Enjoy Optimal Trading with us.

OPTIM INVESTMENTS

OPTIM Investments

ANTI MONEY LAUNDERING AND KNOW YOUR CLIENT PROCEDURES MANUAL (Internal)

Updated: 12 October 2020

The following company officers and representatives have reviewed and signed this policy as adopted and approved for use by OPTIM Investments Limited.

Approved by (Signature)	Name	Position	Date
	Kevin Rawoteea	MLRO/Compliance Officer	
	Christopher R Milinazzo	CEO/Director	

CONTENTS

Forward: This Procedures Manual sets out the control standards and procedures that exist at OPTIM Investments Limited (the "Company" or the "Firm") in relation to AML and KYC policies and procedures. The overall aim is to provide a comprehensive analysis of the policies and procedures applied clients and processes within the company to halt money laundering and terrorist financing.

1. PURPOSE

The purpose of this Anti Money Laundering and Know Your Client Procedures Manual (the "Manual" or "Procedures Manual") is to provide the principles and procedures of the overall approach in place at OPTIM Investments Limited (the "Company") in relation to the prevention and suppression of money laundering and terrorist financing and implementation of a risk based approach in identifying clients, their sources of funds and client classification for the purpose of minimizing operational and reputation risks and to achieve full compliance with the relevant anti money laundering laws and regulations.

In addition, this AML/KYC Manual is intended to:

- Bring awareness to the Company's personnel of their reporting and other obligations in relation to activities which raise suspicions of money laundering activity and/or financing of terrorism;
- Prescribe the role of the Money Laundering Reporting Officer ("**MLRO**") and his/her obligation to report suspicious activity to the Financial Intelligence Unit of Mauritius ("**FIU**").

This document applies to all the Company's personnel and should be read in conjunction with other related policies. Where any provisions are in conflict, this document should take precedence. It is clarified that this document is not intended to cover all eventualities and all circumstances that may be encountered on a day to day basis. Where such circumstances arise, input from the MLRO shall be provided as appropriate.

Through the following Guidelines, the Company stands committed to:

a. Accept those clients whose identity is established by conducting due diligence appropriate to the risk profile of the clients.

b. Record and preserve the activities conducted by clients to facilitate investigation.

c. Report to regulatory authorities in Mauritius, or any other country as required, the details of activities of all or selected clients if and when requested or at regular frequency as may be suggested by such authorities; and

d. Cooperate with investigative agencies / law enforcement agencies in their efforts to trace the money laundering activities and persons involved in such activities.

e. Educate and train partners and staff to recognize and report suspicions of money laundering.

2. LEGAL FRAMEWORK

Investment dealers are required to comply with the provisions of the Financial Intelligence and Anti-Money Laundering Act 2002, the Prevention of Corruption Act 2002, the Prevention of Terrorism Act 2002 (collectively, the "**Law**") and the relevant circulars and rules of the Financial Intelligence Unit and the Financial Services Commission (the "**Commission**") of Mauritius, as may be amended from time to time, including the Code on the Prevention of Money Laundering and Terrorist Financing of the Commission issued on 30 March 2012 (the "**Code**").

In accordance with the Law, investment dealer firms are obliged to set out policies and procedures for preventing money laundering activities. Those procedures, which are implemented by the Company, as these are requested by the Law, are the following:

i. Identification and due diligence procedures of clients through the implementation of a risk-based approach.
ii. Record keeping procedures in relation to clients' identity and their transactions.
iii. Internal reporting procedures to a competent person (e.g. the MLRO) appointed to receive and consider information that give rise to knowledge or suspicion that a client is engaged in money laundering activities.
iv. Appropriate procedures of internal control, risk management, with the purpose of preventing money laundering activities.
v. The examination of transactions that due to their nature are considered vulnerable to money laundering, and especially for complicated or unusually large transactions and transactions that are taken place without an obvious financial or legal purpose.
vi. Measures for making employees aware of the above-mentioned procedures to prevent money laundering and of the legislation relating to money laundering.
vii. Provision of regular training to employees in the recognition and handling of transactions suspected to be associated with money laundering.

In addition, in accordance with the Law, the MLRO shall prepare a risk management and procedures manual regarding money laundering and terrorist financing. In this respect this Manual has been prepared by the MLRO and has been approved by the Board of Directors of the Company.

3. ROLES AND RESPONSIBILITIES

The Company must ensure that the management body defines, oversees and is accountable for the implementation of governance arrangements that ensure effective and prudent management of the firm.

3.1 Board of Directors Obligations

The Board's overriding principle is that the Company should be compliant with the applicable AML legislation. As part of the overall responsibility, the Board of Directors' obligations in relation to this Manual have been set as follows:

a. To determine, record and approve the general policy principles of the Company in relation to the prevention of money laundering and terrorist financing and communicate them to the MLRO.

b. To appoint a compliance officer and, where necessary, assistant compliance officers and determine their duties and responsibilities, which are recorded in the relevant section of this Procedures Manual.

c. To approve this Manual, which is communicated to all employees of the Company that manage, monitor or control in any way the customers' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined.

d. To ensure that all requirements of the Law are applied, and that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement.

e. To assure that the MLRO and their assistants (if any) and any other person who has been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, have complete and timely access to all data and information concerning customers' identity, transactions' documents and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties.

f. To ensure that all employees are aware of the person who has been assigned with the duties of the MLRO, as well as his assistants, to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing.

g. To establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the MLRO, either directly or through their assistant.

h. To ensure that the compliance officer has sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties.

i. To assess and approve the Annual Report of the MLRO and to take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report.

j. To communicate to the MLRO the AML related guidelines.

k. To review and approve the AML Training plan which is submitted by the MLRO.

3.2 MLRO's Obligations

3.2.1 General duties of the MLRO

The Money Laundering Reporting Officer's obligations are as follows:

a. To design the internal practice, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing and to describe and allocate the appropriateness and the limits of responsibility of each department that is involved.

b. To develop and establish the customers' acceptance policy and to submit it to the Board of Directors for consideration and approval.

c. To prepare a risk management and procedures manual regarding money laundering and terrorist financing.

d. To monitor and assess the correct and effective implementation of this Procedures Manual.

e. To receive information from the employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information is received through the "Internal Suspicion Report" which is included as **Appendix 1** of this Manual.

f. To evaluate and examine the information received as per point (e). The evaluation of the information is done in the form of a report, referred as "Internal Evaluation Report". An example is included as **Appendix 2** of this Manual however, the MLRO may use a different form as they deem appropriate.

g. To timely notify FIU of any suspicions of money laundering or terrorism financing in accordance with the requirements of the Code.

h. To provide guidance to the employees on subjects related to Money Laundering and terrorist financing.

i. To prepare and submit to the Commission the reports for the prevention of money laundering and terrorist financing.

j. To prepare the MLRO's annual report.

k. To maintain a registry which includes the reports of points (e), (f) and (g), and relevant statistical information (department that submitted the internal report, date of submission to the compliance officer, date of assessment, date of reporting to FIU), the evaluation reports of point (d) and all the documents that verify the accomplishment of his duties specified in the present subparagraph.

l. To maintain a list of clients who are categorized following a risk-based approach, which contains, *inter alia*, the names of clients, their account number and the date of the commencement of the business relationship. Moreover, the MLRO ensures the updating of the said lists with all new or existing clients, in the light of additional information obtained.

m. To review, on an annual basis, the appropriateness of policies and procedures, given new clients, geographical areas of operations, new financial instruments etc. and to implement corrections. Particular attention is given to electronic/internet trading and telephone orders.

n. To submit the findings and observations, in a written report form, to the board of directors which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected.

o. To evaluate the systems and procedures applied by a third person on whom the Company relies for client identification and due diligence procedures and to approve the cooperation with it.

p. To assess the training need of the Company's departments and employees. The MLRO prepares and applies annual staff training program and then records the seminars/training courses attended by each employee.

q. To reply to all requests and queries from FIU and the Commission;

3.2.2 Annual report of the MLRO

The Annual MLRO's Report ("**AML Report**") is prepared by the MLRO and submitted to the Board for discussion and approval, at the latest by end of February following the year under review. After its approval, the AML Report and the minutes of the Board meeting shall be recorded in the Company's record and shall remain available submitted for examination by the Commission and the FIU for at least 7 years.

The content of the AML Report s shall include at a minimum the following:

a. Information about measures undertaken and/or procedures introduced by the Company for compliance with any amendments and/or new provisions of the Law and the Code:

- Reference to changes or upcoming changes (if already known) of the regulatory framework regarding the prevention of money laundering and terrorist financing, such as the Law, the Code and the relevant circulars and guidance's of the Commission and the FIU.
- Reference to relevant data, information, reports from international organisations (FATF, Moneyval, IMF etc.)
- Specific measures and procedures taken/adopted concerning the above.
- Suggestions for further measures and implementation of further procedures in the case of any weaknesses or deficiencies in relation to points i and ii above, setting a timeframe for implementation.

b. Information on the reviews performed by the MLRO during the year, reporting material weaknesses and deficiencies identified in the policy, practises, measures, procedures and controls that the Company applies for the prevention of money laundering and terrorist financing. In this respect, the report outlines the seriousness of the deficiencies and/or weaknesses identified, the risk implications and actions taken and/or recommendations made for rectifying the situation.

c. Specific reference to the content and the method/way of conduct of the inspections and reviews, regarding, at least, **the following sectors:**

- Completeness of this Procedures Manual;
- Implementation of customers' acceptance policy;
- Constructions and content of economic profile;

- Identification of suspicious transactions, internal suspicion reporting and external reporting to FIU.
- Simplified customer identification and due diligence procedures of low risk customers.
- Customer identification and due diligence measures of normal risk customers.
- Enhanced customer identification and due diligence procedures of high-risk customers.
- Timing of customers' identification.
- Reliance on third parties for customer identification and due diligence purposes.
- Ongoing monitoring of customers' accounts and transactions.
- Record keeping.
- Implementation of measures and procedures on a risk-based approach.
- Implementation of the financial sanctions imposed by the United Nations, USA, the European Union and the Government of Mauritius.
- Education and training of staff.

d. The number of internal suspicion reports submitted to the MLRO by the Company's employees and possible comments/observations thereon, **including the following details:**

- Number of Internal Suspicion Reports submitted by the employees of the Company to the Compliance Officer and comparative data with the previous year;
- Number of Internal Suspicion Reports that have not been notified to FIU and comparative data with the previous year; and
- Circumstances that led to the increase/decrease of Internal Suspicion Reports and significant trends observed.

e. The number of reports submitted by the MLRO to FIU with information/details on the main reasons for suspicion and highlights of any particular trends, including the following details:

- Information on cases related to money laundering and terrorist financing for which no report was made.
- Number of Compliance Officer's Reports to FIU, comparative data with the previous year, summary of data/information for the main reasons of the suspicion and significant trends observed.
- Feedback from FIU regarding the submitted Reports, if any.

f. Summary figures, on an annualized basis, of clients' total cash deposits in currencies in excess of the set limit of USD$12,500 (MUR500,000) (together with comparative figures of the previous year) as reported in the Monthly Prevention Statement. Any comments on material changes observed compared with the previous year are also reported, **including the following details:**

- Reference on an annual basis of customers' total cash deposits, in currencies in excess of the set limit of USD$12,500 (MUR500,000) and comparative data with the previous year.

- Circumstances that led to the increase of customers' cash deposits and significant trends observed.

- Reference in the measures and actions of the Company regarding cash deposits by customers (e.g. method/way of identification and investigation, recording the investigation in the customer's file, result of the investigation and possible actions taken).

- Recommendations for further actions and implementation of further procedures in case of deficiencies and weaknesses in relation to point above, setting a timeframe for implementation.

g. Information, details or observations regarding the communication with the employees on money laundering and terrorist financing preventive issues.

h. Information on the policy, measures, practices, procedures and controls applied by the Company in relation to high risk clients as well as number and country of origin of high risk clients with whom a business relationship is established or an occasional transaction has been **executed:**

- Information on the policy, measures, practices, procedures and controls applied by the Company in relation to high risk customers;

- Number, country of origin and type of high-risk customers with whom a business relationship is established or an occasional transaction has been executed and comparative data with the previous year.

i. Information about systems and procedures applied by the Company for the ongoing monitoring of client accounts and transactions.

- Analysis of the way/method (automated or non-automated) of the ongoing monitoring of customers' accounts and transactions.

- Details for any variation of the ongoing monitoring of customers' accounts transactions according to the customer's categorization on a risk-based approach.

- Details of the timing of the ongoing monitoring of customers' accounts and transactions (e.g. in real time or after the completion of an event).

- Details of the way/method of documenting the ongoing monitoring of customers' accounts and transactions.

j. Information on training courses attended by the MLRO and any other educational material received.

k. Information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants. The following specific details shall be **provided:**

- Reference to specific issues/cases, questions/clarifications and any other form of communication with the staff and the specific results that have arisen from the relevant communication.

- Information on training courses/seminars attended by the MLRO and the rest of the staff of the Company during the year **and** courses/seminars planned for the next year, **including:**

  - ✓ Summarized data of the program/content of the training courses/seminars.

  - ✓ Number and duration of the training courses/seminars.

  - ✓ Number and position of the employees participating in the training courses/seminars.

  - ✓ Number and position of employees who did not participate in the training courses/seminars and their duties are relevant with the prevention of money laundering and terrorist financing. Information on the reasons for not participating.

  - ✓ Instructors' names and qualifications.

  - ✓ Whether the training courses/seminars were performed in-house or by an external organization or consultants.

  - ✓ Information for the educational material received.

l. Results of the assessment of the adequacy and effectiveness of staff training.

m. Information on the recommended next year's training program.

n. Information on the structure and staffing of the department of the MLRO as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

3.2.3 Monthly Prevention Statement

The Monthly Prevention Statement includes details for the total cash deposits over USD$12,500 (MUR500,000) or equivalent amount in other currency accepted by the Company in any individual client account, the Internal Suspicious Activity/ Transactions Report and the MLRO's reports to FIU. The completion of the said report offers the opportunity to evaluate and reinforce the Company's systems of controls and monitor the Company's operations in respect of early identification and detection of cash transactions which increase the risk of money laundering and terrorist financing activities taking place.

The completion and preparation of the Monthly Prevention Statement is within the duties of the MLRO.

3.2.4 Right of Access

The MLRO, as well as any members of the MLRO team that they may designate, shall have through relevant organizational arrangements, full and prompt access to all client data, including indicatively data on clients' identities and clients' transactions.

The MLRO has a professional obligation to report, directly to the Board of Directors, any incidents where their work was interrupted and/or inhibited by any person within the internal organization of the Company.

3.3 Duties of MLRO

The MLRO reviews and assesses on a 6 months' basis the AML and KYC procedures that are followed by the Company. In addition, the MLRO approves any changes that may occur in the AML policies of the Company and this Procedures Manual.

3.4 Duties of the Company's Employees

The Company expects from its employees to perform the following:

i. Conduct business in accordance with applicable anti-money laundering laws, corporate policies, and the highest ethical standards;

ii. Do not provide advice or other assistance to persons who attempt to violate or avoid anti-money laundering laws or corporate policies;

iii. Consider the MLRO's approval or rejection of any disputable transaction as final and binding;

iv. Fully execute their obligations against the Law to disclose any suspicions about a transaction that might be related to money laundering and terrorist financing;

v. Adequately record and retain details of all transactions undertaken with or for third parties, including payments and receipts of funds, as well as all dealings in financial instruments. At all times the policy for third party deposits must be adhered to;

vi. Not to notify the clients of their suspicion or the fact that an employee has made a report. It is a criminal offence in the Republic of Mauritius to inform a person who is known or suspected to be engaged in money laundering that they have been reported or may be under investigation;

vii. In the case the employee begins to suspect that a money laundering activity is taking place, even if he has already assisted the suspected launderer, he must immediately report the matter to the MLRO. The communication to the MLRO should be in the form of a written report referred to as an 'Internal Suspicion Report' (see Appendix 1 of this Policy). Failure to do so may constitute a criminal offence in the Republic of Mauritius. The MLRO will advise on how to proceed in subsequent dealings with the client.

The Company's employees failing to fulfil their obligations and to adhere the provisions of present AML/KYC Procedures Manual shall face internal disciplinary actions, as these may be decided by their direct supervisor, the MLRO and the CEO of the Company, including termination of their employment agreement.

3.5 Reporting Lines

The following reporting lines have been set by the Company:

1. MLRO reports to the Senior Management and members of the Board;
2. Assistants of the MLRO shall report to the MLRO;
3. Employees of Customer Support/Back Office/Finance report to the MLRO where needed.

4. CLIENT ACCEPTANCE POLICY

4.1 Risk Based Approach in client verification

The Company applies appropriate measures and procedures, on a risk-based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher. A risk-based approach is adopted by the Company during the verification of the clients' identity, the collection of information for the construction of their economic profile and monitoring of their transactions and activities. Taking into consideration the assessed risk, the Company determines the type and extent of measures it adopts, to manage and mitigate the identified risks.

Client acceptance procedure is prepared following detailed assessment of the risks faced by the Company from its clients and/or their transactions and/or their countries of origin or operations and/or any other factors the Company may identify as significant from time from time. The Company identifies its clients prior or during to commencing a business relationship and demonstrates that the KYC process has been completed in line with the AML legislation prior or during to commencing such relationship.

In particular, due diligence procedures are applied in the following cases:

a. When establishing a business relationship;

b. When carrying out one-off transactions amounting to USD$12,500 (MUR500,000) or equivalent in other currencies or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

c. When there is a suspicion of money laundering or terrorist financing, irrespective of the amount of the transaction.

d. When there are doubts about the veracity or adequacy of previously obtained client identification data.

The Company conducts the verification of the identity of the customer and the beneficial owner during the establishment of the business relationship since this is necessary in order not to interrupt the normal conduct of business when the money laundering and terrorist financing risk is low. The verification of clients' information is made in two ways: via the submission of documents or electronically.

4.2 Timing of Client Identification

The Company performs identification of the client prior the establishment of the business relationship and proceeds with verification of the potential client's identity prior or during the establishment of a business relationship if not to interrupt the normal conduct of business and where there is limited risk of money laundering or terrorist financing occurring. In case of the latter, the due diligence procedure shall be completed as soon as practicable after the initial contact. The said procedure is further elaborated below. Where the risk of money laundering and terrorist financing cannot be determined as low the CDD must be completed prior the establishment of a business relationship. Each account holder is required to complete the customer due diligence (CDD) procedure by submitting the relevant KYC documentation or pass electronic verification.

4.3 Client Acceptance Policy and Risk Classification

The establishment of a business relationship is considered by the Company to commence upon the client being marked as "Compliant" in the Company's Customer Relationship Management system, and/or when the client is able to trade on a real account with own funds, in which case the person, natural or legal, is considered to be accepted by the Company as a client.

The client acceptance policy is determined and implemented under particular criteria related to the client's risk profile. In particular, the factors that specify the risk category of a client are the following:

i. Type of client (natural or legal person);

ii. Nature of business;

iii. Country of domiciliation/ residency, especially if from high risk countries or from countries known for high level of corruption or organized crime or drug trafficking;

iv. Information used to construct the economic profile;

v. Amount of deposited funds (for subsequent re-classification after acceptance);

vi. Trading Activity (for subsequent re-classification after acceptance);

vii. Potential involvement of politically exposed persons ('PEPs'); and

viii. Willingness to provide documentation.

During the on-boarding process, upon the client completing the registration process (in the case of natural persons- online completion, in the case of legal persons-completion of hard-copy), an account is created and allocated to the client. The AML risk classification is also assigned to the client at this point following the construction of the client's economic profile.

Despite proper completion of the account registration by a potential client, they shall not be considered as accepted until verification of the due diligence process, following which the client will be permitted to commence trading. It is noted that the client will **not** be able to use the deposited funds until they have provided the necessary supportive information/documentation for the Company and comply with the Company's policies for verification of the ownership of the payment method.

Based on the aforementioned and given the nature of the Company's business being conducted through its online trading websites rather than physical interaction, most of the clients of the Company are considered non-face-to-face, therefore by default are categorized as High Risk clients. Enhanced customer identification and due diligence measures are in place in order to effectively mitigate the risks associated with such business relationships as prescribed below.

The main client types and the indicative AML risk status assigned to each type are outlined in the table below. It is clarified that it is in the discretion of the MLRO to reclassify a client to a higher or lower risk category where there are circumstances, he/she deems appropriate justifying such reclassification.

Risk classification is as prescribed below:

	Client Type	**AML Risk Category**
1	Credit or financial institutions regulated in EU or EU equivalent jurisdictions, in the USA or in Mauritius, acting as principals	Low Risk
2	Public companies listed in EU markets or EU equivalent jurisdictions, in the USA or in Mauritius	Low Risk
3	Domestic public authorities in EU, USA or Mauritius	Low Risk
4	Credit or financial institutions regulated outside of jurisdictions specified in point (1) above, acting as principals	Medium Risk
5	Public companies listed in jurisdictions other than those specified in point (2) above	Medium Risk
6	Unregulated private companies irrespective of jurisdiction	High Risk
7	Private companies owned by PEPs	High Risk
8	Companies whose shares are in bearer form	High Risk
9	Trusts	High Risk
10	'Client accounts' in the name of a third person	High Risk

11	**Non face to face Individuals/ Natural persons**	**High Risk**
12	Politically Exposed Persons	High Risk
13	**Customer offering electronic gambling/gaming through the internet**	High Risk
14	Customers from countries which inadequately apply Financial Action Task Force's recommendations.	High Risk

The Company may at any given time, and following consultation with the MLRO decide not to accept specific types of natural or legal persons as clients. The Company as at the date of this policy does not accept the following types:

1. Client accounts in the name of a third person
2. Companies whose shares are in bearer form
3. Customers from countries which inadequately apply Financial Action Task Force's recommendations
4. Trusts

All clients on boarded through non face to face interaction are classified as High Risk. Given the nature of the Company's activities where all clients are non-face to face, registering on the Company's trading platforms, the Company has proceeded to introduce three subcategories within the High-Risk classification. This enables the Company to deploy its AML efforts on a more granular risk-based approach. These three subcategories in the High-Risk classification are as follows:

- High-High Risk Client
- High-Medium Risk Client
- High-Low Risk Client

Legal entities and Joint accounts are considered by the Company of higher risk and are therefore, classified as of High-Medium risk. PEPs are considered of higher risk and are classified as High-High.

Following an assessment of the customer's profile following initial registration, based on the customer's risk-scoring and subsequent monitoring, reclassification may follow and a client may be subjected to additional requirements in accordance to the risk-based approach followed by the Company.

As mentioned above, the client's AML risk classification is always assigned prior to the commencement of the business relationship as part of the client's Compliance approval process and is recorded in the Company's CRM system.

4.4 Acceptance of deposits and Trading

4.4.1 Trading during the establishment of a business relationship

The Company only enables a client to trade during the establishment of the business relationship when the customer is deemed as being of low risk of money laundering and terrorism financing and provides full KYC within 14 days and further subject to a maximum cumulative deposit limit of USD$12,500 (MUR500,000) or equivalent in other currencies. This applies only for clients who do not provide proof of residence (POR). Clients who are unable to provide a proof of identity (POI) are not onboarded. It is noted that for practical implementation purposes the Company considers the 14 days to commence from the date of the first deposit, since customers deposit almost immediately or within a couple of days from registration. The Company does not expect that the 14-day procedure applies to the majority of its clients and therefore, clients are only permitted to trade upon satisfying the established due diligence requirements.

The above mentioned 14 days procedure is implemented in practice by the Company **as follows:**

a. A client registers for the establishment of a trading account with the Company during which, the potential client is requested to provide the Company with all necessary information required by the Company for establishing the economic profile and assessing the potential client's appropriateness. At the same time the Company identifies its potential client by receipt of the potential client's name, address, email and telephone number, among other information.

b. The client may proceed with a deposit to fund the trading platform of a maximum of USD$12,500 (MUR500,000).

c. The funds are not credited to the potential client's account held by the Company and **cannot be used for trading**, unless the client has provided the Company with a POI and has received a clean World Check result in order to be classified as low risk for money laundering and terrorist financing.

d. Upon classification of low risk for money laundering and terrorist financing purposes, a notice is sent to the client informing them that:

    i. The client is given 14 days from the date of deposit to complete the due diligence procedure by providing a POR and any other pending documentation as requested by the Company;

    ii. During this period, and prior completing the full customer due diligence, the client may not exceed the total deposit of USD$12,500 (MUR500,000) or equivalent in other currency. Any deposits received exceeding this amount will be returned to the client immediately as per the procedure indicated below for deposits exceeding USD$12,500 (MUR500,000) or equivalent in other currency prior completion of the due diligence;

iii. In case the due diligence procedures are not satisfied and/or in case 14 days have passed (from the date of deposit) then the balance in the account, including profits and losses, will be returned to the client to the same source from which they were transferred from. Any open positions will be closed on the last available price upon the end of the designated period;

iv. In case the due diligence procedures are satisfied the client may continue trading and any limitations placed to the account (e.g. amount of deposits) are lifted.

The maximum amount of deposit a potential client may make **prior** to the establishment of the business relationship and before CDD procedure is completed is USD$12,500 (MUR500,000) or equivalent in other currency (in aggregate). In case the client has made a deposit of more than USD$12,500 (MUR500,000) or equivalent in other currency and therefore, cannot qualify as a low risk client, the Company must immediately proceed with a return of the funds and not permit the client to trade prior completion of the due diligence. The funds shall be returned to the same source they were transferred from. For procedural reasons, the return will be made during 24 hours from the deposit date. During that period the customer may proceed with complying with the Company's due diligence requirements in order to avoid the return of the funds. In such case, and upon the client successfully meeting the Company's due diligence requirements, the Company may accept the client and permit the client to start trading. The above also, applies in case of excess of the amount of USD$12,500 (MUR500,000) or equivalent in other currency, as per paragraph 4.4.1(d)(ii) above.

The above procedure must be documented in the Company's Client Agreement acknowledged and accepted by the potential client during account registration. To this extent, the Company determines that a business relationship with the potential client is only deemed to have been established for the purposes of the AML law once the due diligence procedures have been fully satisfied.

4.4.2 Demo/Practice accounts trading

In the case of practice/demo accounts, the Company permits trading without requesting the demo client to complete the CDD process, since such accounts do not carry any risk of money laundering as the trading is on a virtual environment with virtual funds. Trading on demo accounts enables a client and/or potential client to familiarize himself with a near-real trading environment. Nonetheless, when a client proceeds with the transfer from a demo to a real trading account, the Company must complete CDD measures as these are analyzed below.

4.4.3 Trading on real platform with virtual funds (e.g. bonus)

In addition to the above, the Company may also permit trading on the real platform in situations where the client and/or potential client has not completed the CDD and made (or not made) a deposit but he is using funds credited by the Company as a bonus and/or award prior to the client making any deposits. Such funds in the aforementioned situation are considered as **virtual** which the client may not withdraw regardless of volume prior to the completion of the CDD procedure (i.e. submission of full KYC documents). The aforementioned scenario may also give the tools to a client to acquire sufficient knowledge and experience in a real platform under real market conditions without facing the risk of loss of funds and does not involve any risks of money laundering. In this situation, the client is not able to trade with real funds to the real trading platform prior to completing the CDD procedure.

5. INABILITY TO COMPLETE CDD

It should be clear that in situations where an account has been created but problems of verification arise during the course of the establishment of the relationship that cannot be resolved (such as provision of fake documents, identification of minor customers, etc.), the Company closes or blocks access to the account.

Clients are given 14 days from the day of receipt of the deposit to complete the CDD procedure. In case where a client /potential client is unable to comply with the CDD requirements and/or has not been deemed as low risk in order to be able to trade during the establishment of the business relationship, the Company shall take one of the following measures, on a case by case basis:

i. Not proceed with the establishment of the business relationship;
ii. Not proceed with execution of requested transaction by the client;
iii. The Company must:

- Return the funds as part of the termination process and close the account. In this case, the relationship is to be considered void and the funds have to be returned to a bank account in the name of the depositor; and
- Where the Company is unable to return the funds to its source of deposit, it must retain the funds in a separate bank account until the client completes the CDD procedure to the
- Company's satisfaction in order to be able to withdraw the funds. Such deposits must be reported to the MLRO to assess whether it is justified under the circumstances to submit a report to FIU, in which case the Company must retain the funds until consent has been given by FIU in returning the funds to the source they came from.

6. SIMPLIFIED CLIENT DUE DILIGENCE – LOW RISK CLIENTS

Simplified procedures apply for low risk clients as depicted in the table 1 above. The following types of clients are considered lower risk:

a. Credit or financial institutions regulated in the member states of the European Union, United States of America or Mauritius.
b. Credit or financial institutions situated in a third country which imposes requirements equivalent to those laid down by the European Union (the "EU equivalent jurisdictions") and are under supervision for compliance with those requirements.
c. Listed companies whose securities are admitted to trading on a regulated market in the member states of the European Union, United States of America or Mauritius.
d. Domestic public authorities in the member states of the European Union, United States of America or Mauritius.

The Company may apply simplified due diligence, and therefore, not apply the following client identification and due diligence measures in respect to the Low Risk Clients:

a. identifying the client and verifying the client's identity on the basis of documents, data or information obtained from a reliable and independent source;

b. identifying the beneficial owner and taking risk-based and adequate measures to verify the identity on the basis of documents, data or information obtained from a reliable and independent source so that the person carrying on in financial or other business knows who the beneficial owner is; as regards legal persons, trusts and similar legal arrangements, taking risk based and adequate measures to understand the ownership and control structure of the client;

c. obtaining information on the purpose and intended nature of the business relationship;

d. conducting on-going monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the person engaged in financial or other business in relation to the client, the business and risk profile, including where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

e. the verification of the identity of the client and the beneficial owner is performed before the establishment of a business relationship or the carrying out of the transaction.

With reference to the above it is also clarified that EU equivalent jurisdictions are those third countries outside EU jurisdictions which impose procedures and take measures for preventing money laundering and terrorist financing equivalent to those laid down by the European Directive 2005/60/EC and as such are considered to be of low AML risk. Such countries are specified in **Appendix 3.**

It should be noted that the Company gathers sufficient information to establish if the client qualifies to be classified as lower risk client.

The Company does not apply simplified due diligence where, despite the client falling in one of the above categories, there is a risk of money laundering activity.

Where the Company applies simplified due diligence measures it requires the collection of the following documents:

i. Proof of regulated status e.g. copy of the license
ii. Certificate of incorporation
iii. Proof of Identity and Proof of residence below from the authorized person(s) to operate the account
iv. Latest Audited Financial Statements (where applicable)

The entities need to complete the Company's "Account opening form" and World Check is performed for all "natural" persons involved.

7. ENHANCED CLIENT DUE DILIGENCE – HIGH RISK CLIENTS

Due to the fact that the vast majority of the Company's clients are non-face-to-face clients, they are by default categorized as High Risk. For ascertaining the true identity of such customers, the Company obtains the following information:

i. True name as stated on the official identity card or passport;
ii. Full residential address, including postal code;
iii. Telephone;
iv. Email address;
v. Date of birth;
vi. Nationality; and
vii. Details of profession and other occupations of the customer.

The Company takes additional measures when conducting client due diligence in cases where there is elevated higher risk of money laundering and the client is considered as High Risk by:

- Performing searches on the database of World Check – to identify sanctioned individuals or entities as well as verifying passport authenticity. In particular, all potential clients need to be screened against international databased through World Check to identify potential matches.

- Assessing whether the type of the natural or legal person falls under one of the high-risk categories as described above.

Specifically, the Company requests for the following documents during the on-boarding procedure to verify the above information of the client and performs the following actions:

i. a valid proof of identity; the Company requests for international passports; where the potential client is unable to provide with a passport the Company may collect a national ID or driver's license. The potential client is advised to provide the Company with an international passport as soon as practicable;

ii. recent proof of residence, in the form of a utility bill, local tax authority bill or a bank statement (not older than 6 months);

iii. Completes satisfactorily the financial information section in the account registration on the basis of which the client's economic profile is constructed;

iv. Checks such clients against World Check or equivalent online AML databases to identify validity of passport and validity of economic profile provided on the account opening portal, PEP status, involvement in any illegal activities, inclusion in any sanctions lists, etc. Performing a WC is very important for the compliance procedure. The compliance status of an account **cannot** be changed without performing a WC on a customer's profile and there are no results that match or are possible matches to our customer's profile; and

v. Requires that deposits to the client's account are always from a source in the name of the client which is not subject to any international sanctions and withdrawals are always to the source from where the deposit was received. In case where this is not possible (e.g. credit card refund is not possible because a year since deposit has passed) withdrawals may be executed to a source on the name of the client.

8. STANDARD CLIENT DUE DILIGENCE-MEDIUM RISK CLIENTS

The Company considers as Medium Risk those clients who do not fall under the Low or High Risk categories. The client types falling under the Medium Risk category are shown in the table above.

The due diligence procedures the Company applies on all medium risk clients in order to compensate for the elevated risk versus the low risk clients include the following:

a. Ensuring that the client's identity is established by additional documents, data or information.
b. Verifying or certifying the documents supplied, or requiring confirmatory certification by 3rd party independent sources.
c. Checks all Medium risk clients against "World-check" database and internet search engines to identify validity of passport, PEP status, involvement in any illegal activities, inclusion in any sanctions lists, etc.
d. Conducting enhanced and continuous monitoring of the business relationship.

9. APPROVAL OF CLIENTS

The approval of clients is performed by the Company's verification department and monitored by the MLRO and relevant records/statements are properly recorded online in the Company's system. Corporate accounts and joint accounts can only be established and confirmed as compliant following the approval of the MLRO.

10. CLIENT'S ECONOMIC PROFILE

The client's economic profile is constructed, initially, through completion of the account opening portal data fields. Subsequently, and subject to its risk-based approach the Company may request additional information should it consider that clarifications are required for a better understanding of the client's profile. The Company may also require the updating of the economic profile as part of its reviews on high risk clients. The Company requires the construction of the economic profile of all its clients irrespective of risk categorization exceeding the requirements of the Law.

The economic profile questions include the following:

a. The anticipated account turnover

b. Nature of transactions

c. Expected origin of incoming funds to be credited in the account

d. The customer's size of wealth

e. Industry/Source of funds

f. Origin of funds

It is noted that for legal persons the data and information that are used for the construction of clients' economic profile include, inter alia, the name of the company, the country of its incorporation, the head offices address, the names and the identification information of the beneficial owners, directors and authorized signatories, financial information, ownership structure of the group that the company may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information).

The said data and information are recorded electronically in a separate section designed for this purpose which is retained in the customer's file in the Company's clients' database along with all other documents. The said form is updated whenever new information emerges that needs to be added to the economic profile of the customer or alters existing information that makes up the economic profile of the customer.

The Company has the right not to proceed with the establishment of a business relationship or execution of an occasional transaction or can terminate a business relationship with a prospective client in case the client fails or refuses to submit the requested information for the verification of his identity and the creation of his economic profile.

The information as regards the economic profile of the client is reviewed by the MLRO as part of the client ongoing review process and is used as reference when comparing client account activity with the client's representations.

11. CLIENT IDENTIFICATION-ADDITIONAL GUIDANCE

11.1 Identification of Ultimate Beneficial Owners (UBOs)

UBO of corporate clients are identified through either of the following:

i. In cases of clients whose shareholders are nominees, the Company requires the Nominee agreement/ Declaration of Trust from such Nominee shareholder.
ii. In cases of clients whose shareholders are other legal entities, the following UBO identification documentation is required:

- Full legalization documents of the ultimate legal entity which exercises actual control or, in the case of many ultimate legal entity shareholders, of those legal entities that exercise such control. Full legalization documents proving shareholder details of intermediary holding companies are also required;

- In case of complex legal structure, the Company may request from the prospective client a legal structure (chart or table) showing the full ownership chain (including all intermediate entities) between our Client/ Counterparty and the Ultimate Beneficial Owner(s);

11.2 Politically Exposed Persons (PEP)

Establishing business relationship with persons who have important public position or political office or their immediate family members or persons known to be their close associates entails additional risks that the Company is not willing to accept. Accordingly, it is the Company's policy not to accept PEPs as its clients.

Checks must be performed in relation to the potential client in World Search database in order to identify if the respective potential client is considered a PEP or is included in any sanctions list.

The meaning of PEP includes the following natural persons who are or have been entrusted with prominent public functions whether in Mauritius or in a foreign country:

i. Heads of state, heads of government, ministers and deputy or assistant ministers;

ii. Members of parliaments;

iii. Members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

iv. Members of courts of auditors or of the boards of central banks;

v. Ambassadors and high-ranking officers in the armed forces; and

vi. Members of the administrative, management or supervisory bodies of State-owned enterprises.

Note: None of the above shall be understood as covering middle ranking or more junior officials.

Immediate family members include the following:

i. spouse or the person with which cohabit for at least one year;

ii. children and their spouses or the persons with which cohabit for at least one year; and

iii. parents.

Persons known to be close associates includes the following:

i. Any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements or any other close business relations with a person defined as a PEP

ii. Any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of a PEP.

Existing clients

When the business relationship has already been established with a customer (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then the Company shall proceed with immediate termination of the Client Agreement with such client in accordance with the guidance to that effect that shall be provided by the Legal Department.

11.3 Joint accounts

In case of joint accounts, the identity of all individuals that hold or have the right to manage the account are verified in accordance to the requirements for natural persons prescribed in this policy. Joint Accounts are considered of higher risk by the Company and further information and documentation may be requested where the Company deems appropriate.

All requested information must be provided to the Company prior the creation of the joint account. Joint Account Application Form (Appendix 5) must be duly signed by the clients and match the details provided in Personal Details documentation. In the Joint Account Application Form the clients must agree to be jointly and severally responsible for the Account and must acknowledge that they have read and understood the Company's terms and conditions.

11.4 Anonymous or Numbered accounts

The Company does not establish anonymous or numbered accounts. Additionally, the Company pays special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favor anonymity and takes measures to prevent their use for money laundering or terrorist financing purposes.

11.5 Non-acceptable clients

The Company does not approve the establishment of a business relationship with natural or legal persons engaged in illegal activities such as arms dealing and drug trafficking.

In order for the Company to assess whether to accept or reject a client, it also takes into consideration factors such as the client's background, type and nature of its business activities, its country of origin, the anticipated level and nature of trading activity as well as the source and origin of funds.

In addition, the clients who are residents of a restricted jurisdiction are not accepted by the Company. All the high-risk countries in accordance to the FATF recommendations are indicated as restricted jurisdictions in the Company's website www.optimfx.com terms and conditions from which the Company does not accept clients. The list may be amended from time to time depending to the updates from the FATF. The list of banned countries may be found in Appendix 6.

11.6 Lead and Practice Account

Lead is a registration created in the Company's CRM system when the customer is only registered at the website without completing the full account registration procedure. The potential client at this stage cannot deposit nor trade and is not yet considered a Company's client.

Practice account is a demonstration (demo) account which the customer registers for and provides a risk-free account that simulates real trading conditions which is active for the period of 30days. Since both, lead and practice accounts, are not real accounts the Company does not obtain and complete the KYC verification process.

11.7 Deceased client

In cases of deceased clients, the following procedures shall be followed:

i. In case of **active bank account on the name of the deceased**: The inheritors should provide **death certificate**, a **Certificate of Inheritance** and **POI** of the Inheritor. Afterwards a withdrawal request form should be submitted. The Company shall transfer the money to the bank account of the deceased client.

ii. In case of **no active bank account**, the funds can be withdrawn to a bank account owned by an inheritor or a notary. The Company shall require:

- Death certificate;
- certificate of Inheritance;
- POI of all Inheritors;
- Notarized document, showing that all the inheritors agreed the money from the Company to be paid to a specific bank account owned by one of the inheritors or by the Notary;

If one of the inheritors is underage, a certificate showing who is the guardian and the POI of the guardian together with the POI of the underage (if the under aged person has an ID) shall be collected.

11.8 Under age clients

The Company does not accept minors, i.e. person below the age of 18, as clients. In case an underage person signs up electronically for the creation of an account by providing the Company with false and/or fake details, the Company, as soon as it becomes aware of this, must terminate and/or close immediately the account of the underage person.

To that respect, the underage person, as a person not entitled to enter into any contracts and/or engagements under the law, is perceived as not having a business relationship with the Company. Upon the Company receiving knowledge as to the person being an underage, the Company informs them through email and/or phone call, that the Company is unable to accept them as clients since they do not match the Company's profile and that any money deposited in their trading account will be refunded to them in the same way a deposit was made.

Should it be impossible for the Company to refund the underage person in the same way the deposit was made, then the underage person needs to provide the Company, following a request, with a bank account to which they are the beneficial owners. In case, the underage person does not have a bank account to which they are a beneficial owner, the underage person's parent and/or legal guardian has to be contacted.

The parent and/or legal guardian has to provide the Company with the following:

i. POI;
ii. Official documentation proving the relationship between the underage person and the parent and/or legal guardian such as a birth certificate; and
iii. Bank account to which the parent and/or legal guardian is a beneficial owner

As soon as the Company receives the documents from the underage person's parent and/or legal guardian and the underage person confirms return of the money to the parent's and/or legal guardian's bank account, the Company proceeds with refunding the money deposited by the underage person to the parent's and/or legal guardian's bank account.
Should the customer wish to open an account following turning 18 years old, a new account must be created.

11.9 Reliance on third parties for KYC identification

Recognizing that the ultimate responsibility for client identification is with it, it is the Company's policy not to rely on third parties for KYC identification, where third party means credit/ financial institutions, auditors, legal professionals, trust and corporate services providers.

12. DOCUMENTATION

12.1 Documentation standards

The Company, given the nature of its business collects copies of the documents provided by the customers.

However, in cases the MLRO may deem appropriate due to the increased risk, identification documentation needs to be in their original or in certified true copy form. Certified true copy means that the person certifying the copy of the document had seen of the original document and is in a position to certify that the copy is a true and complete copy of the original document.

Client identification documentation obtained at the account opening stage or during ongoing client account/documentation reviews should be recent (where applicable) and always up-to-date. Documents relating to the verification of the client's permanent address and bank references are considered as recent when submitted to the Company within 6 months from the issue date. Detailed information regarding the specific documentation collected depending on the type of the potential client is indicated in **Appendix 7**.

12.2 Supporting documentation:

A. Proof of ID can be demonstrated through any of the following documents**: Passport, national identification card (ID card), or driver's license.**

Valid POI must fulfil the following criteria:

- **Full Name** – same as in the CRM. In case it differs, it needs to be verified over the phone;
- **Date of Birth** – same as in the CRM. In case it differs, it needs to be verified over the phone;

- **Expiration Date** – must be valid. If the POI expires in less than a month, it cannot be accepted and client should be requested to send another POI;
- **Picture** should be **clear** enough;
- **All** the **details** on the POI must be clearly **visible.**

The Company as a default requests from potential clients to provide the Company with a copy of their international passport. Where this is not available, potential clients may provide the Company with a copy of their ID card or driver's license but must provide the Company with a copy of their passport once available.

B. Proof of address can be demonstrated through any of the following documents: Utility Bill (internet, television, water, electricity, phone or gas), bank or credit card statement, local tax authority bill or an equivalent document.

Valid POR must fulfil the following criteria:

- **Full Name** – same as in the identification document;
- **Address** – same as the residence address in the CRM. In case the address is different, we need address verification over the phone**;**
- **Issued date** – **not older than 6 months**. Any POR older than 6 months will not be accepted;
- **Official POR** with **Logo** and/or **stamp**

The following documents **cannot be accepted** as POR**:**

- SWIFT;
- Wire Transfer Document in hand writing;
- Courier Bill;
- Other document in hand writing unless it is a government issued doc with stamp and signature;
- Editable WORD documents.

In derogation from the above and where the client is unable to provide a POR in the prescribed methods indicated above, the Company may accept a document produced, signed and stamped by the municipality verifying the clients' or potential clients' residency.

12.3 Document verification

Depending on the type of document takes the necessary steps to confirm the authenticity of documents and information provided by potential clients as follows:

i. For verification of the authenticity of the document of the potential client's Proof of Identity the following are used:

a. Check how the actual document looks like, by checking evidence of watermarks and security elements via the following websites or google:

   1. http://www.documentchecker.com/ (Keesing)
   2. http://www.consilium.europa.eu/prado/en/search-by-documentcountry.html

b. Run a World Check on the Machine-Readable Zone (MRZ) line of an identity card or passport in order to determine authenticity (where applicable).

c. Confirm validity of the MRZ (Machine Readable Zone) line via Keesing

d. Where applicable and/or possible, check in governmental websites in terms of the document's authenticity

e. Where possible, proceed with Google/Facebook search on the name/email of the potential client, to identify real pictures matching the one on the proof of identity.

ii. For verification of the authenticity of a Proof of residence the following are used:

a. Perform a Google search on the issuing company of the proof of residence.

b. Run a google street view where possible

c. Run a Facebook search

12.4 Reliable/ independent authenticators for document certifications

Reliable authenticators are authenticators from which the Company will accept document certifications as true copies:

- A Regulated Financial Institution from an EU, USA, Mauritius or EU equivalent jurisdiction provided the authenticator is of a relevant position (director, management, compliance, legal, secretariat, operations);
- A licensed lawyer, auditor, fiduciary services provider, fund administrator, notary public, from an EU, US, Mauritius or EU equivalent jurisdiction;
- The Embassy or Consulate of the client's home country;
- The Embassy of Mauritius in the client's home country;
- A Company Registrar in an EU, US, Mauritius or EU equivalent jurisdiction;
- Any full-time employee of the Company;
- The national courts.

12.5 Language of documentation

The Company may receive documents from customers in any language. Where the documents are in a language other than French or English, a true translation is required. Translations may be performed by employees of the Company who fluent are in the English or French language. The name and capacity/position of the person translating the document as well as the date of the translation, shall be recorded in the CRM system.

13. ELECTRONIC VERIFICATIONS

13.1 Performance of electronic verification – Selection of data provider

The Company may verify its clients' information electronically, through third party data providers. The Company must ensure that the following criteria are met by the third-party data provider:

i. The electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information (at least customer's full name, address and date of birth) and negative information (e.g. committing of offences such as identity theft, including in deceased person records, inclusion in sanctions and restrictive measures' list by the Council of the EU and UN Security Council);

ii. The electronic databases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alters;

iii. The information and search are saved in the Company's records and the result in relation to identity verification can be tracked.

Prior use of any third party for the purposes of EV, the MLRO runs the necessary checks as these are mentioned above including a check on the reliability and validity of the data sources from which the information is derived. A list with the data sources is kept by the MLRO in the Company's records including as assessment of the check performed by the MLRO towards the approval of the use of the third-party provider.

13.2 Procedure for EV

It is to be noted that any third parties engaged for electronic verification purposes are subject to prior enhanced due diligence to ensure that they are fit and proper to offer such services to the Company and have the right credentials, expertise and track record in such electronic verification services. The assessment is done by the MLRO.

In order for a client to be verified electronically, information must come from two or more electronic sources. The procedure satisfies the following correlation standard:

a. Identification of the customer's full name and current address from our source, and

b. Identification of the customer's full name and either his current address of date of birth from a second source

14. AML/KYC MONITORING PROCEDURES

14.1 Updating clients' files

The Company is required to carry out on-going monitoring of the business relationships established with clients. On-going monitoring is performed by the Company in order to ensure that the account activity is in line with the information that the Company obtained for the construction of client's economic profile and in order to identify any suspicious transactions. As part of monitoring procedures, the Company is further under an obligation to request to update the documents kept for due diligence purposes.

The Company ensures that the information and documentation obtained for the client identification and for the construction of his economic profile remains updated through the business relationship.

In case the Company becomes aware that important information pertaining to a client has changed, it requests the relevant details from the client. Important information among others includes:

a. A significant transaction takes place which appears to be unusual and/or significant compared to the normal pattern of the transactions and the economic profile of the client;

b. A material change in the way and the rules the client's account operates such as change of the persons that are authorised to operate the account;

c. In the case of a corporate client, a material change in the clients' legal status and situation such as:

- Change of directors/secretary,
- Change of registered shareholders and/or beneficial owners,
- Change of registered office,
- Change of trustees,
- Change of trading and/or corporate name,
- Change of the principal trading partners and/or undertake new major business activities.

The review and request for update of client information depends on the client's risk classification. In particular, the Company proceeds with the review and update of information as follows:

- **High High-risk clients:** review of files/refresh of information is carried out at least once a year or where transaction or other work requires otherwise;
- **High Medium-risk clients:** review of files/refresh of information is carried out at least once every two years or where a transaction or other work requires otherwise;

- **High Low risk-clients:** review of files/refresh of information is carried out at least once every three years or where a transaction or other work requires otherwise.

In the event which any of the KYC documentation is no longer valid, the clients shall receive automatic system notifications informing them of the upcoming expiration of their submitted documentation requesting the submission of new up-to-date documentation.
It is clarified that in order to make best use of the Company's resources, only active clients (non-dormant) are reviewed (i.e. clients who had trading activity in the last 90 days). In case of no activity the client is disabled from further trading. Further information on the handling of inactive and dormant accounts can be found below.

14.2 Outdated documentation and/or incomplete economic profile

For those clients who refuse to provide the Company with updated KYC documentation upon request and/or which have not provided material information for the establishment of their economic profile, particularly for the verification of their source of funds, the Company shall proceed as follows:

Phase A:
Clients who will not provide the Company with updated data/documentation required for their identification and verification and/or material information for the completion of a client's economic profile (including information required for verifying a client's source of funds requested on a risk based approach) are segregated from the normal pool of clients and are placed in a specific status in the Company's CRM system, namely "Compliance Suspended" with ground "Expired/Outdated documentation". Accordingly, those clients' ability to deposit or trade will be disabled.

Phase B:
Upon those clients being placed in the specific status, the clients will be given 3 months to revert with the requested information/documentation. Following the end of the 3 months period the legal relationship between the Company and the Client will be terminated. It is noted that during those 3 months the following will apply:

a. During the 3 months, clients will not be permitted to trade or make any deposits;

b. Clients will be able to close their existing open positions by contacting dealing desk or through the platform;

c. Clients receive numerous reminders for the submission of the pending information/data with explanation on the consequences in case they do not revert within the indicated timeframe;

d. Clients are able to request termination of the business relationship with the Company and receipt of the remaining balance of their account without the need to provide the pending information/data. At this point the Company will investigate whether there are any grounds to raise suspicion and accordingly make a report to FIU.

During the 3 months, once a client submits the pending information/documentation, and upon confirmation of the adequacy of the information/documentation, the client will be enabled to continue his engagement with the Company as normal and the account will be reactivated for trading. Upon the end of the 3 months the Company will:

a. Inform the client of the termination of the business relationship (including legal agreement) with the Company;

b. Close any pending open positions (if any);

c. Return to the client any remaining balance of the account (including profits or losses);

d. The MLRO may consider reporting non complying clients to FIU in case there are reasonable grounds to suspect that such clients relate to money laundering and terrorist financing activities.

14.3 Ongoing monitoring of clients' trading activity

The Company is required to carry out on-going monitoring of the business relationships established with clients. On-going monitoring is performed by the Company in order to ensure that the account activity is in line with the clients' economic profile and in order to identify any suspicious transactions.

The procedures and frequency of monitoring of clients' trading activity is risk based. In this respect, the Company monitors high risk material clients with particular emphasis to those with high trading volumes, high deposit and withdrawals volumes. The monitoring exercise involves comparing the client account turnover against anticipated figures based on the clients' economic profile as set out at the onboarding stage. Material variances, from expected levels of trading, together with particularly complex, suspicious or highly unusual transactions and deposits/ withdrawals without any apparent economic reason are investigated by the Company. A more detailed list with examples of suspicious transactions can be found below (Appendix 9).

The procedure followed for the monitoring of client's transactions are analyzed below:

1. Monthly review of the top 15 depositors per month;

2. Sample check of 50 clients per quarter;

3. Monitoring of credit card deposits and identification of suspicious activity.

4. Monitoring of transactions shall be focused, indicatively, on the following key indicator scenarios:

a. **Scenario 1:** High deposits and no activity for 30 days. The scenario generates an alert when a customer makes a high deposit (minimum USD$12,500 (MUR500,000)) and has no activity for the following 30 days

b. **Scenario 2:** Unusual trading activity during 30 days: the scenario is examining unusual trading behavior in a period of 30 days comparing to the average of the same customer's activity during the last 6 months.

c. **Scenario 3:** Unusual trading behavior comparing to peer group activity: this scenario compares trading activity of customers with the same characteristics.

5. All deposits and withdrawals equal or exceeding USD$12,500 (MUR500,000) must be reported to the MLRO for review.

6. **Risk-based ongoing monitoring of source of funds/wealth information based on deposit thresholds and client's AML risk categorisation**. A significant factor when monitoring client accounts is considered by the Company to be the level of deposit made by each client. Clients with higher deposits are considered to pose higher risk to the Company and to this extent should be more closely monitored. The new procedure applied requires clients to submit additional information for the establishment of their source of funds on a risk-based approach, when clients meet certain deposit thresholds or in case of activity mismatch. The deposit thresholds vary depending on the client's AML risk classification i.e. the higher the AML risk classification is, the lower is the deposit threshold for the ongoing monitoring. More information is presented in **Appendix 10**.

Upon performing any of the aforementioned checks, and upon receipt and review of clients' additional documentation/information, where needed, the findings shall be summarised in a single note in the Company's "Monitoring list" where all the checks performed per client are summarised.

14.4 Dormant/Inactive Accounts

As per the Company's terms and conditions, any trading account held with the Company where the client has not:

a. Placed a trade;

b. Opened or closed a positions; and/or

c. Made a deposit into the account,

for a period of 90 days (3 months) and more, is considered by the Company as Inactive Account ("**Inactive Account**"). Inactive Accounts that do not hold any balance are considered by the Company as Dormant ("**Dormant Accounts**").

Clients which have been inactive for more than one year shall be turned to status "Compliance Suspended". Accordingly, clients will be requested to submit updated KYC documentation, when they wish to activate an Inactive Account which has been inactive for one year or more.

14.5 Funds transfers (Deposits and Withdrawals)

14.5.1 Payment methods

Recognizing the AML risks associated with 3rd party funds transfers and considering the risks associated with its clients being non-face to face the Company decided to prohibit fully any 3rd party deposits and 3rd party withdrawals.

Specifically, the Company requires that deposits to the client's account are always from a payment method in the name of the client and withdrawals are always to the same source from where the deposit was received.

14.5.2 Deposits from Joint bank accounts

When the Company receives a deposit from a Joint Bank Account, the following documents shall be collected by the Company:

a. Proof of Identity (POI) of both parties;
b. Perform World Check and Panama Papers checks for both parties;
c. POI of the third party must contain a signature;
d. Joint Bank Account Declaration Form completed by the third party (**Appendix 8**).

Upon receipt of the Joint Bank Account Declaration Form the Company must ensure that the form is signed by the third party by comparing the signature of the form with the signature on the third party's POI.

14.5.3 Withdrawals

Withdrawals are permitted following the submission of a withdrawal request by the customer through the relevant procedure indicated on the Company's websites. Withdrawals as a default are performed to the same source as the deposit was made. Should the initial bank account or other payment method (e.g. client's credit card has expired) be no longer available for withdrawal the Company will proceed with a withdrawal to a bank account in the name of the client, which the client shall indicate. The client will need to provide proof of the unavailability of the initial deposit method. Withdrawals to third parties are as a default not permitted and may be only performed in exceptional cases, following senior management approval, further to assessment of the reason for the request and the situation.

14.5.4 Cash Transactions

In a further effort to eliminate AML risks the Company **does not accept** cash deposits or withdrawals in any form.

Restrictions on incoming and outgoing payments

Further to sanctions imposed by international bodies such as OFAC, the Company does not accept any incoming funds and does not perform any outgoing payments to the following countries:

1. Iran
2. North Korea
3. Syria
4. Iraq
5. Myanmar (Burma)

To this extent, safeguards are in place with the Company's processor and banks to prevent deposits from the specific jurisdictions. The Company's employees are aware of the aforementioned policy in order to ensure that no payments are made to any of the aforementioned countries.

15. APPROVAL OF BUSINESS TO BUSINESS COUNTERPARTIES

The Company may from time to time engage in business to business ("B2B") activity by offering liquidity and acting as a hedging counterparty solely to regulated investment firms or by obtaining services from third parties.

The on boarding process for any B2B counterparties, comprises of four constituent elements:

a. KYC / AML review work (see below) of the B2B counterparty premised on primarily the principles set out in the Wolfsburg Questionnaire, as further described below;

b. Reputational assessment and investment services risks analysis

c. Credit risk assessment on the B2B counterparty;

d. Legal and commercial agreement setting out respective duties, responsibilities, rights and obligations.

With respect to AML / KYC, the following due diligence measures are performed for B2B Clients:

1. Collection of KYC documentation – the Company collects the following:

- Company's full name;
- Company's Address (place of operations);
- Certificate of Incorporation;
- Memorandum of Articles and Association
- Certificate of Registered Address;
- Certificate of Directors and Secretary;
- Certificate of Shareholders;
- Proof of residence of all shareholders with more than 10% holdings;
- Proof of identity of any shareholder with more than 10% holdings;
- Information and economic profile of all shareholders with a beneficial ownership of more than 10%
- Board resolution for the opening of the trading account indicating the authorised person;
- POI and POR of the authorised person if other than the shareholders;
- Latest audited financial statements (if available).

2. Information on the business activities and profile of the B2B counterparty to have an overall understanding of the business activities, the financial standing and sources of the B2B counterparty, the background and profile of the key Directors, management, shareholders and persons exercising significant influence and of the B2B counterparty's general reputation and conduct.

3. Location of the B2B counterparty – the Company confirms that the third party or the controllers of such B2B counterparty (as appropriate) do not operate from a country with strategic AML deficiencies in accordance with the FATF guidelines.

4. Clean World Check result – all potential B2B counterparties, its directors and shareholders need to have a clean World Check result in order to engage with the Company.

16. REPORTING OBLIGATIONS TO FIU

Types of suspicious transactions which may be used for money laundering and terrorist financing are almost unlimited. A suspicious transaction is often defined as any transaction which is out of the ordinary size and scope of a client's business, size of transactions and personal activities or either with the normal business of the specific account. In general, a suspicious transaction will often be one which is inconsistent with the economic profile constructed for the client.

16.1 Recognition of suspicious transactions

- The Company ensures that it maintains adequate information and knows sufficient information about its clients' activities in order to promptly recognize that a transaction or series of transactions is/ are unusual or suspicious;
- The Company takes reasonable steps to ensure that its employees are able to recognize and report suspicious transactions or activity through the provision of appropriate training and the development of this AML policy. Such training is provided via both the day to day interaction of employees with the Compliance officers, as well as through training sessions which include all relevant departments;
- If the Company knows or suspects that a transaction relates with money laundering or terrorist financing, it refrains from carrying out the transaction before informing FIU;
- The Company recognizes that if it is impossible to refrain from carrying out the transaction or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the MLRO, will inform FIU immediately afterwards.

Examples of suspicious transactions

a. Transactions with unclear economic purpose/ rationale.
b. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the client.
c. The transactions or the size of the transactions of the client do not comply with his usual practice and business activity.

d. Large volume of transactions and/or money deposited or credited into an account when the nature of the client's business activities would not appear to justify such activity.

e. There are frequent transactions of the same nature or direction without obvious reason and in conditions that appear unusual.
f. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.
g. Frequent or large transactions that a client makes and has no record of past or present employment experience/ appropriateness.
h. The stated occupation of the customer is not commensurate with the level or size of the executed transactions.

16.2 Reporting of suspicious transactions to FIU

- The Company, in cases where there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, reports through the MLRO its suspicion to FIU;
- The Company, also submits to FIU, the clients who have proceeded with the depositing of cash funds equal or exceeding USD$12,500 (MUR500,000) or any other cash deposits the MLRO upon review considers suspicious and the said funds are not returned to the client until a decision is made from FIU;
- Reports submitted to FIU are via the online reporting system of the FIU (goAML system).
- All reports related to serious suspicious transactions in relation to money laundering issues must be prepared and sent by the MLRO to FIU.
- The Company cooperates fully with FIU and follows any instructions received from them particularly as regards to whether or not to conclude certain trades with the given client. FIU is empowered to instruct the Company to stop, delay or execute a trade with a client, without this being considered a breach of the contractual relationship between the client and the Company

The Company must not disclose to the client that it has reported an issue to FIU (tipping off).

The clients' accounts concerned as well as any other connected accounts are placed under the close monitoring of the MLRO.

17. Record keeping

The Company's policy towards record keeping and archives is as follows.

In case of a suspicious transaction investigation by FIU, the Company will provide without delay the following:

1. Details of the identity of the account;
2. The identity of the true/beneficial owners of the account;
3. The identity of the authorised persons who can operate the account;
4. Details of the volume of funds and the transactions performed through the account;
5. Any connected/related accounts;

6. In relation to specific transactions:

a. The origin of funds,

b. The type and amount of the currency involved in the transaction,

c. The form in which the funds were placed or withdrawn, for example cash, cheques and wire transfers,

d. The identity of the person that gave the order for the transaction,

e. The destination of the funds,

f. The form of instructions and authorization that have been given,

g. The type and identification number of any account involved in the transaction.

All the above records are kept for 7 years from the date of execution of the clients' transactions or the termination of the business relationship with the client, as applicable. The documents/data relevant to on-going investigations by FIU are kept until the said authority confirms that the investigations are completed and the case has been closed.

Further to the abovementioned documents/data, any suspicious activity reports are also recorded.

a. Documents are kept in electronic form as required in this Procedures Manual. Retention of the documents/data may be kept electronically, provided that the Company is able to retrieve the said documents/data without any delay and present them at any time to FSC or to FIU, after request;

b. Retaining identification documents of the client and evidence of the World check performed;

c. Retaining details of the transactions of the clients (client statements);

d. Retaining internal and external reports on suspicious transactions which were actually reported;

e. Retaining annual reports of the MLRO;

f. Retaining reports on suspicious transactions which were investigated internally but not reported to FIU;

g. Retaining records of monitoring of both clients KYC documents and transactions compared to the information submitted as part of the economic profile.

All the above records are kept for 7 years from the date the relationship with a client is being terminated

If there is an on-going investigation by FIU, such relevant information should be retained for as long as the investigation lasts.

18. TRAINING

The training program aims at educating employees on the recognition and handling of transactions and activities which may be related to money laundering or terrorist financing as well as providing an update on the latest developments in this area. The training sessions are structured to ensure relevance to the roles, duties and responsibilities of the Company's personnel.
Training shall be provided on important legal provisions as well as updates on important legislative amendments and on the system and procedures followed in relation to the matters below:

- Relevant Anti-Money Laundering Legislation which is effective in Mauritius;
- Laws and regulations of Mauritius and directives and circulars by competent authorities in relation to the prevention of the use of the financial system for legalization of proceeds from money laundering and terrorist financing activities;
- Guidance and Circulars issued by FSC in relation to AML legal framework;
- Identification and handling of transactions and activities which may relate to money laundering and terrorist financing activity.

Training on issues regarding the prevention of money laundering and terrorist financing should be provided at least once a year to key management and employees in key positions. Training in relation to changes to any of the above matters should be provided on an ad hoc basis as and when any significant changes take place.

The training program has a different structure for new employees and existing employees and for different departments of the Company according to the services provided. In respect of establishing an AML/KYC culture across the organization, all employees should be trained on the respective issues. All the employees of the Company are subject to annual online AML training approved by the Company's MLRO. The Company keeps records and/or evidence for the personnel who attended training/seminars and ensures that proper record keeping procedures are established.

Training Plan
It is noted that the MLRO shall prepare a training plan for each year. The training plan shall at least include the following information:

- Summarized data of the program/content of the training courses/seminars including online training and regulatory training.
- Number and duration of the training courses/seminars.
- Instructors' names and qualifications (where applicable).
- Whether the training courses/seminars were performed in-house or by an external organization or consultants.
- Information for the educational material received

In addition, the MLRO shall also have available information on the specific way/method with which the adequacy and effectiveness of staff training has been assessed and reference to the results and receive feedback from the trainees regarding the quality of the course/seminar and the effectiveness of the trainee.

APPENDIX 1 – Internal MRLO CTF Report

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING	
A. INFORMER'S DETAILS	
Name:	
Position and Department:	
Telephone:	
Email Address:	
B. CUSTOMERS DETAILS	
Name:	
Country of residence:	
Citizenship:	
AID:	
C. INFORMATION / SUSPICION	
Brief description of activities/transactions:	
Reason(s) for Suspicion:	
Date and Signature:	
D. MONEY LAUNDERING COMPLIANCE OFFICER'S USE	
Date Received:	
Reference:	

APPENDIX 2 – Internal MLRO Report

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING	
A. CUSTOMERS DETAILS	
Name:	
Address:	
Country:	
Informer:	
Department:	
B. INQUIRES UNDERTAKEN	
Brief description of activities/transactions:	
C. ATTACHED DOCUMENTS	
D. COMPLIANCE OFFICER'S DECISION	
D. MONEY LAUNDERING COMPLIANCE OFFICER'S USE	
Signature / Date:	
Reference:	

APPENDIX 3 – EU Equivalent Jurisdictions

EU EQUIVALENT JURISDICTIONS
1. Australia 2. South Korea 3. Brazil 4. Mexico 5. Canada 6. Singapore 7. Hong Kong 8. Switzerland 9. India 10. South Africa 11. Japan 12. The United States of America 13. Netherlands Antilles (as the Dutch overseas territories) 14. Aruba (as the Dutch overseas territories) 15. Jersey (as UK Crown Dependencies) 16. Guernsey (as UK Crown Dependencies) 17. Isle of Man (as UK Crown Dependencies) 18. Mayotte (as French overseas territories) 19. New Caledonia (as French overseas territories) 20. French Polynesia (as French overseas territories) 21. Wallis and Futuna (as French overseas territories) 22. Saint Pierre and Miquelon (as French overseas territories)

APPENDIX 4 – PEP ONBOARDING FORM

[AT THE MOMENT THE COMPANY DOES NOT WORK WITH PEPS. LEFT INTENTIONALLY BLANK]

APPENDIX 5 – Joint Account Form

JOINT ACCOUNT APPLICATION FORM	
ACCOUNT HOLDER 1	
Name :	
Address:	
Date of Birth:	
Permanent Address:	
City/Town:	
Country:	
Postcode:	
Years at Current Address:	
Previous Address (if less than 3 years)	
City/Town:	
Country:	
Postcode:	
CONTACT DETAILS	
Telephone:	
Email:	
ACCOUNT HOLDER 2	
Name :	
Address:	
Date of Birth:	
Permanent Address:	
City/Town:	
Country:	
Postcode:	
Years at Current Address:	
Previous Address (if less than 3 years)	
City/Town:	
Country:	
Postcode:	
CONTACT DETAILS	
Telephone:	
Email:	

CLIENT CONFIRMATION

We hereby confirm that we [Names in Full] _____and ("**Joint Account Holders**") are applying to OPTIM Investments Limited for a joint trading Account and enclose this Declaration Form for your consideration.

By applying for a Joint Trading Account with OPTIM Investments Limited we fully understand that if granted:

- The Account will be opened in our joint names.
- The Account will be allocated a single account number.
- The Account will be allocated only one Log-in and Password.
- The above is not a multiple user Log-in and will only support one user at any one time.

By signing this Declaration Form we BOTH declare to OPTIM Investments Limited that:

- We will be jointly and severally responsible for the managing of the Account.
- We have read and understood the terms of this Declaration.
- OPTIM Investments Limited can act on the instructions of either of us without having to first obtain confirmation from the other Joint Account holder unless there is a dispute between us, in such circumstances, we must inform OPTIM Investments Limited of such a dispute. In cases of dispute all of us may be required to provide OPTIM Investments Limited with written instructions on the management of the account.
- That the information that you have provided in this form is true and correct and you will notify OPTIM Investments Limited in writing if any information provided changes or ceases to be correct.

Please note that the email address that you specify in this Declaration Form will be used as a main form of communication with you in the future.

Signed on this day the _____of _____20

Name in full ACCOUNT HOLDER 1

_____

Signature_____

Name in full ACCOUNT HOLDER 2

_____

Signature_____

END OF JOINT ACCOUNT APPLICATION

APPENDIX 6 – Banned Jurisdictions

BANNED JURISDICTIONS
1. Bahamas
2. Botswana
3. Cambodia
4. Democratic People's Republic of Korea (DPRK)
5. Ethiopia
6. Ghana
7. Iran
8. Pakistan
9. Panama
10. Sri Lanka
11. Syria
12. Trinidad and Tobago
13. Tunisia
14. Yemen

APPENDIX 7 - Client identification checklists

The Company is required by its Regulator and by applicable laws and regulations to identify its clients and verify their identity. The documentation that the Company is required to obtain to meet these requirements is contained within the below checklists.

In general terms, the documentation that is required is to enable financial institutions to know their client, including their legal status, constitution, the controlling individuals (e.g. ultimate beneficial owners, directors and signatories), their business activity and the legitimacy of their source of income and assets.

It is also clarified that all of the below are only standardized KYC checklists and the MLRO may request additional or subsequent information or documentation. Failure of the client to supply information required by MLRO could result in the Company terminating its business with a client.

A. KYC Documentation for Natural Persons

Applicable to:

- Natural persons
- Joint Accounts between natural persons

Requirements (as these vary between High Minor, High Median and High Major risk clients):

1. **Proof of Identity (POI):** Copy of Passport or equivalent document

2. **Proof of residence/address (POR):** a document up to 6 months old such as a utility bill, bank or credit card statement, or any other official equivalent document

3. Satisfactory completion of the financial information section of the account opening portal on the basis of which the client's economic profile is constructed

4. **Acceptance of the Company's Policies and Client Agreement**
5. Clean World-check and other online searches (where deemed necessary) result
6. Deposit from a source on the name of the client and from a source is not subject to any international sanctions

In case of **joint accounts** of two or more persons, the identity of all individuals that hold or have the right to manage the account are verified in accordance to the aforementioned requirements. All requested information must be provided to the Company prior the creation of the joint account. Joint Account Application Declaration form (**Appendix 5**) must be duly signed by the clients and match the details provided in Personal Details documentation. In the Declaration Form the clients must agree to be

jointly and severally responsible for the Account and must acknowledge that they have read and understood the Company's terms and conditions.

B. KYC Documentation for Legal Persons

Applicable to:

- Private companies, partnerships, joint ventures, not-regulated entities

Requirements:

1. *Certificate of incorporation*
2. *Certificate of Good Standing (when the* entity is older than one year);
3. *Certificate of Registered Office*
4. *Certificate of Directors and Secretary*
5. *Certificate of Registered Shareholders*
6. *Memorandum and articles of association*
7. In the cases where the registered shareholders act as nominees of the beneficial owners, a copy of the *trust deed/agreement* concluded between the nominee shareholder and the beneficial owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the beneficial owner has been agreed
8. POI and POR for the natural persons that are authorized by the legal person to act on its behalf
9. POI and POR for the registered shareholders (natural persons) with equal or more than 10% beneficial ownership
10. Copies of its latest audited *financial statements* (if available), and/or copies of its latest management accounts (where necessary).
11. Clean World check result for all "natural" person mentioned

Applicable to:

- Unregulated private companies irrespective of jurisdiction;
- Public companies not listed on stock exchanges;
- Unregulated limited liability partnerships

Requirements:

1. Copy of Certificate of Incorporation, or Certificate of Registration of the Partnership and any Change of Name Certificates;
2. Copy of Certificate of Registered Office
3. Copy of Certificate of Shareholders / Limited Partners;
    a. In case the Shareholders/ Limited Partners are other legal entities the following additional documentation is required:
        i. A legal structure chart showing all intermediate entities up to the Ultimate Beneficial Owners;

4. Full legalization documents of the ultimate legal entity which exercises actual control or,

    i. in the case of many ultimate legal entity shareholders, of those legal entities that exercise such control. The legalization documents of intermediary holding companies are not required. The term "legalisation documents" includes (i) Certificate of Incorporation, (ii) Certificate of Registered Office, (iii) Register of Shareholders, (iv) Register of Directors, (v) Memorandum & Articles, whereas the term "control" applies to direct and indirect ownership of over 50%;
    ii. Additional to requirement #8 below, a UBO resolution from the above ultimate legal

entity exercising control.

b. In cases the Shareholders/Limited Partners are Nominees, additionally the below are required either the Nominee agreement OR a UBO resolution from such Nominee shareholder(s).

5. Copy of Certificate of Directors/ General Partners;
6. POI and POR one *Director/ General Partner* *(different verification documentation required for identity and proof of address)*:
7. Copy of the *Memorandum & Articles of Association* or *Limited Partnership Agreement*
8. KYC requirements applicable for natural persons as specified above on *Ultimate Beneficial Owners with* 10% beneficial ownership or more (different verification documentation required for identity and proof of address):
9. Copy of the *list of authorised Signatories* with signature specimens (Authorised by a Director/ General Partner whose name and position can be seen in the documents provided to us).
10. POI and POR for the natural persons that are authorized by the legal person to act on its behalf
11. Clean World check result for all "natural" person mentioned

C. KYC Documentation for Regulated Financial Institutions From EU, US, Mauritius or Approved Countries

Applicable to:

- Banks, Credit, Investment, Insurance, Custody or Fund Management Institutions as well as Broker-Dealers from EU, US, Mauritius or Approved countries;
- Subsidiaries or branches of the above entities

Requirements:

1. Proof of *regulated status/copy of license*;
2. Board resolution indicating the authorized person(s) to operate the account;
3. KYC requirements applicable for natural persons as specified above for the authorized person(s)

D. KYC Documentation for Public Companies Listed on EU Or Approved Countries' Regulated Stock Markets

Applicable to:

- Public companies (and their subsidiaries) having their securities listed on Regulated Stock Markets in EU, US, Mauritius or Approved countries;

Requirements:

1. *Proof of listed status*;
2. List of *authorised Signatories* (duly authorised);
3. Latest Audited *Financial Statements* (approved and signed by Auditors);

E. KYC Documentation for Trusts

Applicable to:

- Bare Trusts, Discretionary Trusts, Private Trusts, Public (Charitable) Trusts, Purpose Trusts

Requirements:

1. Apostilled copy of the *Trust Deed* in order to identify the Trust structure;
2. KYC of the Beneficiaries
3. KYC of the Trustees
4. KYC of the Settlors

5. Apostilled copy of the list of *authorised Signatories* with signature specimens (Authorised by a Trustee/ Director of the Trustee whose name and position can be seen in the documents provided to us). Authorised signatories for trading and back office purposes should also be included.
6. Resolution /Power of Attorney for the person(s) who will be acting on behalf of the entity (in case this person isn't a Director).
7. POI and POR for the authorised person
8. Clean World check result for all "natural" persons mentioned

APPENDIX 8 - Joint Bank Account Declaration Form

Declaration for use of Joint Bank Account

[day/month/year]

Dear Sirs,

I understand that _____("**Your Client**") has opened a trading account with OPTIM Investments Limited and has funded or intends to fund this trading account from a joint bank account that he/she holds with me.

I am the _____ (state the relationship) of Your Client.
I hereby declare to you that:

a) I am fully aware and consent to the use of the joint bank account by Your Client for funding his/her trading account with OPTIM Investments Limited.
b) I am fully aware of the purposes of the trading account of Your Client with OPTIM Investments Limited, including that this may be used for investing in complex financial instruments or speculative trading which carry risk of loss of all capital invested.
c) I will at all times recognize all actions taken by Your Client with respect to funding the trading account with OPTIM Investments Limited from our joint bank account, including instructions given for the return of funds available on the trading account maintained at OPTIM Investments Limited (including of any profits or losses).
d) I am not a client of OPTIM Investments Limited and recognize that OPTIM Investments Limited does not owe any duties or obligations towards me.
e) I am solely responsible for advising OPTIM Investments Limited for any changes in the status of the joint bank account that I maintain with Your Client.
f) I am fully aware that this Declaration is not subject to any time expiry, unless I specifically inform you otherwise and you acknowledge receipt of such advice.

Sincerely,

_____ _____

Name of Joint Account Holder **Signature**

APPENDIX 9 – Suspicious Transactions Checklist

Examples of suspicious transactions/activities related to money laundering and terrorist financing

A. MONEY LAUNDERING

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the customer.
3. The transactions or the size of the transactions requested by the customer do not comply with his usual practice and business activity.
4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the customer's business activities would not appear to justify such activity.
5. The business relationship involves only one transaction or it has a short duration.
6. There is no visible justification for a customer using the services of a particular Financial Organisation. For example, the customer is situated far away from the particular Financial Organisation and in a place where he could be provided services by another Financial Organisation.
7. There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).
8. There are frequent small purchases of a particular financial instrument by a customer who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the customer's instructions, in an account other than his usual account.
9. Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.
10. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.
11. The settlement of any transaction but mainly large transactions, in cash.
12. Settlement of the transaction by a third person which is different than the customer which gave the order.
13. Instructions of payment to a third person that does not seem to be related with the instructor.
14. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on money laundering and terrorist financing.
15. A customer is reluctant to provide complete information when establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with Financial Organisations, names of its officers and directors, or information on its business location. The customer usually provides minimum or misleading information that is difficult or expensive for the Financial Organisation to verify.
16. A customer provides unusual or suspicious identification documents that cannot be readily verified.
17. A customer's home/business telephone is disconnected.
18. A customer that makes frequent or large transactions and has no record of past or present employment experience.
19. Difficulties or delays on the submission of the financial statements or other identification documents, of a customer/legal person.
20. A customer who has been introduced by a foreign Financial Organisation, or by a third person whose countries or geographical areas of origin do not apply or they apply

inadequately FATF's recommendations on money laundering and terrorist financing.

21. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).
22. The stated occupation of the customer is not commensurate with the level or size of the executed transactions.
23. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.
24. Unexplained inconsistencies arising during the process of identifying and verifying the customer (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).
25. Complex trust or nominee network.
26. Transactions or company structures established or working with an unneeded commercial way. e.g. companies with bearer shares or bearer financial instruments or use of a postal box.
27. Use of general nominee documents in a way that restricts the control exercised by the company's board of directors.
28. Changes in the lifestyle of employees of the Financial Organisation, e.g. luxurious way of life or avoiding being out of office due to holidays.
29. Changes the performance and the behaviour of the employees of the Financial Organisation.

B. TERRORIST FINANCING

1. Sources and methods

The funding of terrorist organisations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding "protection" money), smuggling, thefts, robbery and narcotics trafficking. Legal fund-raising methods used by terrorist groups include:

i. collection of membership dues and/or subscriptions,
ii. sale of books and other publications,
iii. cultural and social events,
iv. donations,
v. community solicitations and fund-raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of financial instruments, wire transfers by using "straw men", false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

2. Non-profit organisations

Non–profit and charitable organisations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organisations can be made in the following

ways:

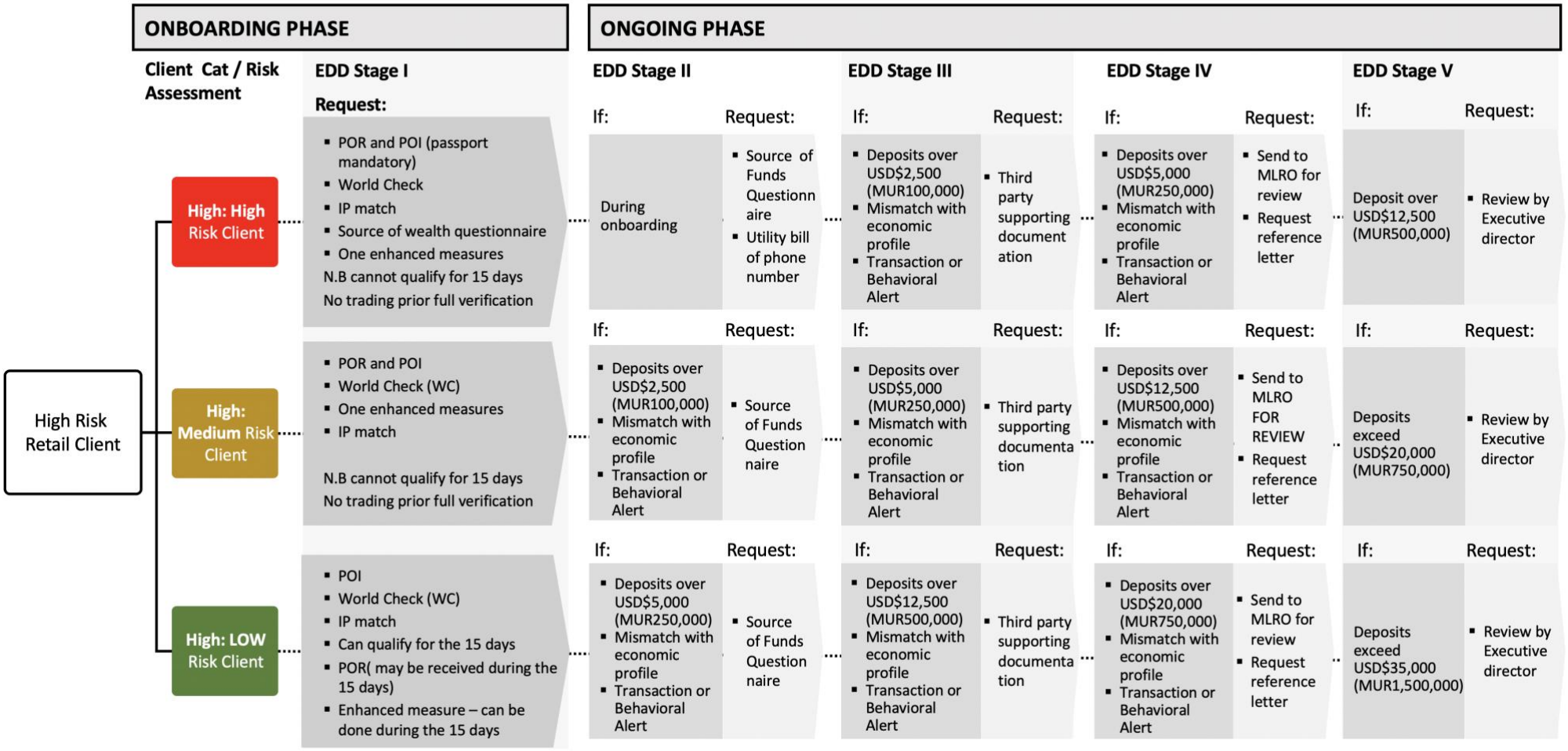
i. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.
ii. A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated
by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
iii. The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.
iv. The non-profit organisation provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organisations indicating that the they may be used for an unlawful purpose are the following:

i. Inconsistencies between the apparent sources and amount of funds raised or moved.
ii. A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.
iii. A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.
iv. Large and unexplained cash transactions by non-profit organisations.
v. The absence of contributions from donors located within the country of origin of the non-profit organisation.

APPENDIX 10 – EDD Client Matrix

New Onboarding and Ongoing Due Diligence Policy



APPENDIX 11 – Glossary of Terms

Acronym	Term	Description
AML	Anti-Money Laundering	A set of measures that financial institutions take to prevent and combat money laundering, terrorism financing, and other financial crimes
AMS	Alexander Management Services Ltd.	A regulated Mauritius Management Company.
B2B	Business to Business	
BoD	Board of Directors	
CDD/DD	Customer Due Diligence	Also known as Due Diligence
CFD	Contract for Difference	A contract between two parties (a "buyer" and a "seller") that stipulates the seller will pay to the buyer the difference between the current value of an asset and its value at contract time
CFT	Combating the Financing of Terrorism	A set of measures that financial institutions take to prevent and combat terrorism financing
CRM	Customer Relationship Management	Software used to manage a company's relationships with clients and potential clients.
CT	Countering Terrorism	
DPA	Data Protection Act	
EDD	Enhanced Due Diligence	When a client's legality is in question, the client onboarding is flagged. This requires a compliance review and approval via an enhanced series of checks. The EDD guidelines are well defined in the AML and KYC policies of the Company.
EMI	Electronic Money Institution	A licensed entity for issuing electronic money
EV	Electronic Evaluation	
FATF	Financial Action Task Force	The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society.
FIAMLA	Financial Intelligence and Anti-Money Laundering	The regulatory authority that oversees regulation, supervision, and inspection of AML guidelines in Mauritius.
FIU	Financial Intelligence Unit	
FSC	Financial Services Commission	The regulatory authority that oversees regulation, supervision, and inspection of all non-bank financial services registered in Mauritius
FX	Foreign Exchange	Foreign Currency Exchange with two pairs, example EUR/USD.
GDPR	General Data Protection Regulation	European Union General Data Protection Regulation 2016/679 (GDPR).
HR	High Risk	
IMF	International Monetary Fund	Organization of 189 countries, working to foster global monetary cooperation, secure financial stability.
IP	Internet Protocol Address	It is an identifying number that is associated with a specific computer or computer network
IT	Information Technology	

Acronym	Term	Description
KYC	Know Your Customer (or Client)	The process that financial institutions must take to verify their customer's identities before providing services
Keesing	Keesing Technologies	Online word check and document verification system.
LR	Low Risk	
MCB	Mauritius Commercial Bank	Local Mauritian Bank under the central banking system.
MD	Managing Director	Equivalent to COO and CEO charges with supporting operations and management functions.
MT4/MT5	MetaTrader 4/5	Trading software provided by MetaQuotes and utilized by thousands of traders
MLRO	Money Laundering Reporting Officer	Compliance Officer that is charged with monitoring inflowing and outflows of company and clients funds to ensure all AML and KYC guidelines are followed.
MONEYVAL		A permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards.
MR	Medium Risk	
MRZ	Machine Readable Zone	Scannable data on Passports and ID cards that can be decoded for verification
MUR	Mauritian Rupees	
NB	Not Onboarded	
OTC	Over-the-Counter	Securities that are traded through a broker-dealer network instead of a formal centralized exchange
PEP	Politically Exposed Person	An individual with a prominent public function, who as a result of their position and influence is likely to have a higher risk for potential involvement in bribery and corruption
PSP	Payment Service Provider	A third-party service that connects merchants to the broader financial system so they can accept electronic payments
PPI	Personal Private Information	A client or customers personal or corporate information.
POI	Proof of Identity	Government ID Card, Driver's license, Passport
POR	Proof of Residence	Utility Bill, Bank Statement, Visa or Yellow card.
SBM	State Bank of Mauritius	Local Mauritian Bank under the central banking system.
STP	Straight-through processing	An automated electronic payment process. The payment and routing information is streamlined, thus eliminating the need for manual inputs from multiple departments and drastically reducing payment times
SWIFT	Society for Worldwide Interbank Financial Telecommunication	Brussels SWFIT messages on bank-to bank transfers, usually MT103 for payments.
TCF	Treating Customers Fairly	The guidelines for treating clients in a professional and supportive manner, providing transparency at all levels to allow clients the ability to make best choices.
USD	United States Dollars	
WC	World Check	Search of online government and news services for PEP and other findings.

OPTIM Investments Limited
30 Saint Georges Street,
3rd Floor, Manor House, Port Louis
www.optimfx.com | info@optimfx.com

OPTIM Investments Ltd is regulated by the
Financial Services Commission (FSC) Mauritius