozen, there is a requirement to maintain the value of such an asset.

6.4. Unfreezing

Aron Brokers Ltd will be informed of a designation removal or unfreezing order in the same manner that they are informed of a new designation.

Important Aspects

- Financial sanctions apply to all clients and all transactions; there is no minimum financial limit.
- Politically Exposed Persons (PEPs) can be, but are not necessarily designated persons under targeted financial sanction regimes. The requirement to identify clients that are PEPs and the requirement to identify clients that are designated persons for targeted financial sanctions are separate obligations.

- The targeted financial sanctions regime is not the same as the FSC's enforcement regime, which sanctions Licensee's for non-compliance with their AML/CFT and targeted financial sanctions obligations.
- Freezing and unfreezing assets of designated persons shall take place within 24 Hours of identifying and verifying the related Sanctions, in line with Section 3 & 4 of the United Nations (Financial Prohibition, Arms Embargo and Travel Ban).

7. Ongoing Monitoring

An existing business relationship is required to be monitored so that money laundering or terrorist financing may be identified and prevented, and to ensure that it is consistent with the nature of business stated at the establishment of the relationship.

There are two types of ongoing monitoring:

- The first relates to the transactions and activity which occur on a day-to-day basis within business relationship and which need to be monitored to ensure they remain consistent with the Company's understanding of the client and the product or service it is providing to the client.
    - Scrutiny of transactions undertaken throughout the course of the relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with his knowledge of the client, and the business and risk profile of the client.
- The second relates to the clients themselves and the requirement for the Company to ensure that it continues to have a good understanding of its clients and their beneficial owners. This is achieved through maintaining relevant and appropriate CDD and applying appropriate ongoing screening.
    - Ensuring that documents data or information collected under the Customer Due Diligence (CDD) process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of clients.

Examples of the additional monitoring arrangements for high-risk relationships could include:

- Undertaking more frequent reviews of high risk relationships and updating CDD;
- Information on a more regular basis;
- Undertaking more regular reviews of transactions and activity against the profile and expected activity of the business relationship;
- Applying lower monetary thresholds for the monitoring of transactions and activity;
- Reviews being conducted by persons not directly involved in managing the relationship, for example, the CO;
- Ensuring that the Company has adequate MI systems to provide the board and CO with the timely information needed to identify, analyze and effectively monitor high-risk relationships and accounts;
- Appropriate approval procedures for high value transactions in respect of high risk relationships; and/or a greater understanding of the personal circumstances of high risk relationships, including an awareness of sources of third party information.

8. Transactions

Transactions include opening of an account, issuing an account number, renting safe deposit boxes or entering into a fiduciary relationship electronically or otherwise and it also includes a Proposed Transaction.

8.1. Transaction Verification

In order to verify a Transaction, the following data is required:

- Name of the Client / Entity;
- Address of Client / Entity;
- Name of Invoicing party;
- Company / Entity registration number;
- Bank Name;
- Bank Address;
- Bank account details.

The Principals of the Contracting parties

- Online searches using AML Manual specified websites, Consolidated United Nations Security Council Sanctions List (UN), European Union Consolidated List(EU), Higher Risk countries identified by FATF; Internet Explorer and Google website search.

8.2. Suspicious Transactions

- A suspicious transaction is a transaction where the laundering of money or the proceeds of any crime or funds linked to or related to or being used for terrorism or acts of terrorism by prescribed organizations, whether or not the funds represent the proceeds of a crime itself; and or
- The transaction is made in circumstances which are unusual or unjustifiably complex; have no economic justification or lawful objective; and or
- The Transactions are made by or on behalf of a person whose identify cannot be established to the satisfaction of the parties carrying out the instruction; and or gives rise to suspicion for any reason.

8.3. Suspicion

The transacting party may believe that a transaction is suspicious if the transaction involves:

- Laundering of money or proceeds of any crime; funds linked or related to terrorism or terrorist activities; unjustifiable complexity; unjustifiable economic or lawful objective; identity cannot be established or any other valid and justifiable reason;
- The Guidance Note 4 on Suspicious Transaction Report on 21 January 2014 (updated November 2020) to be read in conjunction with this document for relevance of specific examples of indicators of Suspicious Transactions;

Examples of Red Flag indicators of a Suspicious Transaction:

- Same day abnormal amount of deposits and withdrawals;
- Transaction does not match usual activity patterns or lacks economic substance;

- The Client is secretive or evasive about who they are, the reason for the Transaction or the source of funds.

9. Suspicious Transactions Report (STR)

- All staff members are required to submit an STR to the MLRO, when coming across a transaction, client or activity that they consider suspicious and after further examination of the same;
- The STR shall be passed from the CO to the MLRO, or from the staff member directly to the MLRO;
- The MLRO shall assess the information contained within the report to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to ML/TF or Proliferation Financing;
- The MLRO shall forthwith make a report to the FIU where there is reason to believe that an internal disclosure may be suspicious;
- An internal registry should be kept for STRs that have not been submitted to the FIU; and
- The internal registry should be updated in a monthly basis, regardless of any suspicious transactions, clients or activities have been flagged or a STR being submitted;
- An external registry should be kept for STRs that have been submitted to the FIU;
- A maximum delay of 5 working days is required for the reporting of the STR to the FIU, after the MLRO becomes aware of a suspicious transaction or activity;
- Where the reporting person becomes aware of a suspicious transaction, or ought reasonably to have become aware of a suspicious transaction, and he/she fails to make a report to FIU of such transaction not later than 5 working days after the suspicion arose he shall commit an offence and shall, on conviction, be liable to fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years;
- A STR can be submitted to the FIU electronically only from Banks as they are registered with the FIU. MC's are required to submit STR's manually;
- The STR Form is found under the Manual's Annexures. It needs to be completed manually and submitted by hand delivery at the reception of the FIU building at 7th Floor, Ebène Heights, 34, Ebène Cybercity, Ebène, Republic of Mauritius, or by facsimile at fax number +230 466 2431;
- The form proposed by the FIU is very complete and reporting parties are therefore required to complete the form as prescribed, both completely and with sufficient information so that the necessary follow-up and action can take place. The information should include WHO, WHAT, WHEN, WHERE, WHY. (Details thereto are found on the Guidance Notes from the FIU.) Late filings or incomplete filings negate the effectiveness of the law enforcement ability to determine what has transpired and what action is to be taken. To note the Entity Reference Number is key and will be referred to on all investigation and documentation relating to said STR. This ERN will be allocated by the FIU upon receipt and acceptance of the filed STR. The Indicator prompting the filing of the STR; the Description of the STR and the Material impact are all part of this form

which needs to be filled out prior to filing the STR. Transaction details for advice/guidance, please refer to the FIU Guidance Note 4.

9.1. Action to be taken

- Inform a law enforcement agency, or your supervisory body/ regulatory authority;
- Discontinue the business relationship with the client e.g. closed his/her account;
- Continue to monitor the clients account;
- Commence an internal investigation on the client's accounts/business;
- Any other steps taken in addition to reporting the suspicion to the FIU.

9.2. Further action to be taken or information to be supplied

- The Director of the FIU may ask for additional information and to note that no action can be taken against the party making the report. However, non-reporting incurs fines and criminal charges;
- The FIU operates in compliance with the Data Protection Act of 2004 but this Act has been superseded by the DPA of 2018. The Guidance notes should be updated shortly by the FIU and as such the STR procedures will be updated.

10. Tipping Off

Section 16(1) of the FIAMLA states that no person directly or indirectly involved in the reporting of a suspicious transaction shall inform any person involved in the transaction or an unauthorized third party that the transaction has been reported or that information has been supplied to the FIU pursuant to a request made under section 13(2) or (3) of the FIAMLA. The MLRO should acknowledge receipt of the internal disclosure and at the same time, provide a reminder of the obligation to do nothing that might prejudice enquiries, such as tipping off the customer or any other third party. The MLRO should provide guidance on how to avoid tipping off the customer if any disclosure is made. If the Company reasonably believes that performing the CDD process will tip off the customer or potential customer, it should stop the CDD process and will need to file a STR with the FIU in such circumstances.

In the event that the Company (Board of Directors/Senior Management) determine and decide that the Business Relationship with a Client whose STR has been filed should be terminated, the Company shall take into consideration the following points when interacting with the same client:

- It will become apparent to criminals that elements of their criminal activity is known to the Company, if it begins to ask probing questions regarding certain activities or if it seeks to terminate the relationship or decline entering into a business relationship without a meaningful pretext. The Company is therefore encouraged to carefully consider the wording of any statements made to customers explaining their decision; and
- The more information is included in the STR, the more valuable it will be to the FIU.

11. Loss of Contact with Client (PEP) or otherwise

There could be a situation when there are assets on a client's account but the contact with such client has been lost. The loss of contact with the client may occur when the client has either

deceased and not left any alternate contacts; has moved physical address for personal or business reasons and purposely does leave either forwarding contact details or any means of further contact or simply has been negligent in keeping up to date on his affairs. The Client should have already been classified one of low, medium or high risk.
In the event the Client is of low or medium risk it is possible that there is no contact with the client within an 11-month period.

In the event the Client is of High risk or a Politically Exposed Person, there should be regular contact throughout the year and review of the file because of the nature of the client. If the Client is not responding to regular contact methods, the following steps should be taken by the Compliance Officer.

- The client shall be contacted via telephone and email. The documentation advising the client of the proceedings of the Company, including fees and other responsibilities may be delivered by the local office to the physical address of the client if known;
- Although the client may persist in not responding to any of the contact made, a continued annual contact is to be made until such stage as the Company itself is wound up or the Board takes alternative action;
- Should the client be unreachable within a period of one year, the FSC will be informed accordingly;

The Board is to review on an annual basis all Client files where the client is no longer responding to any contact and may take further action on the Client as is deemed appropriate taking into account the Business Risk to the Company.

12. Examples of Documentary Evidence to be collected to evidence Source of Wealth

12.1. Sales of Securities or other Investment

- Investment/savings certificates, contract notes or statements;
- Written confirmation from the relevant investment company on letter headed paper
- Bank statement showing receipt of funds from investment company name; or 35
- Signed letter detailing funds from a warranted accountant on letter headed paper.

12.2. Sale of Property

- Signed letter from a lawyer or a notary on a letter headed paper; or
- Contract of Sale.

12.3. Maturing Investment or Policy Claim

- Letter from previous investment company on letter headed paper notifying proceeds of claim;
- Chargeable Event Certificate; or
- Closing statement.

12.4. Individual owns policy/company pays premium

- A copy of trading details or an annual report from the company's website (if applicable)
- Hard copy of the latest annual report; or
- Copy of the company's certificate of incorporation (or equivalent); and
- Policy statement; or
- Bank statement showing credit.

12.5. Dividends or profits from private company

- Dividend contract note;
- Letter showing dividend details signed by a warranted accountant on letter headed paper
- Set of company accounts showing the dividends details; or
- Bank statement clearly showing receipt of funds and the name of the company paying dividend; and
- A document providing proof of shareholding such as a copy of the Memo & Arts, Certificate of Incumbency or a dated print-out of a company registry search.

12.6. Company Sale

- Signed letter from a lawyer on a letter headed paper;
- Signed letter from a warranted accountant on a letter headed paper;
- Copy of contract of sale and bank statement showing credit to account consequent to the sale; or
- Copies of media coverage (where applicable) as supporting evidence.

12.7. Inheritance

- A copy of the will that must include the value of the estate; or
- A lawyer or notary's letter on letter headed paper or a letter from the trustees of an estate that includes the type of asset and respective value.

12.8. Maturity or redemption or a shareholder's loan

- Loan agreement;
- Recent loan statements.

12.9. Gift

Document (e.g. letter from the donor) showing who gave the gift, when, the relationship between the donor and done and (if possible and applicable) why the donation was made, together with the verification of identity of the donor, and information about the source of the donor's wealth.

12.10. Lottery/betting/casino win

- Letter from relevant organization (lottery, headquarters/betting shop/casino);
- A certificate of winnings issued by the relevant company or casino;
- In the case of lottery winnings, a bank statement showing funds deposited by company name; or

- Copies of media coverage (if applicable) as supporting evidence.

12.11. Compensation payment (this could be a decision or award by a court, Tribunal or arbiter or else and out-of-court settlement)

- A letter/court order from a compensating body clearly showing the amount of compensation; or
- Lawyer's letter on letter headed paper clearly establishing the amount.

12.12. Savings and investment

- Bank Statement/s demonstrating deposit/gifted monies; or
- Documentation evidencing an inward transfer from portfolio.

12.13. Insurance claims

- A letter from the insurance provider on a letter headed paper.

12.14. Divorce or separation settlement

- A copy of the court order or judicial separation agreement and verification that funds have originated from the account of the former spouse.

12.15. Income from employment (including bonus)

- An original or certified copy of a recent pay slip;
- Written confirmation of annual salary/bonus amounts signed by employer; or
- Bank statement clearly showing receipt for most recent regular salary payment from named employer.

12.16. Retirement Income

- Pension Statement;
- Letter from a warranted accountant on letter headed paper;
- Letter from annuity provider; or
- Bank statement showing receipt of latest pension income and name of provider.

12.17. Other Monies:

- Appropriate supporting documentation; or
- Signed letter detailing funds from warranted accountant/lawyer/entity licensed to provide investment services on letter headed paper.

ADDITIONAL MANUALS THAT FORM PART OF THE COMPANY'S POLICY DOCUMENTS

The following manuals, Policies and appendices should be read in conjunction with this AML / CFT / GRC Operations Manual:

- Business Risk Assessment Policy;
- Cleversoft KYC User Guide;
- Internal Policy;

- Disaster Recovery Plan Policy and Procedure;
- Human Resources Manual;
- Privacy Policy;
- Compliant Handling Policy & Processing;
- PEP Register.