Finvasia Capital Ltd

("FCL")

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM & PROLIFERATION – ("AML/CFT") MANUAL

Approved by the Board at its meeting held on 01st Oct 2024

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 About Finvasia Capital Ltd

Finvasia Capital Ltd will act as a one-stop-shop by providing a wide range of regulated activities in accordance with the Financial Services (Investment Banking) Rules 2016 including mergers and acquisitions, listings, IPOs, cross-border investment, structuring and also to provide financial advisory services.

As a licensee of the FSC, FCL has an active and important role to play in preventing the exploitation of the industry and the jurisdiction in general by money launderers and terrorist financiers.

Its scope of services would include:

- Investment dealer (full service dealer including underwriting),
- Investment adviser (unrestricted),
- Investment adviser (corporate finance advisory),
- Asset management,
- Distribution of financial services and such other activities
- Providing investment advice, and
- Managing individual, institutional mandates including assets of family offices and High Net Worth Investors.

FCL firmly considers that the key to the prevention and detection of ML and TF lies in the implementation of, and compliance with, effective systems and controls, including sound CDD measures based on international standards.

1.2 Purpose of this Manual and Updates

The purpose of this Manual is to highlight the commitment of FCL to comply with the FIAMLA, the FIAML Regulations, related AML/CFT legislations and generally the highest level of best industry practices in terms of AML/CFT measures and controls.

By adopting this Manual, FCL strongly aspires to formalizes the day-to- day measures taken to combat ML and TF and enhance the board's, senior management's and all employees' understanding of relevant laws, rules, regulations and codes of conduct on ML and TF applicable to FCL's operations. All employees, including senior management and directors of FCL shall receive a copy of this Manual in any format, and they shall acknowledge, in writing, having read and understood the provisions of this Manual. The same shall be evidenced via an acknowledgement form. This procedure shall apply to new employees within one month of them joining FCL.

This Manual has also been designed to guide and assist FCL and its employees to fully apply a more effective, risk based and focused approach in the course their day to day operations and duties respectively.

This Manual will be updated on a yearly basis or earlier as may be required by law and/or upon changes in FCL's internal compliance policy. Any such updates and/or changes will be brought to the attention of all the stakeholders.

2.0 MONEY LAUNDERING, TERRORIST AND PROLIFERATION FINANCING

2.1 What is Money Laundering?

Money laundering is the generic term used to describe the process by which criminals attempt to conceal the original ownership and control of the proceeds of criminal activities by making such proceeds appear to have derived from a legitimate source.

The nature of the services and products offered by the financial services industry (namely managing, controlling and possessing money and property belonging to others) makes it vulnerable to money laundering.

Money laundering is traditionally considered as occurring in three stages:

- **Placement:** Where the proceeds of crime are placed into the financial system. This usually consists of cash payments into a bank account.

- **Layering:** Where funds are converted from one form to another, e.g moved between various accounts or jurisdictions to disguise the audit trail and the illegitimate source of funds. These could involve the use of monetary instruments, electronic funds transfers, property purchases, multiple accounts among others.

- **Integration:** Where the funds that now appear legitimate re-enter the economy for what would appear to be normal business or personal transactions. This typically consists of a complex web of transactions designed to make tracing funds sources nearly impossible.

One or more of these stages may occur consecutively or concurrently. There are no hard and fast rules as to how money laundering occurs, the only limitations being the imagination of the

money launderer and his perception of the risks of being caught.

2.2 What is Terrorist Financing?

TF is defined as the financial support, in any form, of terrorism or those who encourage, plan or engage in terrorism. TF differs from ML in that the source of funds can either be legitimate, such as an individual's salary, or illegitimate, like the proceeds of crimes such as fraud or drug trafficking.

Usually, the focus of scrutiny for potential terrorist financing activity will be the end beneficiary and intended use of the money or assets.

A terrorist financer may only need to disguise the origin of the property if it was generated from criminal activity but in the vast majority of cases they will seek to disguise the intended use i.e. providing support to terrorists or supporting acts of terrorism.

Terrorist financing often involves a complex series of transactions, generally considered as representing three separate phases and this could be sourced through various means for example through seeking donations, carrying out criminal acts and from genuine charities, as detailed hereunder:

- **Collection:** Funds are often acquired through seeking donations, conducting criminal acts or diverting funds from genuine charities.

- **Transmission:** Where funds are pooled and transferred to a terrorist or terrorist group.

- **Use:** Where the funds are used to finance terrorist acts, training, propaganda among others.

Ultimately, what is important to remember is the following:

- Both ML and TF need the support of the financial system; and
- The circumstances that help to raise suspicion about ML, TF and other crimes are more or less the same so that one needs not find out what type of criminal activity possibly lies behind, but is simply required to raise the red flag in case of suspicion.

2.3 What is the Financing of Proliferation of Weapons of Mass Destruction?

Proliferation of weapons of mass destruction involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles).

The proliferation support networks may use the international financial system to conduct transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organizations or acting as representatives or middlemen.

2.4 Overview of Legislative and Regulatory Framework

Mauritius has taken several initiatives over the previous years to introduce relevant laws and regulations in view of reinforcing the country's AML/CFT regulatory framework.

The applicable AML/CFT regulatory framework includes but is not limited to the following:

- The Financial Intelligence and Anti- Money Laundering Act 2002.
- The Financial Intelligence and Anti-Money Laundering Regulations 2018
- The FSC Anti-Money Laundering and Countering the Financing of Terrorism Handbook 2020 ("the Handbook")
- The Prevention of Terrorism Act 2002
- The Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019
- The Prevention of Corruption Act 2002.
- The Convention for the Suppression of the Financing of Terrorism Act 2003
- The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
- International Standards of Best Practice for the Prevention of Money Laundering and Terrorist Financing:

Mauritius is a member of Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) which aims at combatting money laundering and terrorist and proliferation financing on an international level by implementing the FATF Recommendations.

The FATF is an independent and intergovernmental body that develops and promotes policies on AML, CFT and proliferation of weapons of mass destruction and is the most influential body in terms of AML/CFT. It is the global standard setting body for AML/CFT and generally seeks to ensure that the implementation of the FATF Recommendations is broadly consistent from country to country.

In an attempt to further harmonise AML/CFT efforts with international standards and best practices, Mauritius is also party to the following conventions relating to international cooperation:

- The Convention for the Suppression of the Financing of International Terrorism (1999) -
- Memorandum of Understanding on Anti-Money Laundering with members of ESAAMLG (1999);
- United Nations Convention Against Transnational Organised Crime (2001);
- The United Nations Convention against Corruption (2004);
- The African Union Convention on Preventing and Combating Corruption;
- SADC Protocol against Corruption.

The FSC has also adopted international AML/CFT initiatives with which Mauritius as a financial centre must comply. IOSCO Statement of Principles provides a comprehensive framework that complements FATF's Recommendations and addresses the regulator's role in monitoring industry compliance with AML obligations. The list may be consulted at the following address: http://www.iosco.org.

2.5 Summary of Offences under the FIAMLA and the FIAML Regulations

The FIAMLA and FIAML Regulations provide for offences which are related to Money Laundering and Terrorist & Proliferation Financing and related offences. Some of these offences, as applicable to FCL and its employees, are listed at Appendix 1, for ease of reference.

3.0 CORPORATE GOVERNANCE

FCL is committed to high standards of Corporate Governance and the Board acknowledges that the National Code of Corporate Governance for Mauritius 2016 sets out the best practices in terms of corporate governance. The Corporate Governance Report accordingly describes the Company's main governance framework and disclosure requirements under the Code.

Additionally, pursuant to the regulatory framework of FCL, the Board considers that good corporate governance not only provides proper incentives for the directors and senior management to pursue objectives that are in the interest of FCL and its stakeholders, but also facilitates effective monitoring of the Company in respect of compliance with its AML/CFT obligations.

Bottom line, the board and senior management acknowledge that they have a responsibility to ensure that FCL's systems and controls are appropriately designed and implemented, and are effectively operated to reduce the risk of the business being used in connection with ML and TF.

3.1 Board Responsibility for Compliance

Pursuant to the recommended AML/CFT practices set out in the Handbook, the Board's responsibilities for compliance with FCL's AML/CFT requirements are as follows:

(a) To manage FCL effectively and evaluate all potential risks to the organization, including those of ML and TF.
(b) To take ownership of, and responsibility for, the business risk assessments and ensure that they remain up to date and relevant.
(c) To establish a formal strategy to counter money laundering and financing of terrorism on the basis of its business risk assessment.
(d) To document its systems and controls (including policies and procedures) and clearly apportion responsibilities for countering money laundering and financing of terrorism, and, in particular, responsibilities of the CO and MLRO.
(e) To establish and maintain an effective policy, which shall include provision as to the extent and frequency of compliance reviews.
(f) To take a risk-based approach when defining its compliance review policy and ensure that those areas deemed to pose the greatest risk to FCL are reviewed more frequently.
(g) To consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance at a minimum annually, or whenever material changes to the financial institution occur.
(h) Where, as a result of the aforesaid review, changes to the compliance arrangements or review policy are required, to ensure that FCL makes those changes in a timely manner.
(i) To appoint a CO who is responsible for the implementation and ongoing compliance of FCL with internal programmes, controls and procedures in accordance with the requirements of the FIAMLA and FIAML Regulations.
(j) To appoint an independent audit function to test the ML and TF policies, procedures and controls of FCL.
To ensure that the compliance review policy takes into account the size, nature and complexity of the business of FCL, including the risks identified in the business risk assessments.

3.2 Compliance Culture

The board is also mindful of the fact that a hierarchical approach within the Company may hinder an effective system of AML/CFT control. The board strongly deems that the human element is particularly important since systems and controls may only work if they are clearly understood, adhered to and enforced by everyone within FCL.

The board is adamant to and is conscious of the importance to instilling the required compliance culture within the Company so as to have the commitment and collaboration of all employees in meeting its AML/CFT objectives.

At FCL, while it is recognized that the hierarchical relationships face the damaging barriers, as detailed hereunder, the board and senior management are committed to addressing same by encouraging a collaborative approach among the employees and with customers:

(a) senior management being unwilling to lead on the concept of the need for sound corporate ethics;
(b) junior employees assuming that their concerns or suspicions are not significant;
(c) employees being unwilling to subject high value (therefore important) customers to effective CDD checks;
(d) management outside Mauritius pressurizing employees in Mauritius to transact without obtaining all relevant CDD and business relationship information;
(e) employees being unable to understand the commercial rationale for customer relationships and the use of certain products / services, so that potentially suspicious activity is not identified;
(f) lack of time and/or resources to address concerns generating a tendency for line managers to discourage employees from raising concerns; and
(g) conflict between the desire on the part of employees to provide a confidential and efficient customer service and the requirement for employee vigilance in respect of prevention and detection of ML and TF.

3.3 Appointment of Key Persons

3.3.1 Appointment of Compliance Officer

Pursuant to the FIAML Regulations and the FSA, FCL shall appointed and designated a CO at senior management level. The CO is responsible for the implementation and ongoing compliance of the financial institution with internal programmes, controls and procedures with the requirements of the FIAMLA and FIAML Regulations.

The CO appointed by FCL:

a. is a natural person;
b. is of senior management level as defined under FIAML Regulations;
c. is an approved officer under the FSA; and
d. has the appropriate qualification knowledge, skill and experience to fulfil a compliance role within FCL.

FCL ensures that the CO:

a. has timely and unrestricted access to its records;
b. has sufficient resources to perform his duties;
c. has the full co-operation of the financial institution staff;
d. is fully aware of his obligations and those of FCL; and

e. reports directly to, and has regular contact with, the board so as to enable the board to satisfy itself that all statutory obligations and provisions in FIAMLA and FIAML Regulations, and the Handbook are being met and that FCL is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF.

Pursuant to the FIAML Regulations, the main functions of the CO comprise the following:

a. To ensure continued compliance with the requirements of the FIAMLA and FIAML Regulations subject to the ongoing oversight of the board of the financial institution FCL and senior management;
b. To undertake day-to-day oversight of the program for combatting money laundering and terrorism financing;
c. To regularly report, including reporting of non-compliance, to the board and senior management; and
d. To contribute to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism financing.

3.3.2 Appointment of Money Laundering Reporting Officer

Pursuant to the FIAML Regulations, FCL shall appointed an MLRO and a Deputy MLRO who shall perform the duties of the MLRO in his absence.

The MLRO is the one to whom an internal disclosure is made of any information or other matter which comes to the attention of any employee handling a transaction and which, in the opinion of the employee gives rise to knowledge or reasonable suspicion that an individual is engaged in ML or TF.

Pursuant to the FIAML Regulations, the MLRO is:
a. sufficiently senior and has sufficient experience and authority within FCL; and
b. has a right of direct access to the board of FCL and has sufficient time and resources to effectively discharge his functions.

Similarly, the MLRO is an approved officer under the FSA with the appropriate knowledge, skill, experience and competence and is the person who is nominated to ultimately receive internal disclosures and who considers any report to determine whether an external disclosure is required.

FCL ensures that the MLRO:
a. is the main point of contact with the FIU in the handling of disclosures;
b. has unrestricted access to the CDD information of FCL's customers, including the beneficial owners[1] thereof;
c. has sufficient resources to perform his duties;
d. is available on a day-to-day basis;
e. reports directly to, and has regular contact with, the board or equivalent of FCL; and
f. is fully aware of both his personal obligations and those of FCL's under the FIAMLA and FIAML Regulations and the Handbook.

Where the same person acts as MLRO on multiple financial institutions, he will ensure that in accordance with the FIAML Regulations, he has sufficient time and resources to effectively discharge his functions.

[1] The FIAMLA defines the beneficial owner as the natural person who ultimately owns or controls a customer; on whose behalf a transaction is being conducted; and includes those natural persons who exercise ultimate control over a legal person or arrangement.

The responsibilities of the MLRO comprise the following:

a. undertaking a review of all internal disclosures in the light of all available relevant information and determining whether or not such internal disclosures have substance and require an external disclosure to be made to the FIU;
b. maintaining all related records;
c. giving guidance on how to avoid tipping off the customer if any disclosure is made;
d. liaising with the FIU and if required the FSC and participating in any other third party enquiries in relation to ML or TF prevention, detection, investigation or compliance; and
e. providing reports and other information to senior management.

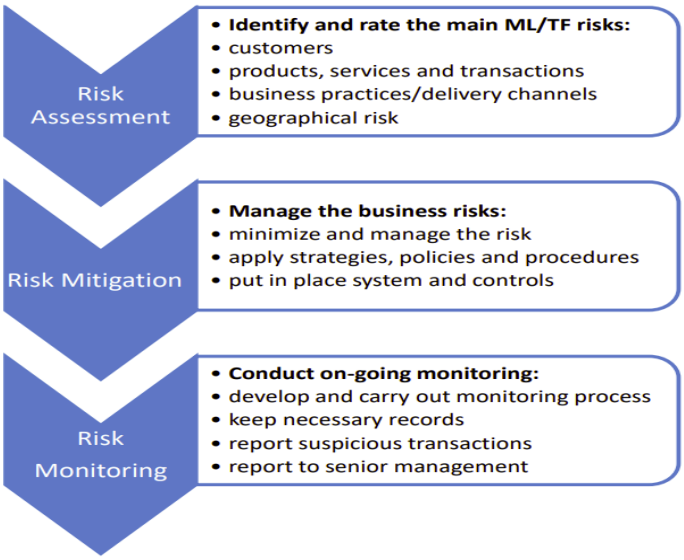
4.0 RISK BASED APPROACH

4.1 Overview

A Risk Based Approach to AML/CFT means that countries, competent authorities and financial institutions, such as FCL, should identify, assess and understand the ML and TF risks to which they are exposed and take reasonable and proportionate AML/CFT measures to effectively and efficiently mitigate and manage the risks accordingly.

An RBA towards the prevention and detection of ML and TF aims at developing preventive and mitigating measures that are commensurate with the ML and TF risks identified by FCL.

To this effect the Board of FCL shall undertake a Business Risk Assessment (BRA) to identify risks to which it may be exposed to and ensure that the BRA remains up to date. Policies and procedures shall be implemented to mitigate the risks identified. FCL shall allocate resources depending on the risks identified. The diagram depicts visually the three different steps in implementing a Risk Based Approach, that is, risk assessment, risk mitigation and risk monitoring.



FCL adopts an AML/CFT approach that corresponds to the risks it is exposed to as a result of the nature of its business, customers, products, services and any other matters which are relevant in the context of AML/CFT and ensures such risk-based assessments are: (i) objective and proportionate to the risks; (ii) based on reasonable grounds; (iii) properly documented; and (iv) reviewed and updated at appropriate intervals.

As part of the Risk Based Approach, FCL shall have the following in place:

(a) Business risk assessments: periodic assessments of FCL's business which enable the directors and the senior management to understand the ML and TF risks facing FCL; assess FCL's vulnerabilities to those risks and take all reasonable steps to eliminate or manage them. Where relevant, FCL must also assess and mitigate money laundering risks relating to a new product, business practice or technology before their launch or use.

(b) Customer risk assessments: assessments of the ML and TF risks presented by each customer of FCL. All applications for business shall be risk rated and depending on the level of risk (Low, Medium or High) resources shall be allocated throughout the client relationship with FCL, that is, from onboarding the client until the client closes its accounts with FCL.

(c) Different Due Diligence standards: Enhanced due diligence measures for high risk (including PEPs) applications and simplified due diligence where risks are lower;

(d) Different approval authorities for approving client onboarding;

(e) Risk mitigation by means of robust internal controls, policies and processes and on-going monitoring that are proportionate to the risks that have been assessed. Some measures include:

- Ongoing screening for all customers;
- Different degrees of transaction monitoring
  Transaction monitoring should be conducted using a risk based approach. The extent of monitoring, that is, the frequency and intensity of monitoring should be commensurate with the risk profile of the customer. Where the risks are high, FCL should conduct enhanced transaction monitoring, while in low risk situations, FCL may consider reducing the extent of monitoring; and
- Different approval authorities for processing of transactions.

The above is not an exhaustive list of measures implemented as part of FCL Risk Based Approach.

4.2 Business risk assessment

- FCL will, at least annually, identify and assess any money laundering risks to which its business is exposed, taking into consideration the nature, size and complexity of its activities and when any material changes are made to its business, and to the extent relevant, any vulnerabilities relating to:

a. **The Nature, Scale and Complexity of FCL's activities.**
b. **The Products and Services provided by FCL.**
c. **The Persons to whom and the Manner in which the products and services are provided.**
d. **The Nature, Scale, Complexity and Location of the Customer's activities.**
e. **Reliance on Third Parties for elements of the customer due diligence process.**
f. **Technological Developments.**

- FCL will ensure that any risk identified in the business risk assessment is taken into account in its day to day operations, including in relation to: (i) the development of new products, business practices, delivery channels and the use of new technologies for both new and existing product; (ii) the onboarding of new customers and (iii) changes to its business profile.
- FCL will ensure that reasonable steps are taken to assess the risks described above prior to launching and using the new product, practice or technology. The CO will determine whether any additional CDD Information or beneficial owner information should be collected from relevant customers, either before any new products, practice or technology is provided to the customer.
- FCL will use the information obtained in its periodic business risk assessments to develop and maintain its AML/CFT policies, procedures, systems and controls, ensure that they adequately mitigate the risks that have been identified, assess their effectiveness, and assist in the allocation and prioritization of AML/CFT resources and in carrying out its customer risk assessments.
- When conducting the business risk assessment, FCL will assess its vulnerabilities to money laundering, the results of this assessment will also feed into the assessment of customers; however this does not mean that FCL will treat all its customers under one business line as posing the same level of risk. All customers will be assessed on a case-by-case basis.

4.3 Customer risk assessment

- FCL will conduct a customer risk assessment and assign the customer a risk-rating proportionate to the latter's ML and TF risks prior to onboarding a new customer.
- When conducting a customer risk assessment, FCL will:

(a) identify the customer and any beneficial owner;
(b) obtain information on the purpose and intended nature of the business relationship;
(c) obtain information on, and take into consideration, the nature of the customer's business;
(d) take into consideration:

(i) the use of complex and unusual corporate structures, location of the customer's business if different from where the customer lives (without adequate explanation), unusual customer inference or reluctance by the customer to communicate directly with FCL, and other potential higher risk factors, in assessing the tax crime risk associated with the customer; the nature of the customer, its ownership and control structure, and its beneficial ownership, if any, i.e. its legal structure, business or occupation, location of the customer's business and commercial rationale for its business model; and the potential that the customer may be involved in tax crimes;
(ii) the nature of the customer's business relationship with FCL, i.e. how the customer is introduced to FCL and whether the relationship will be purely advisory or involve arranging and/or executing transactions;
(iii) the customer's country of origin, residence, nationality, place of incorporation or place of business;
(iv) the relevant product, service or transaction; and
(v) the outcomes of the business risk assessment.

- The customer will be assigned a risk rating of “high”, “medium” or “low”. Of note that customers having similar characteristics may be assigned different risk ratings having regard to the product concerned and any other relevant factors relevant to the customer risk assessment.
- FCL will periodically review each of its customer’s risk rating to ensure that it remains appropriate in light of current ML and TF risks.
- When conducting its customer risk assessment, FCL will stand guided by the risk factors provided under relevant AML/CFT legislations.

The methodology for risk rating customers shall be submitted to the Board for approval and same shall be reviewed on a yearly basis or more frequently (if required).

4.4 Client Onboarding Approval Matrix

After carrying the CDD process upon being satisfied of same, the Company will adopt a sign off / approval matrix for onboarding clients or to accept to continue relationship in case of deterioration of risk profile for an on- going relationship.

Risk Category	Sign off	Approval
Low Risk	Onboarding System / Team	Automated (unless there is a potential hit) Sample check by CO on a monthly basis or such earlier frequency.
Medium Risk	Onboarding System / Team	Automated (unless there is a potential hit) Sample check by CO on a monthly basis or such earlier frequency.
High Risk	Onboarding System / Team	Prior approval of: 1. CO; and 2. Managing Director or any executive director

The names of the person undertaking or responsible for the onboarding procedure shall be noted on the file, together with the name of the higher ranking officer (CO/Managing Director/Executive Director) who has approved the business relationship.

4.5 Prohibited business

- FCL will not establish a business relationship with a Legal Person or legal arrangement if the ownership or control arrangements of the customer prevent FCL from identifying one or more of the customer’s beneficial owners.
- FCL will not establish or maintain an anonymous account, an account in a fictitious name or a nominee account which is held in the name of one person but which is controlled by or held for the benefit of another person whose identity has not been disclosed to FCL.
- FCL will not establish or maintain a business relationship with a shell bank or enter into a correspondent banking relationship with a Shell Bank and take appropriate measures to ensure that FCL does not enter into, or continue a corresponding banking relationship with, a bank which is known to permit its accounts to be used by Shell Banks.

- FCL will not do business with a client or business partner who is identified by reference to findings, recommendations, resolutions, sanctions of, inter alia, the UN, any Mauritius enforcement agency, HMT or OFAC as a proscribed person.

5.0 CUSTOMER DUE DILIGENCE

5.1 Introduction

The term *"customer due diligence"* or *"CDD"* refers to the identification and verification of the customer, the beneficial owner(s) and the principals of the customer (where the customer is a legal person or arrangement) using reliable, independent source documents, data or information, the understanding of the nature and purpose of the business, the identification of the risks associated with the business and the ongoing monitoring of those risks throughout the customer relationship.

FCL is required to identify its customers, and where applicable, their beneficial owners and then verify their identities, which FCL deems essential to the prevention of money laundering and combating the financing of terrorism.

Similarly, the terms Identification and Verification refer to the process of establishing and verifying a customer's identity.

Verification relates to the verification of elements of the identification information, by using independent reliable sources, which may include data obtained from the customer such as a passport to verify the customer's name. In brief, it is the process through which FCL satisfies itself that its customers are who they state they are.

FCL acknowledges that the inadequacy or the absence of satisfactory CDD measures can subject FCL to serious customer and counterparty risks, as well as reputational, operational, legal and regulatory risks, any of which can result in significant financial cost to its business.

FCL shall carry out customer due diligence checks on the incoming clients in accordance with the laws and regulations of Mauritius.

5.2 Objectives of CDD Measures

FCL considers that having sufficient information about a customer or prospective customer, and making effective use of that information reinforces all other AML/CFT procedures. In addition to minimizing the risk of being used for illicit activities, it provides protection against fraud, enables suspicious activities to be recognized and protects FCL from reputational and financial risks.

The second requirement is to ensure that when a business relationship is being established, the nature of the business that the customer expects to conduct is ascertained at the outset in view of determining the expected business activity. In order to be able to determine whether a transaction is suspicious or not, employees need to have a clear understanding of the legitimate business of customers.

The main objectives of FCL's CDD measures are to ensure that:

- A prospective customer is who he/ she claims to be.
- Any ML and/or TF activity will be identified, flagged internally to the MLRO and, if required, reported externally by the MLRO to the FIU.
- There will be sufficient information available with respect to a customer, his/ her principals, his/ her entity, his/ her business and the beneficial owner(s) in order to assist any regulatory authority in the case of a request or an investigation.
- FCL is not used as a vehicle by money launderers and criminals to carry out ML and TF activities.
- The business of a customer does not expose FCL to unwanted risks.

5.3 Applicable CDD Measures

The CDD measures which FCL is statutorily required to undertake include the following:

a. identifying and verifying the identity of each applicant for business;
b. identifying and verifying the identity of individuals connected to the account or transaction, such as the customer's beneficial owner(s);
c. obtaining information on the purpose and intended nature of the business relationship (the inability for employees of FCL to understand the commercial rationale for business relationship may result in the failure to identify non-commercial purpose and therefore potential ML and TF activity);
d. conducting ongoing due diligence on the business relationship and scrutiny of transactions throughout the course of that relationship, to ensure that the transactions in which the customer is engaged are consistent with FCL's knowledge of the customer and its business and risk profile (including the source of funds);
e. achieving each of the above measures by using reliable, independently sourced documents, data or information (this is intended through the use of commercial databases and public information); and ensuring that all documents collected under the CDD process is kept relevant and up to date (for example undertaking reactive reviews in response to trigger events, and by undertaking regular planned reviews of existing records at intervals determined by risk rating, with higher risk customers warranting more frequent reviews).

5.4 Circumstances under which FCL will conduct CDD

FCL shall conduct CDD measures when:

a. establishing a new business relationship with an applicant for business[2]

[2] It includes any natural or legal person or arrangement-corporate or unincorporated that seeks to form a business relationship or to carry out a one-off transaction with FCL.

[3] An "Occasional transaction" means any transaction carried out other than in the course of a business relationship.

b. conducting occasional transactions[3] or making fund transfers in excess of Rs. 500,000 or an equivalent amount in foreign currency, either in a single operation or in several operations that appear to be linked;
c. there is a suspicion of ML and/or TF; and
d. it is required by any law.

Once identification procedures have been satisfactorily completed and the customer relationship has been established, as long as regular contact is maintained and records concerning that customer are kept in accordance with FCL's internal procedures, no further evidence of identity may be needed when transactions are subsequently undertaken unless doubts have arisen about the accuracy or adequacy of the identification evidence that has been obtained previously.

Employees need to ensure that the primary documentation secured is valid at the time of request and on an ongoing basis, as may be determined by the risk profile of customer.

When an existing customer incorporates another company, there may be no need to re- verify his/her identity as long as regular contact has been maintained. However, the opportunity should be taken to request for any missing or additional information concerning the customer and to re-confirm the name, address and signature. This is particularly important if there has been no recent contact with the customer, for e.g. within the past twelve months or when a previously dormant business relationship is re-activated.

5.5 Whose Identity should be verified?

Employees are requested to verify the identity of all applicants for business and the principals of such applicant. A principal of an applicant for business is any person who is a beneficial owner of, or who has a beneficial interest in, or has direct or indirect control of any relationship established with FCL. For the avoidance of any doubt, the following should be considered as principals of customers:

a. *for trusts*: settlors or Contributors of capital, whether named or otherwise, trustees, beneficiaries[4], protectors and enforcers;
b. *for companies:* at least two directors, shareholder(s) holding the voting rights at general meetings or which is in a position to control the appointment and/or removal of directors holding a majority of voting rights at board meetings on all or substantially all matters;
c. *for partnerships*: partners owning or controlling the partnership, including limited partners; and
d. in all the above cases: account signatories and persons operating under power of attorneys.

FCL is aware that an applicant for business may be an individual acting on his own behalf or for others (for example, a trustee of an express trust), or a legal body or legal arrangements seeking to enter into or having entered into a business relationship or to conduct an occasional transaction, as principal or on

[4] In the case of discretionary members, verification of the identity may be delayed until prior to the making of any distributions to them

behalf of a third party.

In this respect, FCL will take reasonable measures at the time of establishing a business relationship to determine whether the applicant for business is acting on behalf of a third party.

Should FCL determine that the applicant is acting for a third party, it will accordingly keep a record setting out:

a. the identity of the third party (and any beneficial owners or associated persons as required);
b. the proofs of identity; and
c. the relationship between the third party and the applicant for business.

Similarly, where funds are received from any natural or legal person or arrangement - corporate or unincorporated - on behalf of the applicant for business, appropriate CDD measures should be undertaken prior to accepting same in view of understanding the relationship between the relevant parties.
In all cases, the identity of the ultimate beneficial owner should be identified and verified.

5.6 Timing of Verification of Identity

Before the establishment of a new customer relationship and before providing any financial services, FCL should be in a position to complete all the required CDD measures. A Customer Acceptance Form shall be completed by the staff members for review and sign off by the Compliance Department.

In exceptional circumstances, CDD measures can be completed within a reasonable delay of the establishment of the customer relationship. In the event where it is necessary to provide financial services to a customer prior to completion of CDD measures, then the decision to perform same must be authorised by the board or senior management of FCL. However, as a general rule, no transaction should be undertaken prior to receiving all required CDD information and documentation.

Factors such as nature of business activity, profile and geographical location of the parties, and whether it is practical to obtain evidence can be considered prior to accepting a relationship without full CDD. In all cases, funds should not be wired in or out of the customer bank's account.

In the event that satisfactory CDD documentation has not been obtained within the prescribed time period, the funds must be returned to the applicant. *No funds must be returned to a third party.*

The failure by an applicant to provide satisfactory identification evidence without adequate explanation may in itself lead to a suspicion of ML or TF.

Should FCL form a suspicion that one or more actual or proposed transactions relate to ML or TF, it should take into account the risk of tipping off when performing the CDD process.

In this respect, should FCL reasonably believe that performing the CDD process will tip off the customer or potential customer, it should stop the CDD process and make an external disclosure with the FIU in such circumstances.

5.7 Risk Based Approach to CDD Measures

FCL will adopt a risk based approach in applying CDD measures. The risk assessment of a customer will determine the extent of identification information (and other CDD information) that will be required and requested, the manner in which the information will be verified and the extent to which the resulting relationship will be monitored.

Besides, the extent of customer relationship information sought in respect of a particular applicant or type of applicant, will depend upon the jurisdiction with which the applicant is connected, the characteristics of the product or services requested, the delivery channel of the product or service as well as factors specific to the applicant and the associated risk ratings.

5.8 Examination of Source of Funds and Source of Wealth

As part of the CDD information which FCL is required to keep the declaration and evidence of source of funds and the source of wealth of the customer.

The source of funds refers to the origin of the particular funds or assets which are the subject of the business relationship between FCL and its customer and the transactions FCL is required to undertake on the customer's behalf, such as the amounts invested, deposited or remitted.

The source of funds requirements relate to where the funds are coming from in order to fund the relationship or transaction. This does not refer to every payment going through the account, however FCL must ensure with the ongoing monitoring of the business activity and transactions of the customer.

All relevant information, including email communications, explaining SoF shall be kept in client files.
The source of wealth, on the other hand, refers to the origins of a customer's financial standing or total net worth, i.e those activities which have generated a customer's funds and property.

FCL is required to hold sufficient information to establish the source of wealth and this information must be obtained for all customers and all other relationships where the type of product or service being offered makes it appropriate to do so taking into account the risk profile of the customer. Sufficient SoW information should be collected to enable ACBM to form a reasonable conclusion that the customer has earned or otherwise acquired their accumulated capital legally. This may involve obtaining supporting documentation from the customer to validate the SoW information.

All relevant information, including email communications, explaining SoW shall be kept in client files.

FCL has, to that effect, introduced a Guide to Source of Fund and Source of Wealth as provided under Appendix 4 of this Manual.

5.9 Other Considerations

For express trusts, the CDD information should provide the type of trust (e.g. discretionary), the structure of any underlying legal bodies (if applicable) and nature of activities undertaken by the trust and any underlying legal bodies. This should include the classes of beneficiaries and classes within an expression of wishes.

Likewise, FCL will periodically update relevant CDD information and its risk assessment throughout the business relationship with each customer.

In the event of any material change (for example, in beneficial ownership or control of the applicant / customer or the third parties on whose behalf the applicant/customer acts, or an adverse change in FCL's perception of the reliability of the CDD information it already holds), then reasonable further measures should be undertaken to verify the identity of the applicant/customer.

FCL will ensure that there is consistency between the information it holds on the applicant /customer and the nature of transactions or proposed transactions.

Where there is any indication of abnormal or potentially suspicious activity within the context of the product or service being provided, or any other event occurs to cast doubt on the CDD held by FCL, FCL will then undertake additional measures to verify the information already obtained and to obtain such further information as may be necessary.

5.10 Customer Identification & Verification

FCL shall identify and verify the identity of the customer, the beneficial owner(s), and, where the customer is a legal arrangement or entity, its principals using primary and secondary identification documents. Primary identification documents are those that establish the name, date and place of birth and nationality, while secondary identification documents are used as proof of permanent residential address. The requirement will however vary for an individual, a company, a trust, a partnership and any other type of entity.

Employees should establish to their satisfaction that they are dealing with a real person or entity and obtain identification evidence sufficient to establish that the applicant is that person or entity.

- **Types of Customers and Information & Documentation Required**

FCL shall obtain the minimum information/set of documents from various types of clients, details of which are as hereunder:

5.10.1 Identification & Verification Data for Natural Persons

S/n	Information Required	Documentation Required
1.	Legal name (including any former names, aliases and any other names used)	• Current valid passport • Current valid national identity card • Current valid driving licence (where FCL is satisfied that the driving licensing authority conducts a check on the holder's identity before issuing the license). In each case of the above, the document must incorporate photographic evidence of identity. The documentation required should be provided in certified true copies.
2.	Sex	
3.	Date of birth	
4.	Place of birth	
5.	Nationality	

6.	Current residential address P.O. Box addresses are not acceptable	• Any of the identity sources listed above. • A recent* original or certified true copy of a utility bill issued to the individual by name. • A recent bank or credit card statement or a recent original bank reference[5]. • A recent reference or letter of introduction from: i. A financial institution that is regulated in Mauritius; ii. A regulated financial services business which is operating in an equivalent jurisdiction or a jurisdiction that complies with the FATF standard; or iii. A branch or subsidiary of a group headquartered in a well-regulated overseas country which applies group standards to subsidiaries and branches worldwide, and test application of, and compliance with, such standards. In case any of the above is not available, or where the Compliance department deems it proper, the following additional / alternative identification documents / information and/or actions may be sought or undertaken: - A reference from an attorney and/or an accountant who has known the client ina professional capacity for at least two years; and/or - A bank reference from a recognised banking institution bank (which is found on the banker's almanac) which has known - the person for at least the last two years[6] ***Recent* means within the last three months.**
7.	Permanent residential address (if different to current residential address)	
8.	Any public position held and, where appropriate, nature of employment (including self-employment) and name of employer	•A letter or other written confirmation of the individual's status from the public body in question and/or any enhanced CDD; a letter or other written confirmation of employment. •A curriculum vitae signed by the individual •An Individual Questionnaire, when the client does not fill in the FSC Personal Questionnaire.
9.	Government issued personal identification number or other government issued unique identifier	The relevant government document

[5] The letter should be on the bank's letterhead and should indicate that the customer has been an upstanding customer for a stated period of time (for at least two years) and the permanent residential

address.

[6] To be requested on all providers of funds

5.10.2 Identification & Verification Data for Legal persons

For legal persons/ private entities, in addition to verifying the legal existence of the business, the principal requirement is to look behind the corporate entity to identify and verify the identity of the beneficial owners by obtaining information on:

(a) The identity of all the natural persons who ultimately have a controlling ownership[7] interest in the legal person.
(b) Where there is doubt under (a) above as to whether the person with controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interest, the identity of the natural person exercising effective control of the legal person.
(c) Where no natural person is identified under (a) and (b) above, the identity of the natural person who holds the position of senior managing official[8], the principal owners and controllers, including those who control the company's assets, with particular attention being paid to nominee arrangements. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes to directors/shareholders or to the original nature of the business/activity.

FCL will ensure that any person purporting to act on its behalf has sufficient authority.

The following information/documents will be required on the relevant legal persons:

Persons to be identified	**Information Required**	**Documentation Required**
Underlying persons who are individuals.	As per the information requirements for natural persons as detailed under section 5.10.1 above.	As per the documentation requirements for natural persons as detailed under section 5.10.1 above.
	Where the individual persons are such by virtue of their status as members of the board of directors of a relevant legal person (or equivalent – such as Partnership – *including the General Partners and Limited Partners under a Limited Partnership*, or council members in a Foundation), FCL is required to identify and verify the identity of all such persons	Where the legal person with which the underlying person is associated is low or standard risk, then the documentation required will normally suffice and can be one of the above documentation requirements for natural persons detailed in the previous section However, where the legal person is high risk, then the documentation may depend on the riskiness of the relationship and more than one documentation required may be necessary.

[7] A controller is a person who is able to control or exert significant influence (through shareholding interest or otherwise) over the business or financial operations of a company whether directly or indirectly.
[8] Senior Management includes an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

• Private Companies • Partnerships • Sociétés • Foundations • Other Legal Persons	• Legal status body • Legal name of body • Any trading names • Nature of business • Date and Country of Incorporation / registration • Official identification / registration (for example, company number) • Registered office address • Mailing address (if different) • Principal place of business / operations (if different) • Any other data which FCL considers to be reasonably necessary for the purpose of establishing the true identity of the legal person.	• Certificate of incorporation (or other appropriate certificate of registration or licensing) • Constitution/Memorandum and Articles of Association • Register of Directors/Shareholders, where available • Company registry search, including confirmation that the legal person is not in the process of being dissolved, struck off, wound up or terminated • Latest audited financial statements or equivalent • Annual report or equivalent • Personal visit to principal place of business • Partnership deed or equivalent • Charter of Foundation • Acte de société • Certificate of good standing from a relevant national body • Reputable and satisfactory third party data, such as business information service • Any other source of information to verify that the document submitted is genuine. • Copy / extracts of board resolution authorizing any principal to act on its behalf (if applicable) *The documentation required should be provided in certified true copies.*

5.10.3 Identification and Verification Data for Legal arrangements

The key objective for ML and TF prevention via trusts, foundations, and nominees is to verify the identity of the provider of funds, i.e. the settlor/ founder, those who have control over the funds, i.e. the trustees, and any controllers, protectors or enforcers, who have the power to remove or influence the trustees/council members and any other natural person exercising ultimate effective control over the trust/foundation, including through a chain of control and ownership.

FCL will ascertain and verify the nature and purpose of the trusts/foundations and source of funding. It will also verify the identity of any beneficiaries who are able to exercise influence over the trustees.

Where the trust has migrated from another jurisdiction, FCL will additionally require the deed of retirement and appointment of trustees for its records.

The following information/documents will be required on the relevant legal arrangements:

Person/Arrangement to be identified	Information Required	Documentation Required
Underlying principals who are legal persons	As per the information requirements for legal persons detailed above. Where an applicant for business which is a legal arrangement acts or purports to act on behalf of a legal person, then identification and verification must take place not just in respect of that legal person, but also in respect of that legal person's underlying principals in accordance with the previous paragraph above.	As per the documentation requirements for legal persons detailed above.
Legal arrangement	-Legal status of arrangement (including date of establishment)Legal name of arrangement (if applicable) -Trading or other given name(s) of arrangement (if applicable) -Nature of business -Any official registration or identifying number (if applicable) -Registered office address -Mailing address (if different) -Principal place of business/ operations (if different) -Any other data which FCL considers to be reasonably necessary for the purposes of establishing the true identity of the legal arrangement	• Trust deed or equivalent instrument • Official certificate of registration (if applicable) Where the above proves insufficient, any other document or other source of information on which it is reasonable to place reliance in all the circumstances. *The documentation required should be provided in certified true copies.*

5.10.4 Certification of Documents

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

Where an employee of FCL meets an applicant for business or the principals there of face-to-face and has access to original verification of identity documentation or where the employee has verified the document by means of video call or electronic verifications, he or she may take copies of the verification of identity documentation and certify them personally as true copies of the original documentation. Moreover, whenever a video call is conducted with a client, an evidence of the video

call shall be kept to demonstrate that identification and verification has been conducted. Evidence of the video call may include a recording of the call and/or such evidence (example a screenshot taken during the call, calendar meeting request) which may singly or cumulatively be used to evidence the call.

In other cases, copies of the verification of identity documentation can be certified by a suitable person, such as a lawyer, notary, actuary, an accountant or any other person holding a recognized professional qualification, director or secretary of a regulated financial institution in Mauritius or in an equivalent jurisdiction, a member of the judiciary or a senior civil servant (non-exhaustive list).

The certifier should sign the copy document and clearly indicate his **name**, **address** and **position** or **capacity** (registration number from the professional body, as applicable) on it together with **contact details** to aid tracing of the certifier.

FCL is required to exercise due caution when considering certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction.

Where certified copy documents are accepted, it is FCL's responsibility to ensure that the certifier is appropriate. In all cases, the Company should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document.

5.10.5 Translation of documents

In instances where documents are not in the English or French language, the principle is that officially certified translations of such documents/information in the English or French language must be obtained/ kept. An exception to this is where their document which is not in English or French can be read and understood by at least one officer of FCL. In this situation, FCL may accept the original document, or true certified, provided the prescribed officer of FCL, who does understand the language, translates the necessary points into a due diligence note and signs same, clearly stating his or her full name and date accordingly.

5.11 Understanding the Nature and Purpose of the Business

FCL will take all reasonable measures and exercise due diligence in order to understand the purpose, nature and commercial rationale of the proposed business relationship and to obtain information on the source of funds/property which will be used in the furtherance of the business objectives of the customer.

Such information will be kept up-to-date and the customer undertakes to inform FCL of any change in the purpose and/ or nature of his/ her business activities. This will allow FCL to explain variations in the normal patterns or levels of activity of the customer entity.

Where the customer is entering into the business relationship on behalf of another person or in any other capacity, this must be disclosed and FCL will also have to satisfy itself of the

identity of that other person as it would have done for the customer.

5.12 Enhanced Due Diligence

There are a number of circumstances where the risk of the customer can be higher and hence the requirement to exercise enhanced due diligence. These include both high risk business relationships assessed by FCL based on the risk profiling system and the following categories of business relationships.

1. If the Customer has been assigned a "high" risk rating following the Customer risk assessment FCL will, in addition to undertaking standard CDD, undertake Enhanced CDD.
2. Enhanced CDD involves, to the extent necessary as determined on a case by case basis:

   a. obtaining and verifying additional:

      i. identification information on the customer and any beneficial owner;
      ii. information on the intended nature of the business relationship; and
      iii. information on the reasons for a transaction;

   b. updating more regularly the CDD that FCL holds on the customer and any beneficial owners;
   c. taking reasonable measures to establish the source of funds and source of wealth of the customer or, if applicable, of the beneficial owner;
   d. increasing the degree and nature of monitoring of the business relationship, in order to determine whether the customer's transactions or activities appear unusual or suspicious; and
   e. obtaining a member of senior management's approval to commence or continue a business relationship with the customer.

3. Where appropriate, the Enhanced CDD measures may include:

   a. obtaining documentary evidence as to the source or circumstances that gave rise to the Customer or Beneficial Owner's funds and wealth;
   b. getting a better understanding of the Customer's business and business structures, the Customer's use of the Company's products and services and the nature and level of business to be expected from the Customer;
   c. taking steps to be satisfied that a Customer's use of complex legal structures and/or the use of trust and private investment vehicles, has a genuine and legitimate purpose and to properly understand the chain of title, authority or control leading to the ultimate Beneficial Owner, settler and beneficiaries, if relevant;
   d. to the extent that the assets belong to the beneficial owner and not the customer, enquiring into the beneficial owner's source of funds and wealth;
   e. taking reasonable measures to establish the Source of Funds that is, where the funds for a particular service or transaction will come from, for example, a specific bank account held with a specific financial institution, and whether that funding is consistent with the source of wealth of the Customer or, if applicable, of the Beneficial Owner. This also includes obtaining independent corroborating evidence such as, for example, proof of dividend payments

connected to a shareholding, bank statements, salary/bonus certificates, loan documentation and proof of a Transaction which gave rise to the payment into the account. A Customer should be able to demonstrate and document how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a Transaction;

f. taking reasonable measures to establish the source of wealth by obtaining independent corroborating evidence; and
g. commissioning an independent third party report to obtain further information on a customer or transaction or to investigate a customer or beneficial owner in very high-risk cases. Such reports may be particularly useful where there is little or no publicly-available information on the person concerned.

5.12.1 Politically Exposed Persons

A Politically Exposed Person (PEP) is defined by the Financial Action Task Force - ("FATF") as an individual who is or has been entrusted with a prominent public function, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials.

Pursuant to the Financial Intelligence Anti Money Laundering Regulations 2018 – ("FIAML Regulations"), A PEP means a Foreign PEP, a Domestic PEP and an International Organisation PEP. The members of their immediate families and known close associates are also pose a higher risk.

Due to their position and influence, it is deemed that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing.

The potential risks associated with PEPs warrant the application of additional AML/CFT preventive measures with respect to business relationships with PEPs, including EDD measures.

This increases the risk of dealings with proceeds of corruption which would jeopardise the organisation's reputation; or even its existence. FCL will take reasonable measures to determine if a customer, or a beneficial owner of a customer, is a PEP.

Customer relationships that fall into this category should be clearly monitored by senior management for transactions or series of transactions above a pre-determined limit[9].

Appropriate due diligence measures can assist in recognising when there is no logical answer to newly acquired wealth or source of funds in these circumstances. When dealing with PEP, FCL will ensure that the customer completes the PEP declaration form at Appendix 2.

[9] Such a pre-determined limit has to be determined at the outset and agreed between the customer take on team and the compliance department.

5.12.2 Non-Face-To-Face Business Relationships & Non-Equivalent Jurisdictions

FCL recognizes that electronic and other non- face-to-face financial services, such as transmission of instructions or establishment of a business relationship through facsimile, internet or other electronic means which carries more risks by reason of the ease of access to the network, lack of personal relationship with the customer, thus causing greater difficulties in conducting CDD measures and identifying suspicious transactions. This applies mainly to transactions involving non-equivalent jurisdictions.

- **Other Specific Circumstances**

- dealing with a customer or receiving funds from a particular jurisdiction that has been classified as being non-cooperative by international standard-setters in AML/CFT;
- dealing with customers from non-equivalent jurisdictions – Reference shall be made to the FATF list of Equivalent Jurisdictions on its website at the following address: www.fatf-gafi.org
- dealing with companies with bearer shares;
- dealing with casino businesses, horse racing betting businesses, slot and other game machine and similar gaming businesses; or
- dealing with a real estate agent and dealer in high value commodities like gold, precious stones among others.

Where the go-ahead has been given to enter into a high risk business relationship, enhanced CDD measures must be applied to that customer on an ongoing basis, having regard to the need to preserve FCL's reputation of a sound financial services provider. This would involve, but is not limited to, making online searches on the customer to know more about him/ her and on his/ her line of business and previous ventures and make an assessment on whether there is any matter for concern.

5.13 Simplified Due Diligence

FCL considers that in general, the full range of CDD measures should be applied. However, it also acknowledges that SDD measures can be implemented in cases where lower risks have been identified and where the CDD measures are commensurate with the lower risk factor in accordance with the statutory requirements.

FCL understands that the application SDD measures does not remove from its responsibility to conduct CDD measures, it only allows for reduced measures.

Under all circumstances, FCL will keep the customer risk assessment up to date and review the appropriateness of CDD obtained even if SDD measures are adopted.

FCL may consider applying apply SDD measures where:

a. Lower risks have been identified and the SDD measures are commensurate with the lower risk factors; and

b. There is a low level of risk which is consistent with the findings of any risk assessment carried out, whichever is most recently issued;

Where FCL adopts SDD measures in respect of a particular applicant or customer, it will:

a. document that decision in a manner which explains the factors which it took into account (including retaining any relevant supporting documentation) and its reasons for adopting the aforesaid measures in question; and
b. keep the relationship with the applicant or customer (including the continued appropriateness of using the SDD measures) under review, and operate appropriate policies, procedures and controls accordingly.

FCL will never apply SDD where it knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in ML or TF or that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in ML or TF and where there are other indicators of ML/TF risk.

In any case, should FCL adopt SDD, it would apply a risk-based approach to determine whether to adopt the SDD measures in a given situation and/or continue with the aforesaid measures, although these customers' transactions and business activities and are still subject to transaction monitoring obligations.

5.14 Failure to Complete CDD Measures

If the CDD exercise has not been completed, or where the CDD documents provided to FCL have proven to be unsatisfactory, for a continuous period of one month from the date of establishment of the customer relationship or request of document/information in the case of an existing customer, FCL will promptly return any funds received from the customer to the account where the funds originated from. This is notwithstanding the fact that the failure of the customer to provide satisfactory CDD documents without a good reason may, in itself lead to a suspicion of ML.

1. If FCL is unable to conduct or complete the CDD, it will apply one or more of the following measures as may be appropriate in the circumstances:

   a. not carry out a Transaction with or for the Customer;
   b. not open an account or provide a service;
   c. not otherwise establish a business relationship or carry out a Transaction;
   d. subject to 2. below, terminate or suspend any existing business relationship with the Customer;
   e. subject to 2. below, return any monies or assets received from the Customer; and
   f. consider whether the circumstances necessitate the making of a STR.

2. Where CDD cannot be completed, it may be appropriate not to carry out a Transaction pending completion of the CDD. Where CDD, or a material part of it, such as identifying and verifying a Beneficial Owner cannot be conducted, the business relationship with the Customer should not be established.

3. FCL is not obliged to apply any of the measures in (1) above if:

a. to do so would amount to “tipping off” the Customer; or
b. The FIU directs FCL to act otherwise.

4. In the case of a new Customer it may be appropriate to terminate the business relationship before a product or service is provided. In the case of an existing Customer, however, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances. In either case the Company must be careful not to tip off the Customer.

5. FCL is not obliged to terminate or suspend any existing business relationship with the Customer, or return any monies or assets received from the Customer, if:

   a. to do so would amount to “tipping off” the Customer; or
   b. the FIU directs FCL to act otherwise.

6. Note that failure to comply with (b) above would constitute a significant violation of the law which may lead to enforcement action by the FIU.

   Any derogation from the above has to be approved by the board, and the reasons of same recorded in writing.

5.15 Dealing with Complex Arrangements & Transactions

FCL will scrutinise all complex, unusual large transactions within customer entities and also all unusual patterns of transactions or structures, especially those which have no apparent/ visible economic or lawful purpose.

5.16 Third Party Reliance for Customer Due Diligence

Where FCL relies on a third party, it shall ensure that the following requirements are complied with:

1. That a contractual arrangement is in place with the third party.
2. That the identification information sought from the third party is adequate and accurate.
3. That the CDD information is submitted immediately in line with section 17D of the FIAMLA upon onboarding notwithstanding that the requisite documentation may be provided upon request at a later stage.
4. That the ultimate responsibility for CDD measures shall remain with FCL.
5. That the third party is regulated, supervised and monitored and subject to CDD in line with section 17C of the FIAMLA and record keeping requirements pursuant to section 17F of the FIAMLA and Regulation 21 of the FIAML Regulations.
6. That, when reliance is placed on a third party that is part of the same financial group, it shall ensure that the group applies the measures as applicable under Regulation 21(4) of the FIAML Regulations.
7. That a country risk assessment of the third party be conducted.
8. That regular assurance testing is carried out in respect of the third party arrangement to ensure that the CDD documents can be retrieved without undue delay and that the documentation received is sufficient pursuant to section 17 (2) (v) of the FIAMLA.
9. That the third party arrangement complies the applicable AML/CFT legislation

Where there is a third party arrangement in the context of investment funds, FCL shall ensure that there is a signed agreement between the investment fund, the third party and FCL in which the third party agrees to being relied upon and undertakes to provide any CDD information obtained immediately upon onboarding.

The signed agreement shall contain clear contractual terms of the obligations of the third party to obtain and maintain the necessary CDD records and to provide the CDD documents upon request and shall not contain any condition term which may result in the inability of the third party to provide the aforesaid CDD documents.

5.17 Electronic Identification and Verification

FCL shall adopt a system providing for the electronic verification of client's identity, FCL shall assess the veracity of the controls inherent within the system in order to determine whether FCL can place reliance on the results produced, or if additional steps are necessary to complement the existing controls.

The additional steps undertaken by FCL could include requiring a representative of FCL or a designated third party for example a lawyer, a notary or an accountant to be present with the natural person when on-boarding software is being used.

In all circumstances, FCL shall adopt a risk based approach to satisfy itself that the documents received adequately verify that the customers are who they say they are and that FCL is comfortable with the authenticity of the documents received. FCL could check the type of file and ensure it is tamper-resistant, it could check the email address it is being received from to ensure it seems legitimate and related to the customer sending in the documentation, if the document has been certified, that same has been done by a suitable certifier etc.

Where FCL is unsure of the authenticity of the documents based on electronic means of collection, or that the documents actually relate to the customer, a cumulative approach should be taken and additional measures or checks undertaken to gain comfort. If still unsatisfied with the verification of identity or address the business relationship must proceed no further, FCL must terminate the business relationship and consideration be given to making an internal disclosure.

Given the nature of the transactions which will take place in a highly competitive environment and the profile of the clients who can open an account with a minimal amount, the due diligence aspect will be conducted on two fronts.

FCL shall have dedicated persons to conduct verification of KYC documents submitted at account-opening stage and run screening checks on the client. Once the documents have been successfully verified, the account of the client is approved, thus enabling the client to transfer the funds. All the KYC documents shall be saved on an online folder which will be made available to the MLRO, Deputy MLRO and Compliance Officer of FCL. Sample checks will be done on a monthly basis or earlier frequency, with any exception reports to the Management and/or the Board for remedial action.

5.17.1 Identity Document Verification

The identity document that a client may upload into the system should meet the following requirements:

- The document is valid for at least one month from the upload date.
- The document is not scratched, stained, or torn.
- The applicant full name, date of birth, MRZ, and other important information is present and can be read.
- All the documents in the application must belong to the same person.

The ID document must contain:

- Full name
- Full date of birth
- Document number
- Validity data (issue date or validity period)
- Owner photo
- Owner signature

The photo of the ID document uploaded to the system should meet the following requirements:

- The uploaded file is an original photo (static image) or scan (not a screenshot or a photo uploaded from social networks) in JPG, JPEG, PNG, PDF.
- If the document has data on the front and back, both sides should be uploaded.
- The size of the uploaded file is no less than 100 KB or 300 DPI.
- The photo is in color.
- The information in the document is readable.
- All corners of the document are visible and no foreign objects or graphic elements are present.
- The uploaded photo has not been edited with any software or converted to PDF.
- The document is not digital (in most cases).

Identity Verification Process

Once an ID document is uploaded, the document is verified in 3 steps:

Step 1: Authenticity

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature and pixel analysis.

Signature Analysis: A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures is used to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Each image gets a digital trust score:

- **Low** – red (high risk of editing).
- **Acceptable** – yellow (there might be something to take a closer look at).
- **Normal** – green (a trusted and authentic image).

Pixel Analysis: This method is used on demand in addition to signature analysis to identify abnormal areas within the image. For example, deviations from sustainable local characteristics. The results of the analysis are shown as a probability map, where areas suspect to tampering are highlighted.
In most cases, pixel analysis is combined with the manual analysis of a forensic expert.

Step 2: Image integrity

Integrity checks are designed to ensure the uploaded image represents an official document by comparing it with a template from a database of original documents.

Sumsub integrity checks:

- General conformity to the template.
- Presence of security features, such as watermarks, holograms, and so on.
- Font originality and compliance with the relevant standards (width, spaces between the letters, and so on.).
- Required fields and inscriptions.

Step 3: Document data validation

At the final step, the data extracted from the document is checked against various sources, including sanctions and watchlists database.

Liveness and face-match

Sumsub's Liveness and Deepfake Detection technology provides robust verification measures. It ensures that applicants are real individuals, preventing the use of deepfakes, paper masks, photos, dolls, or similar fraudulent methods. Moreover, it verifies the authenticity of the provided documents by matching the applicant's face with the image on the document. This comprehensive process helps detect and prevent the creation of duplicate accounts.

5.17.2 Proof of Address document verification (POA)

PoA verification consists of the following steps:

- Uploading a PoA photo.
- Checking the image for authenticity.
- Checking the integrity of the image.
- Data extraction (full name, home address, issue date).
- Data validation (whether the address is complete, if it exists and if it is really a home address).

- Expiry date validation.
- Validation of the extracted data against the ID document data.
- Verification of the provided PoA against available data sources.

Authenticity Detection Technology

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature and pixel analysis.

Integrity Detection Technology

Integrity checks are designed to ensure the uploaded image represents an official document by comparing it with a template from a database of original documents.

Sumsub integrity checks:

- General conformity to the template.
- Font originality and compliance with the relevant standards (width, spaces between the letters, and so on).
- Required fields and inscriptions.

How Sumsub Extracts Data?

Due to a wide variety of PoA document structures, Sumsub uses an OCR engine to extract plain text and then a machine learning algorithm to structure and group all the data into logical blocks.

The system extracts the applicant full name, home address, and the date at which the PoA was issued.

How Sumsub Validates PoA Data?

To ensure the completeness and consistency of the extracted address data, Sumsub utilizes external map services, such as Google Maps, Open Street Map, and others, which allows to see the applicant's geolocation in the Dashboard.

PoA Verification Settings

By default, the system accepts PoA documents that have been issued within the last 3 months. These are cross-validated against a provided proof of identity.

5.17.3 AML and Sanctions Screening

AML and sanction screening checks customers using multiple types of sources (sanctions, watchlists, and PEPs lists, etc.) to ensure they're absent from sanctions lists, not involved in money laundering/ financial crime, and generally trustworthy.

High-risk clients are easily detected with AML screening, while they are continually checked against global watchlists, sanctions, PEPs, and adverse media.

AML screening notifies Sumsub clients whether their applicants (both physical and legal entities) are on any of the various sanctions lists and watchlists.

Ongoing AML monitoring is the process introduced by organizations to ensure that their business relationships are consistent. This keeps information about applicants up-to-date with changes to sanction lists and watchlists across the globe.

Sumsub updates data as soon as changes are made to the sanctions lists and watchlists. This enables us to access reliable data from trustworthy sources, reducing manual labor and protecting our business from crime.

6.0 MONITORING OF TRANSACTIONS & ACTIVITY

6.1 Objectives

FCL acknowledges that the regular monitoring of a business relationship, including any transactions and other activity carried out as part of that relationship, is a key element of effective ongoing CDD measures.

It will undertake on-going monitoring of FCL's customer's business activity upon completion of initial due diligence in order to identify any unusual activity and ensure that due diligence records are up to date.

This is considered as an essential component of effective CDD procedures and the extent of monitoring will be proportional to the risk category of the customer.

FCL will, additionally, scrutinize transactions conducted throughout the course of the business relationship to ensure the transactions are consistent with its knowledge of the customer.

In brief, the monitoring of transactions and customers' activities involves the application of scrutiny to large and unusual or complex transactions, as well as to patterns of transactions to ensure that such transactions are consistent with FCL's knowledge of the customers, their business and risk profile, including where necessary, the source of funds.

Particularly, FCL pays attention to high risk relationships (for example, those involving PEPs), high risk countries and high risk business activities.

6.2 Statutory Obligations

Pursuant to the provisions of the FIAML Regulations, FCL is required to:

a. Understand and obtain adequate and relevant information on the purpose and intended nature of its business relationship or occasional transaction with customers.

b. Conduct ongoing monitoring of its business relationship with its customers, including –

   i. scrutiny of transactions undertaken throughout the course of the relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with its knowledge of the customer and the business and risk profile of the customer; and

ii. ensuring that documents data or information collected under the CDD process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of customers.

c. Consider applying EDD measures for higher risk business relationships including conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

d. Conduct enhanced ongoing monitoring on foreign PEPs, whether as customer or beneficial owner, in addition to performing the CDD measures. The same requirement applies in cases when there is higher risk business relationship with a domestic PEP or an international organisation PEP.

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

(a) undertaking more frequent reviews of high risk relationships and updating CDD

(b) information on a more regular basis;

(c) undertaking more regular reviews of transactions and activity against the profile and expected activity of the business relationship;

(d) applying lower monetary thresholds for the monitoring of transactions and activity;

(e) reviews being conducted by persons not directly involved in managing the relationship, such as the Compliance Officer;

(f) ensuring that FCL has an adequate system in place to provide the board and Compliance Officer with the timely information needed to identify, analyse and effectively monitor high risk relationships;

(g) appropriate approval procedures for high value transactions in respect of high risk relationships; and/or

(h) a greater understanding of the personal circumstances of high risk relationships, including an awareness of sources of third party information.

Similarly, FCL will assess and mitigate the risk for legal persons and legal arrangements to be used as vehicles for ML and TF.

6.3 PEP Relationships

FCL's ongoing monitoring framework provides for the identification of a customer or beneficial owner when he becomes a PEP during the course of the business relationship.

Where a customer or beneficial owner becomes a PEP, FCL's PEP policy (Appendix 2) shall apply.

6.4 High Risk Transactions & Red Flags

When conducting ongoing monitoring, FCL and its employees should be aware of the following non-exhaustive examples of red flags which may indicate high risk transactions or activity within a business relationship:

(a) an unusual transaction in the context of FCL's understanding of the business relationship (for example, abnormal size or frequency for that customer or peer group, or a transaction or activity involving an unknown third party);

(b) funds originating from, or destined for, an unusual location, whether specific to an individual business relationship, or for a generic customer or product type;

(c) transactions or activity unexpectedly occurring after a period of dormancy;

(d) unusual patterns of transactions or activity which have no apparent economic or lawful purpose;

(e) an instruction to effect payments for advisory or consulting activities with no apparent connection to the known activities of the customer or their business;

(f) the involvement of charitable or political donations or sponsorship; or

(g) a relevant connection with a country that has significant levels of corruption, or provides funding or support for terrorist activities.

FCL and its employees understand that they has an obligation under the FIAMLA to prevent and detect ML and TF. Hence, where they are suspicious, or have knowledge of, ML or TF, they will not unquestioningly execute instructions as issued by the customer.

When FCL and its employees are faced with unreasonable customer instructions leading to suspicions of ML/TF, FCL will file a suspicious transaction report and also consider taking legal advice.

6.5 Examination of Transactions

FCL will examine the background and purpose of its customers' complex, or large and unusual transactions or patterns of transactions which have no apparent or economic and lawful purpose.

As part of its examination, FCL will consider the following:

(a) reviewing the identified transaction or activity in conjunction with the relationship risk assessment and the CDD information held;

(b) understanding the background of the activity and making further enquiries to obtain any additional information required to enable a determination to be made by FCL as to whether the transaction or activity has a rational explanation and economic purpose;

(c) reviewing the appropriateness of the relationship risk assessment in light of the unusual transaction or activity, together with any supplemental CDD information obtained; and

(d) considering the transaction or activity in the context of any other connected business relationships and the cumulative effect this may have on the risk attributed to those relationships.

FCL will ensure that the examination of any large and unusual, complex, or otherwise higher risk transaction or pattern of transactions or other activity is sufficiently documented and that such documentation is retained in a readily accessible manner in order to assist the FSC, the FIU, other domestic competent authorities and auditors should FCL be required to provide the aforesaid competent authorities with relevant information.

FCL will ensure that the first payment is carried out through an account in the customer's name with a bank that is subject to the standards set out by the FATF.

Following the conclusion of its examination, FCL will consider whether follow-up action is necessary in light of the identified transaction or activity. This may include, but is not limited to:

(a) applying EDD measures where this is considered necessary or where FCL has reassessed the business relationship as being high risk as a consequence of the transaction or activity;

(b) considering whether further employee training in the identification of large and unusual, complex, or higher risk transactions and activity is needed;

(c) considering whether there is a need to adjust the monitoring system (for example, refining monitoring parameters or enhancing controls for more vulnerable products, services and/or business units); and/or

(d) applying increased levels of on-going monitoring for particular relationships.

6.6 Handling Cash Transactions

FCL recognizes that the use of cash and monetary instruments as a means of payment or method to transfer funds can pose a higher risk of ML/TF than other means, such as wire transfer, cheques or illiquid securities.

This is because unlike other financial products, with cash and monetary instruments, there will likely be no clear audit trail and source of fund.

Pursuant to Section 5 of the FIAMLA, any person who makes or accepts any payment in cash in excess of MUR 500,000 or an equivalent amount in foreign currency, or such amount as may be prescribed, shall commit an offence.

FCL will therefore approach any situation where cash and monetary instrument transactions are being proposed by customers, and where such requests are not in accordance with the customer's known reasonable practice, with caution and will make relevant further enquiries.

FCL will also consider factors such as the amount of cash, currency, denominations and the age of the notes in determining whether the activity is 'normal' for the customer along with a comparison with the customer's expected activity in respect of cash transactions.

FCL will adopt a robust approach in case there are requests for frequent or unusually large amounts of cash and monetary instrument by customers, especially where the customer is resident in jurisdictions where tax evasion is a known problem. FCL will, additionally, be vigilant for explanations given by customers which do not stand up to scrutiny.

Where FCL and /or its employees have been unable to satisfy themselves that the transaction is a legitimate activity, and therefore consider it suspicious, an internal disclosure must be made.

6.7 Real-Time and Post-Event Transaction Monitoring

The transaction and business monitoring procedures of FCL involve a combination of real-time and post-event monitoring.

The over-arching purpose of the monitoring process is to ensure that unusual transactions and activity are identified and flagged for further examination and relevant actions.

FCL will ensure that any alert raised is examined within the shortest delay and properly documented prior to closure.

6.8 Automated and Manual Monitoring

FCL's monitoring processes is proportionate to its size, activities and complexity, together with the risks identified within its business risk assessment.

Considering its size, scales of business and volumes of transactions, FCL considers that a manual real-time and/or post-event monitoring process is adequate.

FCL deems that should its size, scales of business and volumes of transactions grow significantly, the implementation of an automated monitoring process may be considered.

FCL shall monitor transactions depending on the AML risk rating of the client:

AML Risk Rating	Account monitoring
Low	All Client/Account activity will be subject to monitoring on a bi-annual basis
Medium	All Client/Account activity will be subject to monitoring on a quarterly basis
High	Place Client on On-Going Monitoring List (e.g. Transactions, Account Activity). Monitoring frequency at least on a monthly basis or frequent depending on nature, complexity and scale of the Company.

6.9 Ongoing CDD Monitoring

FCL will conduct ongoing CDD monitoring on a risk based approach so that customer information is accordingly updated.

In this respect, updated information on the customer will be requested after having considered and assessed that the existing data held on the customer is not adequate or when FCL is doubtful about the veracity of the aforesaid data. For instance, should there be a material change in the way that the business of the customer is conducted which is inconsistent with its current business profile, or should FCL become aware of changes to a customer's or beneficial owner's circumstances such as a change of professional status, address among others, FCL request updated information for consideration.

FCL will avail of the occurrence of particular trigger events, such as the opening of a new account or the purchase of additional product or service, to review the CDD information held for low risk customers.

While so doing, FCL will also consider conducting an updated customer risk assessment to that effect.

FCL will additionally ensure that any updated CDD information obtained through meetings, discussions or other methods of communication with the customer is duly recorded and kept in the customer's file and available to the MLRO for examination.

Besides triggering factors, client files shall be updated and updated CDD documentation shall be requested as follows:

AML Risk Level	File Review
Low	Request for updated KYC (if expired) every 2 years
Medium	Request for updated KYC (if expired) every 2 years
High	Request for updated KYC (if expired) at least on a yearly basis

6.10 Screening of customers and connected parties

The purpose of screening is to identify associations with ML/FT prior to commencing a business relationship. Screening involves consideration of the risks arising from the following sources:

- Sanctions lists,
- PEP lists,
- Negative news;
- Internet search
- Commercial database, for example, SumSub, World-Check One, Accuity, KYC 360 and other screening tools.

Both the entities and the individuals associated with the entities need to be subjected to screening. Screening against Sanctions, Terrorist, PEP or other lists helps to identify customers and its Connected Parties who may pose a higher risk of financial crime to FCL.

Negative facts/news screening allows FCL to identify further information on the customers and connected parties which contributes to establishing a full understanding of the financial crime risks associated with the relationship.

General Screening Requirement

Upon all required documentation and information is submitted as per the CDD procedures, FCL compliance team shall start the review. The team shall leverage the use of third-party database screening tool (example SumSub, World Check/Accuity, Sanctions Lists, PEP Lists, Internet Search, etc) for customers, connected parties and its BO. All the directors, authorized persons/representatives, partners and beneficial owners (altogether referred as to “associated persons or connected person”) should be screened to confirm they are not sanctioned parties or

PEPs or related to ML/FT negative news. No business relationship can be started before the customers and its Connected Parties have been screened.

If it is known that customers and if relevant, the UBO have changed its name in the past, screening should include both the new name as well as the previous name(s). Both names should also be subject to negative news/facts screening.

FCL shall use SumSub and Internet for screening purposes. Automation shall be preferred.

Information which must be screened against the lists (as applicable):

	Information to be screened
Individuals	Full legal names identified during ID&V; Nationality; City and country of residential address (includes current and permanent if different as well as any other correspondence address) identified during ID&V; and Former Names
Corporates	Full legal names identified during ID&V; Any 'Trading As' names; City and country of registered office address in country of incorporation and city and country of business address identified during ID&V; and Former Names

Associated Persons	**Information to be Screened**
BOs	Full legal name of the individuals or legal entity identified including the UBO(s) and intermediate BO(s) (For Operating Companies, only BOs > 20% ownership needs to be screened) or those having management control; and Address. Individuals - city and country of residential address (includes current and permanent if different as well as any other correspondence address) identified during

	ID&V; or Legal entity - city and country of registered office address in country of incorporation and city and country of business address identified during ID&V.
Legal representatives	Full legal name of the individuals or legal entities; and Address. Individuals - city and country of residential address (includes current and permanent if different as well as any other correspondence address) identified during ID&V; or Legal entity - city and country of registered office address in country of incorporation and city and country of business address identified during ID&V.
Other Directors, not identified as Legal representatives	Full legal name of the individuals identified in ID&V; and City and country of residential address (includes current and permanent if different as well as any other correspondence address) identified during ID&V.
Other third-parties (i.e. authorized agents and power of attorney)	Full legal name and any "Trading as" names identified in ID&V; and Address. Individuals - city and country of residential address (includes current and permanent if different as well as any other correspondence address) identified during ID&V; or Legal entity - city and country of registered office address in country of incorporation and city and country of business address identified during ID&V.
Other Related Parties	**Information to be Screened**
Other related parties with significant influence (including but not limited to settlor, trustee, the protector of a trust)	Where identified, the full legal names and address of these parties must be screened.

Negative News screening

Negative news screening is a key mechanism for identifying adverse news about an individual or an entity. This ensures necessary steps are taken to protect FCL's reputation.

Negative news is defined as adverse information about an individual, an entity or a connected person that may or may not be factual. Negative news may be speculative and may not be supported by a definitive verdict or fact.

For example, a news story from a reputable source indicating individual that is being investigated for a crime relating to money laundering is relevant negative news even if the investigation is ongoing and no verdict has been found.

Negative news involves public source searches and requires a judgmental assessment of the relevance and materiality of any finding. Further investigation may be required to determine the veracity of the information. Negative news screening should be undertaken using search strings and may be limited to public domain information.

Materiality on Negative News Screening

Where negative news is identified, consideration must be given to its materiality and impact on the customer relationship.

This assessment is judgmental. However, negative news must be considered material where the information is relevant to determining whether the customer poses a higher risk of financial crime.

Where there is uncertainty in respect of whether an item of negative news is material, it should be consulted and escalated to the CO.

By way of guidance, the following would be indicative of material negative news:

(i) criminal and regulatory enforcement action, financial crime violation or other illegal activity conducted or facilitated by the customer, Third Parties or other related party; or
(ii) information which raises a serious reputational risk concern from FCL's association with the customer.

Other factors to consider when determining whether negative news is material include:

i. **the seriousness of the news:** For example, information about low level litigation brought against or by customers is generally not material
ii. **aging of the news:** Historic negative news is generally less material than a recent event. Negative facts may still be relevant irrespective of age; and
iii. **reliability and number of sources:** Information which is hearsay or from a single non- established

source may be less material than information obtained from a reputable source and/or where several sources are used to corroborate the negative news.

Alert Clearing

If the individual/entity which was screened (including sanction, PEP and negative news screening) appears to be a match with an individual/entity on one of the official/other lists, this is classified as a potential name match ("**Potential Match**"). Where a Potential Match is identified, further data points of the subject of the Potential Match must be checked e.g. date of birth or address, in order to determine whether or not they are a true name match ("**True Match**"). Where there is any doubt the Potential Match must be escalated to the CO.

During the screening process, FCL must make a determination as to whether a Potential Match is a True Match or a mistaken result ("**False Positive**"). The alert clearing procedure set out in this section enables this process.

A copy of all documentation used during the alert clearance procedure must be retained by FCL for a period of not less than 7 years. The supporting documentation must include a rationale relating to the conclusion (e.g. 'the Potential Match is determined to be a False Positive due to the different age of individual being screened and the Potential Match').

The CO or user completing the screening result should be easily identifiable from the records maintained. In addition, the retained records should clearly show the date on which (i) screening and (ii) alert clearance took place.

If the Potential Match is determined to be a True Match, further action needs to be taken based on the nature of the hit. The following guidance may be referred to for determining the next actions for True Matches:

(i) Individual/entity is sanctioned — immediate escalation to relevant onboarding approving authority with a view to reject account opening application or terminating the business relationship, if there is any, and reporting suspicions to FIU as necessary.
(ii) Individual/entity is found to be a PEP — Additional due diligence will be performed to determine the risk level. The Managing Director will authorize the entry into the relationship.
(iii) Relationship is high risk where negative news is found — The relationship must be considered in light of the negative news. In particular, FCL's Managing Director should be made aware of the negative news. If FCL is comfortable to continue with the relationship, FCL should document the rationale for the conclusion and any additional measures that may be applied.

Criteria for Determining False Positives and True Matches

The criteria below is provided for guidance purposes:

For individuals:

(i) Different age/date of birth;
(ii) Different nationality/location/country of residence/citizenship;
(iii) Different employment (e.g. where a potential match relates to a professional or "white collar" crime);
(iv) Middle names or initials; and
(v) Picture.

For entities:

(i) Different registration and/or business addresses; and
(ii) Different business names
(iii) Different registration / incorporation number;
(iv) Different tax ID;
(v) Different business names.

The data sources to be used are the KYC information obtained on the party that is screened and the information contained in the Potential Match of the screening result.

Ongoing Screening

In addition to new customer onboarding, FCL will undertake screening on an ongoing basis. This shall be done through SumSub (which includes sanctions lists) and negative media search and/or google alert monitoring. In the event that there is a True Match in screening after a business relationship has commenced, FCL compliance team will evaluate the True Match as a matter of urgency and make a determination as to what is the appropriate course of action, which will include consideration of whether or not the MLRO should file a STR to FIU.

6.11 Oversight by the Compliance Officer

The CO is familiar with and has access to the results and output of FCL's monitoring processes for review purposes.

The CO will then report to the Board on a regularly basis by providing relevant management information together with details of any trends and actions taken where concerns or discrepancies have been identified.

The board of FCL will also consider the appropriateness and effectiveness of the monitoring processes as part of its annual review of the Company's business risk assessment and related policies, procedures and controls.

FCL will ensure that the weaknesses identified with regard to the monitoring system are addressed in a timely manner.

7.0 SUSPICIOUS TRANSACTION REPORTING

FCL acknowledges that it has a key responsibility in determining transactions which give rise to reasonable ground to suspect any potential link to ML and TF.

A suspicious transaction will often be one which will be inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of entity or with the customer's risk profile.

7.1 Reporting Obligations under the FIAMLA

Under the FIAMLA, a suspicious transaction is defined as a transaction which:

(a) gives rise to a reasonable suspicion that it may involve –

(i) the laundering of money or the proceeds of any crime; or

(ii) funds linked or related to, or to be used for, the financing of terrorism or proliferation financing or, any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment, whether or not the funds represent the proceeds of a crime;

(b) is made in circumstances of unusual or unjustified complexity;

(c) appears to have no economic justification or lawful objective;

(d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or

(e) gives rise to suspicion for any other reason.

A Suspicious Transaction Report Register/Log has been set up by FCL.

7.2 Applicable Internal Controls

7.2.1 Customer Identification

(a) Pursuant to Regulation 3(1) of the FIAML Regulations, FCL shall identify and verify the identity of all customers, regardless of whether they are permanent or occasional, and verify their identity.

(b) Failure to identify and verify customers as per (a) above constitutes an offence under the FIAMLA and the staff members of FCL shall discharge of their responsibilities in this regard by making an internal suspicious transaction report or disclosure to the MLRO and to the DMLRO in the absence of the MLRO, who shall then do the needful pursuant to section 14 of the FIAMLA.

(c) FCL has in place clear, documented procedures governing how it shall identify and verify the identity of its applicants for business and existing customers on a risk based approach (including

identifying and verifying the identity of any connected individuals such as beneficial owners and controllers of the applicant).

(d) FCL has also established procedures in place to determine whether or not an applicant for business is acting or intending to act for a third party.

(e) If FCL is unable to determine whether the applicant is acting for a third party or not as per (d) above, the MLRO/DMLRO shall make a suspicious transaction report or disclosure under section 14 of the FIAMLA to the FIU.

(f) FCL shall retain the CDD documents as part of its records and in accordance with its Records Keeping Procedures.

The responsibility for applying and monitoring the daily operation of FCL's AML/ CFT controls lies with the MLRO. The MLRO would report to FCL's board thereof of any material breaches of this Manual and of the AML/ CFT laws, regulations, codes and guidelines.

The MLRO shall make annual or other periodic reports (as the MLRO deems fit) to the board thereof on the adequacy/shortcomings of FCL's AML/CFT controls, including making a report on the number of internal disclosures submitted to him/ her, the number of external disclosures made and make recommendations on any remedial action he/ she considers necessary to make FCL fully compliant with this Manual, the relevant AML/ CFT laws, regulations, codes and guidelines.

7.2.2 Transactions Scrutiny & Monitoring

Reasonable steps will be taken to allow the identification of suspicious transactions. In the recognition of suspicious transactions, employees should be particularly aware of two important elements:

1. The usual nature of the customer's business.
2. The usual type of business conducted by the customer's entity.

Suspicions should arise where the two above mentioned components do not match, i.e where the activity is 'unusual'. For ease of guidance, non-exhaustive lists of what may constitute a suspicious transaction and potential red flags of ML and TF activities are provided under Appendices 5 & 6 respectively of this Manual.

In accordance with Regulation 28(1) of the FIAML Regulations, any suspicious activity or reasonable ground to suspect that a transaction is suspicious in the course of a business relationship or occasional transaction, must entail:

(a) EDD measures in accordance with Regulation 12 of the FIAML Regulations and the Compliance Manual
(b) appropriate scrutiny of the activity and
(c) an internal disclosure in accordance with the procedures established under Regulation 27 of the FIAML Regulations.

Where any unusual activity in the course of a business relationship or occasional transaction is noticed, appropriate scrutiny of the activity shall be performed followed by (a) above and consider whether to make an internal disclosure as per (c) above.

To note that the above reporting procedures shall also apply to prospective customers and proposed transactions that were attempted but did not take place.

7.3 Internal & External Disclosures

7.3.1 Internal Disclosure

The MLRO must ensure that all staff members, managers and directors are aware that:

(a) If they believe there is an unusual activity or they become suspicious of a particular customer or transaction, they must report the matter to the MLRO immediately by submitting an Internal Suspicious Transaction Report, template of which is provided under Appendix 7 of this Manual.

(b) Likewise, they must inform the MLRO, or Deputy MLRO in the absence of the latter, of any Listed Party or Designated Party identified *(Please refer to Paragraph 7.6 hereunder for more details on Listed or Designated Party)* .

(c) They must not contact the FIU. The MLRO is the only person allowed to contact the FIU.

(d) They do not have to be certain; suspicion that a transaction(s) relate to criminal activity is sufficient.

(e) If they have suspicion and fail to report them, they are committing a criminal offence and may be liable to disciplinary action for gross misconduct.

(f) They should not inform the customer of their suspicion and of any internal disclosure or reporting made.

(g) Unless instructed otherwise, they should continue dealing with the customer in the normal way.

On receipt of the internal reporting of the unusual / suspicious activity or of the Listed Party or Designated Party, the MLRO or Deputy MLRO will acknowledge receipt and at the same time, provide a reminder of the obligation to do nothing that might prejudice enquiries, such as tipping off the customer(s) or any other third party.

The MLRO or Deputy MLRO must then review the internal disclosure, information / documents received and any other information / documents, as may be necessary, to assess whether an external disclosure need to be made to the FIU (and the NSS and the FSC in the case of a Listed Party or Designated Party).

7.3.2 External Disclosure

The MLRO/DMLRO shall make an external disclosure through the GOAML platform, as warranted. He/she has a maximum of five working days from the date the suspicion arose to file a suspicious transaction report with the FIU.

7.3.3 Filing of Suspicious Transaction Reports

(1) Every report under section 14 shall be submitted to the FIU.
(2) Every report shall be in such form as the FIU may approve and shall include the following:
   (a) the identification of the party or parties to the transaction;
   (b) the amount of the transaction, the description of the nature of the transaction and all the circumstances giving rise to the suspicion;
   (c) the business relationship of the suspect to FCL;
   (d) where the suspect is an insider, any information as to whether the suspect is still affiliated with FCL;
   (e) any voluntary statement as to the origin, source or destination of the proceeds;
   (f) the impact of the suspicious activity on the financial soundness of FCL; and
   (g) the names of all the officers, employees or agents dealing with the transaction.

Details of the suspicious transaction shall be reported to the Board, and decisions in connection with the customer shall be made by the Board, without tipping off the customer.

7.3.4 Register of Internal & External Suspicious Transaction Reports/Disclosures

The MLRO/DMLRO shall keep a register of internal and external (suspicious transaction) reports/ disclosures received / made. As required by Regulation 30(1)(a) of the FIAML Regulations, the register of all ML/TF internal disclosures (including Listed Parties Designated Parties) made to the MLRO or Deputy MLRO must include details of:

(a) the date the report was made;
(b) the person who made the report;
(c) whether the report was made to the MLRO or Deputy MLRO; and
(d) information to allow the papers and relevant documentation to be located.

Pursuant to Regulation 30(2) of the FIAML Regulations, the registers of internal and external disclosures may be contained in a single document if the details included in the registers can be presented separately for internal and external disclosures upon request by a competent authority.

7.4 Tipping Off

Any staff member must avoid exposing him/herself to tipping-off. They should always make an internal disclosure to the MLRO whenever they have reasonable grounds for suspicion.

Accordingly, the concept of tipping-off is somewhat different for the MLRO who has to guide the relevant people in how to deal with the customer from this point onwards. In this respect, the MLRO shall keep a careful record of all his deliberations and decisions for necessary audit trails, as may be required.

7.4.1 How to Avoid Tipping Off

The following guidance on how to avoid tipping off the customer is to be followed by all employees within FCL if any disclosure is made:

(a) In accordance with section 16(1) of the FIAMLA, no person directly or indirectly involved in the reporting of a suspicious transaction shall inform any person involved in the transaction or an unauthorised third party that the transaction has been reported or that information has been supplied to the FIU pursuant to a request made under section 13(2) or (3) of the FIAMLA.

(b) Reasonable enquiries of a customer, conducted in a discreet manner, regarding the background to a transaction or activity which has given rise to the suspicion is prudent practice, forms an integral part of CDD and on-going monitoring, but should not give rise to tipping off.

(c) If an employee suspects that CDD will tip off the customer, the employee should stop conducting CDD and instead FCL should immediately file an STR with the FIU.

(d) The law does not direct FCL to stop providing designated services to or terminate a business relationship with, a customer, even if the reporting entity has formed a suspicion about that particular customer. FCL's management, together with the MLRO, must determine whether to terminate the relationship with the customer based on its risk-assessment, procedures and controls.

(e) If FCL decides to terminate the business relationship with the customer, no officer must disclose to the customer that suspicion has been formed and/or communicated to the FIU.

7.5 Records Keeping of Disclosures

a. FCL shall keep and maintain all necessary records relating to transactions in such a form which enables the prompt reconstruction of each individual transaction.

b. FCL shall ensure that all CDD information and transaction records are kept in such a manner that they are swiftly made available to the FIU or any relevant regulatory body or supervisory authority upon request.

c. Similarly, the MLRO/DMLRO shall keep records of the actions taken to obtain the CDD and transaction information as well as difficulties encountered (if any) during the verification process.

d. Where FCL is responding to a request under section 13(2) of the FIAMLA or to a request from any relevant competent authority, it shall be able to provide for each transaction record –
   i. the full name of the party making a payment; and
   ii. the full name of the party receiving a payment.

e. A Suspicious Transaction Report Log/Register shall be maintained by the MLRO/DMLRO. The aforesaid Log/Register shall also include records of all names matched reported to the NSS, the FIU and the FSC together with relevant information.

7.6 Reporting under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019

FCL takes note of the enactment of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (hereinafter referred to as the "Act" for the purpose of this policy). Through this policy, FCL establishes its procedures and internal controls in accordance with section 41 of the Act to ensure that it shall discharge of all its obligations and duties arising under the Act.

7.6.1 Reporting Procedures

FCL is required to regularly consult the United Nations Security Council Consolidated List accessible at https://the_Company.un.org/securitycouncil/content/un-sc-consolidated-list , particularly whenever updated by the NSS established under section 7 of the Act, and also regularly consult the newspapers for any notice which may be issued by the NSS.

Where a party is listed as a Listed Party or Designated Party, FCL shall proceed as follows:

(a) FCL must immediately (i.e. without delay and not later than 24 hours) verify whether the details of the Listed Party or Designated Party match with the particulars of any of its customer;

(b) If there is a positive match, FCL must identify whether the customer owns any funds or other assets as defined under section 2 of the Act in Mauritius (see Glossary also), including the funds or other assets mentioned in section 23(1) of the Act;

(c) Whether funds or other assets are identified or not, FCL shall make a report to the FSC;

(d) FCL shall adhere to section 23(4) of the Act whereby any person who holds, controls or has in his custody or possession any funds or other assets of a Listed Party or Designated Party must, not later than 24 hours of any notice issued under section 18(1) of the Act, notify the NSS in writing of:

(i) details of the funds or other assets against which action was taken in accordance with the prohibition to deal with the funds or other assets of a Listed Party or Designated Party;
(ii) the name and address of the Listed Party or Designated Party;
(iii) details of any attempted transaction involving the funds or other assets, including inter-alia,
- the name and address of the sender;
- the name and address of the intended recipient;
- the purpose of the attempted transaction;
- the origin of the funds or other assets; and
- where the funds or other assets were intended to be sent.

(e) A nil report must be submitted to the above authorities if no funds or other assets are identified;

(f) Additionally, FCL must immediately submit to the FIU in accordance with section 14 of the FIAMLA, any information relating to a Listed Party or Designated Party which is known to it.

7.6.2 Lapse of Freezing Order or Prohibition

Pursuant to section 34 of the Act, where the name of a Designated or Listed Party is removed from the list of Designated and Listed Parties from the relevant United Nations Sanctions List, FCL shall immediately unfreeze the funds or other assets of the Designated or Listed Party which it holds, controls or has in its custody or possession.

7.6.3 Rights of bona fide third parties regarding freezing order

Pursuant to section 28 (5) of the Act, where FCL holds, controls or has in his custody or possession funds or other assets of a bona fide third party, it shall immediately comply with an application granted under section 28 (3) of the Act.

7.6.4 Rights of bona fide third parties regarding prohibition

Pursuant to section 29 (5) of the Act, where FCL holds, controls or has in his custody or possession funds or other assets of a bona fide third party, it shall immediately comply with an application granted under section 29 (3) of the Act.

7.6.5 Legal Sanctions for Dealing with Funds or Assets of Listed or Designated Parties

It is prohibited to deal with funds or assets of Listed or Designated Parties and section 23(5) of the Act provides that any person who fails to comply with the Act in this regard shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees or twice the amount of the value of the funds or other assets, whichever is greater, and to imprisonment for a term of not less than 3 years.

7.6.6 Internal Sanctions for Non-Compliance with this Policy

FCL shall view any non-compliance with this policy as a breach to its internal policy and the sanction shall be commensurate with the breach committed and sanctioned accordingly.

7.6.7 Legal Sanctions for Non-Compliance with the Act

Any person who contravenes the Act shall commit an offence and shall, on conviction, be liable, where no specific penalty is provided, to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 10 years.

8.0 TRAINING, DEVELOPMENT & EMPLOYEE SCREENING

8.1 Introduction

FCL is committed to ensuring that all the employees including the board members and senior management, are sufficiently trained on an on-going basis on the applicable AML/ CFT regulatory framework.

8.2 Obligations

FCL is required to provide all its directors, officers and employees with on-going AML and CFT training to ensure that they remain fully aware of its procedures and the current regulatory and legislative regimes, in order to:

(i) assist them in recognizing transactions and actions that may be linked to ML or TF; and

(ii) instruct them on the procedures to be followed where any links have been identified under (i) above.

8.3 Board Oversight

The board is aware of the obligations of FCL in relation to continuous employee screening and training.

FCL must provide basic AML/CFT training to all employees at least every year and it will ensure that the training provided to officers and employees is comprehensive and ongoing so that the officers and employees are aware of money laundering and terrorist financing, the associated risks and vulnerabilities of FCL, and their corresponding obligations.

FCL will establish and maintain mechanisms to measure the effectiveness of the AML/CFT training provided to the relevant employees on a risk-based approach.

The board of FCL will ensure that training is provided with adequate information on a sufficiently regular basis in order to satisfy itself that its employees and officers are suitably trained to fulfil their personal and corporate responsibilities.

FCL's training and awareness arrangements include the following:

- Upon joining FCL, all personnel are provided with a copy of this Manual;
- Any subsequent revised versions of the Manual will be circulated to all personnel;
- Personnel must provide a signed undertaking confirming understanding of and adherence to the procedures contained herein, both upon joining FCL;
- AML/CFT training is provided as part of FCL's induction;
- Periodic training is provided to all personnel, based upon changes to FCL's AML/CFT risk and material changes to the regulatory or legislative regime (at a minimum training will be arranged annually),

- Periodic and more frequent training is to be provided to meet all requirements of the FIAMLA Regulations if new legislations or significant changes to the existing AML/CFT framework are introduced, or where there have been significant technological developments within the organization or when new products, services or practices are being introduced;
- The measures to be taken if anyone within FCL believes that performing the CDD process will tip off any customer; and
- An evaluation or assessment / exam at the end of each training programme to ensure understanding by attendees of the content of the training programme as well as the scope of their responsibilities.

In accordance with Regulation 22(1)(c) of FIAMLA Regulations 2018, the ongoing training provided by FCL shall cover:

(a) the FIAMLA, FIAML Regulations, any AML/CFT Code issued by the FSC and the Handbook;
(b) the implications of non-compliance by employees to requirements of FIAMLA, FIAML Regulations, any AML/CFT Code issued by the FSC and the Handbook; and
(c) FCL's policies, procedures and controls for the purposes of foreseeing, preventing and detecting ML and TF.

8.4 Screening Requirements

FCL gives consideration to the following principles prior to, and/or at the time of, recruitment:

(a) obtaining and confirming details of employment history, qualifications and professional memberships;

(b) obtaining and confirming appropriate references;

(c) obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;

(d) obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective employee's criminal record; and

(e) screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

FCL will also conduct periodic ongoing checks of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions., where deemed necessary.

8.5 Content of Training

FCL will ensure that the ongoing training provided to directors, officers and employees covers, to a minimum:

- the requirements for the internal and external disclosing of suspicion;
- the criminal and regulatory sanctions in place, both in respect of the liability of FCL and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of FCL;

- the identity and responsibilities of the MLRO, Compliance Officer and DMLRO;
- dealing with business relationships or occasional transactions subject to an internal disclosure, including managing the risk of tipping off and handling questions from customers;
- those aspects of FCL's business deemed to pose the greatest ML and TF risks, together with the principal vulnerabilities of the products and services offered by FCL, including any new products, services or delivery channels and any technological developments;
- new developments in ML and TF, including information on current techniques, methods, trends and typologies;
- FCL's policies, procedures and controls surrounding risk and risk awareness, particularly in relation to the application of CDD measures and the management of high risk and existing business relationships;
- the identification and examination of unusual transactions or activity outside of that expected for a customer;
- the nature of terrorism funding and terrorist activity in order that employees are alert to transactions or activity that might be terrorist-related;
- the vulnerabilities of FCL to financial misuse by PEPs, including the effective identification of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs; and
- UN, EU and other sanctions and FCL's controls to identify and handle natural persons, legal persons and other entities subject to sanction.

Some categories of FCL's employees will receive additional and specialized training according to their roles. FCL will identify employees who, in view of their particular responsibilities within FCL, will receive additional and ongoing training, appropriate to their roles, as detailed hereunder:

(a) The Board and Senior Management Training

The Board and Senior Management must be provided with adequate training to ensure they have the required knowledge to assess the adequacy and effectiveness of policies, procedures and controls to counter the risk of ML and TF within FCL.

The additional training provided to the Board and Senior Management must include, at least, a clear explanation and understanding of:

- offences and penalties arising for non-reporting or for assisting money launderers or those involved in terrorist financing;
- requirements for CDD including verification of identity and retention of records; and
- the application of FCL's risk-based strategy and procedures.

(b) The MLRO and The DMLRO Training

The MLRO and the DMLRO should be provided with in depth training on all aspects of the prevention and detection of ML/TF, including, but not limited to:

i. AML/CFT legislative and regulatory requirements;
ii. the international standards and requirements on which the Mauritius' strategy is based, namely the FATF 40 Recommendations and ML/TF typology reports that are relevant to their business;
iii. the identification and management of ML/TF risk;
iv. the design and implementation of internal systems of AML/CFT control;
v. the design and implementation of AML/CFT compliance testing and monitoring programs;

vi. the identification and handling of suspicious activity and arrangements and suspicious attempted activity and arrangements;
vii. the money laundering and terrorist financing vulnerabilities of relevant services and products;
viii. the handling and validation of internal disclosures;
ix. the process of submitting an external disclosure;
x. liaising with law enforcement agencies;
xi. money laundering and terrorist financing trends and typologies; and
xii. managing the risk of tipping off.

(c) The Compliance Officer Training

Given the responsibility of the Compliance Officer for ensuring the continued compliance of FCL with the requirements of FIAMLA and FIAMLA Regulations 2018 and for having an overall oversight of the program for AML/CFT amongst others, the Compliance Officer should be provided with in depth training on all aspects of the prevention and detection of ML/TF, including, but not limited to, addressing the monitoring and testing of compliance systems and controls (including details of FCL's policies and procedures) in place to prevent and detect ML and TF.

9.0 RECORDS KEEPING

9.1 Records Keeping Obligations

In accordance with section 190(2) of the Companies Act 2001, FCL shall keep its own office records and those of its clients for a period of seven (7) years as required under the Companies Act 2001, Financial Services Act 2007, the Financial Intelligence and Anti Money Laundering Act 2002, the Handbook and relevant Codes, Guidelines and laws.

FCL shall maintain records as detailed hereunder during and after the course of the business relationship, either in the form of original documents or copies:

- All records obtained through CDD measures, including account files, business correspondences and copies of all documents evidencing the identity of customers and beneficial owners, and records and the results of any analysis/assessment undertaken in accordance with the FIAMLA, should be maintained for a period of at least seven years after the business relationship has ended.

- Where copies of the original identification documents (passports, national ID or any acceptable form of identification) are maintained, these copies shall be duly certified in accordance with the Company's relevant policy and requisite laws in this regard.

- Sufficient records shall be kept to demonstrate that the CDD measures are appropriate in view of the risk of ML/TF.

- Records on transactions - both domestic and international - that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders, which shall be maintained for a period of seven years after the completion of the transaction.

- Transaction records maintained must enable adequate identification of the nature and date of the transaction, who initiated the transaction (instructions can have been given through various means – emails, regular instructions, etc), the type and amount of currency, the type and number of any account with the financial institution, and the name and address of the financial institution and the responsible officer, employee or agent. Correspondence records must be sufficiently detailed to enable a transaction to be readily reconstructed at any time.

- Copies of all suspicious transaction reports (Internal and External disclosure reports) made, including any accompanying and supporting documentation, which shall be maintained for a period of at least seven years from the date the report was made.

  Notwithstanding the above, where the Company is aware that a request for information or an enquiry is being conducted by a competent authority, the Company shall retain the relevant records for as long as required by the relevant authority.

- Accounting records/reports of each customer during the course of the relationship, including its own accounting records and reports and/or any audit report of the different functions of FCL, shall be maintained for a period of at least seven years from the date the report was made.

- Customer transaction records must provide a clear and comprehensive transaction history of incoming and outgoing funds or assets. The following information should be maintained for every transaction carried out in the course of a business relationship or occasional transaction:

  (i) the name and address of the customer, beneficial owner(s), parties involved in the transaction;
  (ii) if a monetary transaction, the kind of currency and the amount;
  (iii) if the transaction involves a customer's account, the number, name or other identifier for the account;
  (iv) the date of the transaction;
  (v) the details of the counterparty, including account details;
  (vi) the nature of the transaction;
  (vii) details of the transaction;
  (viii) correspondence records must be sufficiently detailed to enable a transaction to be readily reconstructed at any time;
  (ix) In the case of negotiable instruments other than currency, records must include particulars of the name of the drawer and the payee (if any), the financial institution on which it was drawn, the amount, date, and number (if any) of the instrument, and any endorsement details.

- Similarly, FCL shall retain documentation on reasons why it applied simplified as compared to standard or enhanced due diligence measures; and on the results of its risk assessment framework.

  In this respect, clear documentation must be prepared and retained to ensure that the board and senior management can demonstrate their compliance with the requirements of section 17 of the FIAMLA (relating to Risk Assessment).

- FCL shall also maintain records of all AML/CFT training delivered to employees. These records must include:

  (i) the dates on which the training was provided;
  (ii) the nature of the training, including its content and mode of delivery; and
  (iii) the names of the employees who received the training.

- Additionally, records shall include any assessment / audit carried out and all logs maintained by FCL.

All records, including inter-alia records of customer identification and verification, must be kept in such a manner that they can be retrieved quickly and without delay.

It is also important that all records held electronically are legible and in a usable filing system, so that they can be retrieved / found without undue delay and produced on a timely basis especially where the originals are not to be retained.

All information regarding the customer's account and instruction are strictly confidential. No statement of account, confirmation of transaction or any other communications are addressed and mailed to other person without the prior written authorization of the customer.

The documents of FCL's customers are stored in both physical and electronic form. Physical documents are kept in filing cabinets which are locked when left unattended. Access to these filing areas is restricted to AFPL's authorized persons only.

AFPL has implemented IT policies to ensure that storage of customers' electronic data or transactions are secured. All computers and laptops containing data are password and virus protected.

10.0 INDEPENDENT AML CFT AUDIT

10.1 Introduction

FCL considers that an AML/CFT independent audit is deemed important for an effective compliance and AML/CFT programme, especially acting as the final line of defence within the organization.

10.2 Scope of Independent Audit

While it is a verification of the AML/CFT risks faced by FCL, the scope of the independent audit exercise is to test FCL's compliance in the following areas using a risk based approach:

a. AML/CFT policies and procedures.
b. Internal Risk Assessment.
c. Risk Assessment on the use of third-party service providers (Outsourcing).
d. CO and MLRO functions and effectiveness.
e. Implementation and Effectiveness of Mitigating Controls, including customer due diligence and enhanced measures.
f. AML/CFT Training.
g. Record Keeping Obligations.
h. Targeted Financial Sanctions.
i. Suspicious Transaction Monitoring and Reporting.
j. The reliability of processes (automated or manual) with regard to the implementation of the AML/CFT programme

10.3 Selection of the Audit Professional

The person or firm conducting the audit – ("the Audit Professional") should be independent and must not be involved in the development of FCL's AML/CFT risk assessment or the establishment, implementation and maintenance of its AML/CFT programme.

The Audit Professional should have the necessary skills, qualification and experience of the audit process, have a proper understanding of the AML/CFT regulatory framework and sufficient knowledge of FCL's industry.

The Audit Professional should provide quality findings and recommendations so that FCL can use same to improve upon deficient areas.

10.4 Assessment of Independence of the Audit Professional

While assessing the independence of the Audit Professional, the following factors shall be considered by FCL:

- FCL must be satisfied and able to demonstrate that the latter is adequately independent from the area of the business function responsible for risk assessment and AML/CFT programme, and ensure that there are no conflicts of interest.
- The independent audit may be conducted by an in-house audit professional not involved in the development and implementation of the AML/CFT programme or outsourced to external accountants or independent consultants duly regulated by relevant competent authorities.
- When sourcing an external audit professional to conduct the audit, FCL should conduct some level of due diligence to confirm that the proposed or selected professional candidate has the requisite competence.
- The criteria considered when assessing the independence and relevant experience of the external audit professional to effectively perform the audit, should be properly documented and shall be made available to the Commission upon request.

10.5 Frequency of the Independent Audit

The frequency of the independent audit is determined by considering FCL's size, nature, context, complexity and internal risk assessment.

FCL has determined that the independent audit shall be conducted on a yearly basis until such time it is comfortable that the policies, procedures, processes, controls and systems are being adhered to diligently and updated where it shall review the frequency of the independent audit.

10.6 Audit Outcome, Report & Recommendations

Upon completion of the independent audit, the Independent Professional shall submit a signed report to ensure that the audit programme:

a. covers all relevant components of the compliance programme as required under FIAMLA and relevant regulations;
b. was adequate and effective throughout a specified period; and
c. identifies areas where FCL did not meet the minimum legal or regulatory standards, and includes actions that are required to rectify non-compliance as well as identifying areas for recommended changes in behaviour and practice to improve the effectiveness of the AML/CFT programme's implementation. This includes an indication of where there are potential failings and a recommended course of action.

FCL acknowledges that a key element of the whole audit process is effective follow-up.

Failure to address recommendations and findings of previous audits should be red flagged to the board and will be in any regulatory inspection.

The findings of the independent audit report, highlighting recommendations and deficiencies, should be reported to senior management and to the board.

It is the responsibility of the board of FCL to take appropriate corrective actions to remediate any issues identified in the independent audit report within the specified timelines.

10.7 Filing with the FSC

While FCL is not required to file the independent audit report with the FSC periodically, it shall file same for a specified period upon request of the FSC.

In this respect, FCL shall duly document and make available to the FSC upon request all independent audit documentation, including work plan, audit scope, transaction testing among others.

11.0 RECOURSE TO THIRD PARTIES

FCL may have recourse to third parties for:

- Introduction of customers/business to FCL (case of the third-party introduction); or
- To avail of the service offered by an external service provider (case of outsourcing).

In both of the above cases, FCL remains fully responsible for implementation of its due diligence obligations.

11.1 Business Introducers

Though FCL may rely on third parties to introduce customers/business to FCL, FCL shall undertake CDD on these clients and will not merely rely on eligible introducer certificates.

Business introducers shall be carefully assessed to ascertain whether they are “fit and proper”. FCL will undertake CDD on the introducer and the introduced clients.

11.2 Outsourcing

It is understood that the services outsourced to a third parties are considered to be carried out by FCL itself and FCL shall be fully responsible for such activities. FCL should therefore conduct appropriate due diligence before appointing a service provider to whom any activity might be outsourced.

Whenever a service is outsourced to a third party, FCL will:

- assess the risks presented in outsourcing the service, its reliability and its compatibility with FCL procedures.
- ensure that the external service provider has a backup solution to ensure the continuity of the service or, failing that, to dispose of it himself.
- ensure that where a failure in the performance of the outsourced company is detected, the following must be ascertained:
  - continuing compliance with the conditions of their authorisation or its other obligations;
  - financial performance; and
  - the soundness or continuity of FCL services and activities.

The terms and conditions of the outsourcing are defined in the contract concluded between FCL and the external service provider. In case using a technological solution developed by a third party, this contract provides for the information of co-contracting financial organizations in the event of modification of the tool (e.g., functionalities, algorithms in place, sources consulted using this tool, etc.) as well as the prior collection of their consent.

12.0 ANTI BRIBERY AND CORRPTION POLICY

12.1 Introduction

One of the Company's core values is to uphold responsible and fair business practices. It is committed to promoting and maintaining the highest level of ethical standards in relation to all of its business activities. Its reputation for maintaining lawful business practices is of paramount importance and this Policy is designed to preserve these values. The Company therefore has a zero tolerance policy towards bribery and corruption and is committed to acting fairly and with integrity in all of its business dealings and relationships and implementing and enforcing effective systems to counter bribery.

12.2 Purpose and Scope

This Policy sets out the Company's position on any form of bribery and corruption and provides guidelines aimed at:

- Ensuring compliance with anti-bribery laws, rules and regulations, not just within Mauritius but in any other country within which the Company may carry out its business or in relation to which its business may be connected.

- Enabling employees and persons associated with the Company to understand the risks associated with bribery and to encourage them to be vigilant and effectively recognise, prevent

and report any wrongdoing, whether by themselves or others.

- Providing suitable and secure reporting and communication channels and ensuring that any information that is reported is properly and effectively dealt with.

- Creating and maintaining a rigorous and effective framework for dealing with any suspected instances of bribery or corruption.

This Policy applies to all permanent and temporary employees of the Company (including any of its intermediaries, subsidiaries or associated companies). It also applies to any individual or corporate entity associated with the Company or who performs functions in relation to, or for and on behalf of, the Company, including, but not limited to, directors, casual workers, contractors, consultants, seconded staff, agents, suppliers and sponsors ("associated persons"). All employees and associated persons are expected to adhere to the principles set out in this Policy.

12.3 Legal Obligations

Mauritius legislation on which this Policy is based is the Prevention of Corruption Act 2002 and it applies to the Company's conduct both in Mauritius and abroad. A bribe is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage.

It is an offence in Mauritius to:

- Offer, promise or give a financial or other advantage to another person (i.e. bribe a person), whether within Mauritius or abroad, with the intention of inducing or rewarding improper conduct.
- Request, agree to receive or accept a financial or other advantage (i.e. receive a bribe) for or in relation to improper conduct.
- Bribe a public official domestic or foreign.

One can be held personally liable for any such offence. It is also an offence in Mauritius for an employee or an associated person to bribe another person in the course of doing business intending either to obtain or retain business, or to obtain or retain an advantage in the conduct of business, for the Company. The Company can be liable for this offence where it has failed to prevent such bribery by associated persons. As well as a fine, it could suffer substantial reputational damage.

12.4 Policy Statement

All employees and associated persons are required to:

- Comply with any anti-bribery and anti-corruption legislation that applies in any jurisdiction in any part of the world in which they might be expected to conduct business.
- Act honestly, responsibly and with integrity.
- Safeguard and uphold the Company's core values by operating in an ethical, professional and lawful manner at all times.

Bribery of any kind is strictly prohibited. Under no circumstances should any provision be made, money set aside or accounts created for the purposes of facilitating the payment or receipt of a bribe.

The Company recognises that industry practices may vary from country to country or from culture to culture. What is considered unacceptable in one place may be normal or usual practice in another. Nevertheless, a strict adherence to the guidelines set out in this Policy is expected of all employees and associated persons at all times. If in doubt as to what might amount to bribery or what might constitute a breach of this Policy, refer the matter to your head of department or to the Group Human Resource Director or to the Company' General Manager or Managing Director.
For the Company's rules and procedures in relation to the receipt of business gifts from third parties and corporate hospitality offered to or received from third parties, please refer to the Company's Gifts from Clients/Suppliers Policy. They form part of the Company's zero tolerance policy towards bribery and they should be read in conjunction with this Policy.

The giving of business gifts to clients, customers, contractors and suppliers is not prohibited provided the following requirements are met:

- The gift is not made with the intention of influencing a third party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage.
- It complies with local laws.
- It is given in the Company's name, not in the giver's personal name.
- It does not include cash or a cash equivalent (such as gift vouchers)
- It is of an appropriate and reasonable type and value and given at an appropriate time.
- It is given openly, not secretly.
- It is approved in advance by a director of the Company.

In summary, it is not acceptable to give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given, or to accept a payment, gift or hospitality from a third party that you know or suspect is offered or provided with the expectation that it will obtain a business advantage for them.

Any payment or gift to a public official or other person to secure or accelerate the prompt or proper performance of a routine government procedure or process, otherwise known as a "facilitation payment", is also strictly prohibited.

12.5 Responsibilities and Reporting Procedure

It is the contractual duty and responsibility of all employees and associated persons to take whatever reasonable steps are necessary to ensure compliance with this Policy and to prevent, detect and report any suspected bribery or corruption in accordance with the procedure set out in this Policy. You must immediately disclose to the Company any knowledge or suspicion you may have that you, or any other employee or associated person, has plans to offer, promise or give a bribe or to request, agree to receive or accept a bribe in connection with the business of the Company. For the avoidance of doubt, this includes reporting your own wrongdoing. The duty to prevent, detect and report any incident of bribery and any potential risks rests not only with the directors of the Company but equally to all employees and associated persons.

The Company encourages all employees and associated persons to be vigilant and to report any unlawful conduct, suspicions or concerns promptly and without undue delay so that investigation may proceed and any action can be taken expeditiously. In the event that you wish to report an instance or suspected instance of bribery, you should report same in writing to the Compliance Officer or to the Managing Director in case the suspected matter relates to the Compliance Officer. Confidentiality will be maintained during the investigation to the extent that this is practical and appropriate in the circumstances. The Company is committed to taking appropriate action against bribery and corruption. This could include either reporting the matter to an appropriate external government department, regulatory agency or the police and/or taking internal disciplinary action against relevant employees and/or terminating contracts with associated persons.

The Company will support anyone who raises genuine concerns in good faith under this Policy, even if they turn out to be mistaken. It is also committed to ensuring nobody suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or corruption offence has taken place or may take place in the future.

12.6 Record Keeping

All accounts, receipts, invoices and other documents and records relating to dealings with third parties must be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off the record" to facilitate or conceal improper payments.

12.7 Sanctions for breach

A breach of any of the provisions of this Policy will constitute a disciplinary offence and will be dealt with in accordance with the Company's disciplinary procedure. Depending on the gravity of the offence, it may be treated as gross misconduct and could render the employee liable to summary dismissal.

As far as associated persons are concerned, a breach of this Policy could lead to the suspension or termination of any relevant contract, sub-contract or other agreement.

12.8 Monitoring Compliance

The Company's Compliance Officer has lead responsibility for ensuring compliance with this Policy and will review its contents on a regular basis. They will be responsible for monitoring its effectiveness and will provide regular reports in this regard to the directors of the Company who have overall responsibility for ensuring this Policy complies with the Company's legal and ethical obligations.

12.9 Training

The Company will provide training to all employees to help them understand their duties and responsibilities under this Policy. The Company's zero tolerance approach to bribery will also be communicated to all business partners at the outset of the business relationship with them and as appropriate thereafter.

13.0 TERMINATION OF BUSINESS RELATIONSHIP

FCL will not carry out any transaction or establish a business relationship, when it is unable to identify and verify the identity of the client (occasional or in a business relationship), and where applicable, of the connected parties and the beneficial owner; or to obtain the elements of knowledge of the business relationship necessary for the exercise of the constant vigilance.

In application of the aforementioned provisions, FCL will put an end to a previously established business relationship when it is unable to:

- either, to verify the identity of the customer, and where applicable of the connected parties and beneficial owner, or to collect elements necessary for knowledge of the business relationship, in the event that the implementation of these procedures was postponed due to the low ML-FT risk and the need to not interrupt the normal exercise of the activity of the financial institution;
- or, to carry out a new identification and verification of the customer's identity, and if applicable, from the beneficial owner, when the information previously obtained is no longer accurate or relevant;
- or, to update knowledge of the business relationship on relevant elements and necessary for the exercise of constant vigilance;
- breach of any terms and conditions by the customer (example none payment of fees).

In addition, FCL will also consider whether an STR needs to be filed.

When closing an account in application of these provisions, FCL will try to comply with a 2 months notice period. FCL may suspend such accounts until they are closed.

14.0 LIST OF ACRONYMS

AML	**Anti-Money Laundering**
AML/CFT	**Anti-Money Laundering and Combating the Financing of Terrorism & Proliferation**
BRA	**Business Risk Assessment**
CDD	**Customer Due Diligence**
CFT	**Countering Financing of Terrorism**
CO	**Compliance Officer**
CRA	**Customer Risk Assessment**
DMLRO	**Deputy Money Laundering Reporting Officer**
DNFBPs	**Designated Non-Financial Businesses and Professions**
EDD	**Enhanced Due Diligence**
ESAAMLG	**Eastern and Southern Africa Anti-Money Laundering Group**
FATF	**Financial Action Task Force**
FIAMLA	**Financial Intelligence and Anti-Money Laundering Act 2002**
FIAML Regulations	**Financial Intelligence and Anti-Money Laundering Regulations 2018**
FIU	**Financial Intelligence Unit**
FSA	**Financial Services Act 2007**
FSC	**Financial Services Commission**
ML	**Money Laundering**
MLRO	**Money Laundering Reporting Officer**
NSS	**National Sanctions Secretariat**
PEP	**Politically Exposed Person**
PF	**Proliferation Financing of Weapons of Massive Destruction**
RBA	**Risk Based Approach**
SDD	**Simplified Due Diligence**
STR	**Suspicious Transaction Report**
TF	**Terrorism Financing**

14.0 APPENDICES

14.1 APPENDIX 1

SUMMARY OF OFFENCES UNDER THE FIAMLA AND THE FIAML REGULATIONS

The FIAMLA and FIAML Regulations provide for offences which are related to Money Laundering and Terrorist & Proliferation Financing and related offences. Some of these offences, as applicable to Ashton Financial Partners Ltd and its employees, are listed below for ease of reference:

1. **Money Laundering – Part II - Section 3 (1); (2) and (3) of the FIAMLA**

- Any person who –
  (a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or
  (b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime,

  where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.

- A reporting person fails to take such measures as are reasonably necessary to ensure that neither he, nor any service offered by him, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism shall commit an offence.

- In the FIAMLA, reference to concealing or disguising property which is, or in whole or in part, directly or indirectly, represents, the proceeds of any crime, shall include concealing or disguising its true nature, source, location, disposition, movement or ownership of or rights with respect to it.

2. **Conspiracy to commit the offence of money laundering - Part II - Section 4 of the FIAMLA**

- Without prejudice to section 109 of the Criminal Code (Supplementary) Act, any person who agrees with one or more other persons to commit an offence specified in section 3(1) and (2) shall commit an offence.

3. **Limitation of payment in cash - Part II - Section 5 (1) and (2) of the FIAMLA**

- Notwithstanding section 37 of the Bank of Mauritius Act 2004, but subject to subsection (2), any person who makes or accepts any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency, or such amount as may be prescribed, shall commit an offence.

- Subsection (1) shall not apply to an exempt transaction.

4. Penalty - Part II - Section 8 of the FIAMLA

- Any person who –
  (a) commits an offence under this Part; or
  (b) disposes or otherwise deals with property subject to a forfeiture order under subsection (2),

  shall, on conviction, be liable to a fine not exceeding 10 million rupees and to penal servitude for a term not exceeding 20 years.

  Any property belonging to or in the possession or under the control of any person who is convicted of an offence under this Part shall be deemed, unless the contrary is proved, to be derived from a crime and the Court may, in addition to any penalty imposed, order that the property be forfeited.

  Sections 150, 151 and Part X of the Criminal Procedure Act and the Probation of Offenders Act shall not apply to a conviction under this Part.

5. Dissemination of Information by Director – Part III - Section 13 (8) of the FIAMLA

- Any reporting person or auditor, or any director, employee, agent or legal representative of a reporting person or auditor who –
  (a) fails to supply any information requested by FIU under section 13(2), (3) or (6) by the date specified in the request; or
  (b) falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, any information, document or material which is or is likely to be relevant to a request under section 13(2), (3) or (6),

  shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

6. Reporting of suspicious transaction by reporting person or auditor – Part IV – Section 14(3)

- Where a reporting person or an auditor –
  (a) becomes aware of a suspicious transaction; or
  (b) ought reasonably to have become aware of a suspicious transaction,

  and he fails to make a report to FIU of such transaction not later than 5 working days after the suspicion arose he shall commit an offence and shall, on conviction, be liable to fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

7. Legal consequences of reporting – Part IV - Section 16(3A) of the FIAMLA

- Any person who fails to comply with subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

8. Customer Due Diligence requirements – Part IV - Section 17(C) (6) of the FIAMLA

- Any person who knowingly provides any false or misleading information to a reporting person in connection with CDD requirements under the FIAMLA or any guidelines issued under same shall commit an offence and shall, on conviction, be liable to a fine not exceeding 500, 000 rupees and to imprisonment for a term not exceeding 5 years.

9. Offences relating to obligation to report and keep records and to disclosure of Information prejudicial to a request – Part IV - Section 19 (1) and (2) of the FIAMLA

- Any reporting person or any director, employee, agent or other legal representative of a reporting person, who, knowingly or without reasonable excuse –

  (a) fails to comply with section 17 to 17G;
  (b) destroys or removes any record, register or document which is required under the FIAMLA or any regulations
  (c) facilitates or permits the performance under a false identity of any transaction falling within this Part,

- Any person who –

  (a) falsifies, conceals, destroys or otherwise disposes of or causes or permits the falsification, concealment, destruction or disposal of any information, document or material which is or is likely to be relevant to a request to under the Mutual Assistance in Criminal and Related Matters Act 2003;

  (b) knowing or suspecting that an investigation into a money laundering offence has been or is about to be conducted, divulges that fact or other information to another person whereby the making or execution of a request to under the Mutual Assistance in Criminal and Related Matters Act 2003 is likely to be prejudiced,

  shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

10. Duty to provide information for purpose of conducting risk assessment – Part IV A – Section 19E (4) of the FIAMLA

- Any person who fails to comply with a request made under subsection (2)(b) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

11. Powers of regulatory body – Part IV B – Section 19FA of the FIAMLA

- Any person who fails to provide any information under subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

12. Request for information - Part IV B –Section 19J (4) of the FIAMLA

- Any person who fails to comply with this section shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 2 years.

13. On-site inspections – Part IV B – Section19K (4) and (5) of the FIAMLA

- Any person who –

  (a) intentionally obstructs the regulatory body in the performance of any of its duties under this section; or
  (b) fails, without reasonable excuse, to comply with any direction of the regulatory body in the performance of its duties under this section,

  shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

- Any person who destroys, falsifies, conceals or disposes of, or causes or permits the destruction, falsification, concealment or disposal of, any document, information stored on a computer or other device or other thing that the person knows or ought reasonably to have known is relevant to an on-site inspection or investigation, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

14. Non-compliance with directions – Part IV B – Section 19M (1) and (2) of the FIAMLA

- Any person to whom a direction is given under this Act shall comply with the direction and where he fails to comply with the direction and a time period is specified for compliance, the person shall commit a separate offence for each day on which the direction is not complied with, after the time period for compliance has elapsed, and shall, on conviction, in respect of each offence, be liable to a fine of 5,000 rupees per day.

- A person who knowingly hinders or prevents compliance with a direction given under this Act shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

15. Offences relating to proceeding of Review Panel – Part IV B – Section 19W of the FIAMLA

- Any person who, without reasonable cause –

  (a) fails to attend the Review Panel after having been summoned to do so under section 19U;
  (b) knowingly gives false evidence, or evidence which he knows to be misleading, before the Review Panel; or
  (c) at any hearing of the Review Panel –
    (i) wilfully insults a member;
    (ii) wilfully interrupts or disturbs the proceedings,

shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 3 years.

16. Confidentiality – Part VII – Section 30 (2A) and 3 of the FIAMLA

- Notwithstanding subsection (2), any information disclosed by FIU shall only be disclosed according to the terms and conditions specified in the disclosure.

  Where a person who receives the information disclosed under paragraph (a) fails to comply with those terms and conditions, he shall commit an offence.

  Any person who contravenes this section shall commit an offence and, on conviction, shall be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 3 years.

17. Offence in respect of contravention of the FIAMLA – Part VII – Section 32A of the FIAMLA

- Any person who contravenes the FIAMLA shall commit an offence and shall, on conviction, be liable, where no specific penalty is provided, to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

1. FIAML Regulations 2018 - Regulation 33

- Any person who contravenes these regulations shall commit an offence and shall on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

14.2 APPENDIX 2

POLITICALLY EXPOSED PERSON – (PEP) POLICY

A. INTRODUCTION

A Politically Exposed Person (PEP) is defined by the Financial Action Task Force - ("FATF") as an individual who is or has been entrusted with a prominent public function, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials.

Pursuant to the Financial Intelligence Anti Money Laundering Regulations 2018 – ("FIAML Regulations"), A PEP means a Foreign PEP, a Domestic PEP and an International Organisation PEP.

Due to their position and influence, it is deemed that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing.

The potential risks associated with PEPs warrant the application of additional AML/CFT preventive measures with respect to business relationships with PEPs.

To address these risks, FATF Recommendations require countries, including the Republic of Mauritius, to ensure that financial institutions and designated non-financial businesses and professions (DNFBPs) implement measures to prevent the misuse of the financial system and non-financial businesses and professions by PEPs, and to detect such potential abuse if and when it occurs.

These requirements are preventive (not criminal) in nature and should not be interpreted as stigmatizing PEPs as such being involved in criminal activity. Refusing a business relationship with a PEP simply based on the determination that the customer is a PEP will be contrary to the letter and spirit of FATF Recommendations.

Consistent with the FATF Recommendations and their objective, FCL is statutorily required, pursuant to the FIAML Regulations, to have appropriate risk management systems in place to determine whether customers or beneficial owners are PEPs, or related or connected to PEPs, and, if so, to take additional measures beyond performing normal customer due diligence (CDD) to determine if and when they are doing business with them.

Pursuant to its statutory obligations, FCL has adopted a policy on the acceptance of business relationships with PEPs as well as on the ongoing monitoring of such relationships.

B. DEFINITIONS

For the purpose of this guidance policy, the definitions set out in the FIAML Regulations and the FATF Recommendations apply.

In particular, the following definitions, which do not cover middle ranking or more junior Individuals, apply to this policy:

1. **Domestic PEP** means a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

2. **Foreign PEP** means a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

For ease of understanding, the difference between a Foreign PEP and a Domestic PEP is the country which has entrusted the individual with the prominent public function. Pursuant to the definition of PEPs, other factors, such as country of domicile or nationality, are not relevant in determining the type of PEP, but may be relevant in determining the level of risk of a specific Domestic PEP (as Foreign PEPs are always high risk). Additionally, a Domestic PEP shall be subject to the foreign PEPs requirements if that individual is also a Foreign PEP through another prominent public function in another country.

3. **International Organisation PEP** means a person who is or has been entrusted with a prominent function by an international organisation and includes members of senior management or individuals who have been entrusted with equivalent functions, including directors, deputy directors and members of the board or equivalent functions and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

For the purpose of this policy and pursuant to the FIAML Regulations, **International Organisations** mean an entity established by formal political agreements between their member States that have the status of international treaties, whose existence is recognized by law in their member countries, and they are not treated as resident institutional units of the countries in which they are located.

4. **Close Associate of a PEP** means an individual closely connected to a PEP, either socially or professionally; and includes any other person, as may be specified by a supervisory authority or regulatory body, after consultation with the National Committee.

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

- **<u>Guide to the Scope of Family Members and Close Associates</u>**

  While the FIAML Regulations do not define the scope of the terms *family members* and *close associates of PEPs,* this depends to some extent on the social-economic and cultural structure of the country of the PEP.

  In the absence of the statutory definition of the scope of family members and close associates of PEPs, guidance is sought from the FATF Recommendations as follows:

i. For ***Family Members of a PEP***, this includes such relevant factors as the influence that particular types of family members generally have, and how broad the circle of close family members and dependents tends to be. For example, in some cultures, the number of family members who are close or who have influence may be quite small (*e.g.*, parents, siblings, spouses/partners, and children). In other cultures, grandparents and grandchildren might also be included, while in others, the circle of family members may be broader, and extend to cousins or even clans.

ii. For ***Close Associates of a PEP***, examples include the following types of relationships:
(Known) (sexual) partners outside the family unit (*e.g.* girlfriends, boyfriends, mistresses); prominent members of the same political party, civil organisation, labour or employee union as the PEP; business partners or associates, especially those that share (beneficial) ownership of legal entities with the PEP, or who are otherwise connected (*e.g.*, through joint membership of a company board). In the case of personal relationships, the social, economic and cultural context may also play a role in determining how close those relationships generally are.

C. THE POLICY

FCL has adopted the following policy on the acceptance of business relationships with PEPs; Close Associates and Family Members of PEPs:

1. FCL shall take reasonable measures to determine whether a customer or beneficial owner is a PEP or a Close Associate / Family Member of a PEP, and then assess the risk of the business relationship.
2. In this respect, FCL has appropriate risk management system in place to determine whether whether a customer or beneficial owner is a PEP or a Close Associate/Family Member of a PEP.
3. FCL shall request relevant information from a new applicant for business and refer to publicly available information to assess whether the customer is a PEP or a Close Associate/Family Member of a PEP. Each customer shall be required to fill in a PEP Declaration Form, as provided below.
4. FCL shall additionally conduct screening checks against national and international PEP lists and databases on each customer.
5. The Screening results and data collected through independent public sources are then compared with the information provided by the customer through the PEP Declaration Form to validate the accuracy of the information in the PEP Declaration Form.
6. Any inaccuracy in information submitted by the customer shall be investigated by FCL without tipping off the customer / applicant for business. Any concealment of material information with the intention to lie or mislead FCL shall result in the immediate rejection of the customer and trigger the making of an external suspicious transaction disclosure under Section 14 of the FIAMLA in accordance with FCL's Internal and External Suspicious Transaction Reporting Policy, as provided in the AML/CFT Manual.
7. Whenever a PEP or Close Associate/ Family Member of a PEP is identified, FCL shall apply EDD to determine whether and when it will establish a business relationship with the PEP or Close Associate/Family Member of the PEP.
8. FCL shall conduct a risk assessment in view of the presence of the PEP or the Close Associate/Family Member of the PEP. The confirmation of PEP or Close Associate/Family Member of a PEP shall automatically risk rate the customer as High Risk.
9. The existing customer shall be required to fill in a PEP Declaration Form.
10. The decision to maintain the business relationship or not shall be reviewed and senior management approval, shall be sought to decide whether to continue or cease such business relationship.
11. In the event the PEP or the Close Associate/Family Member of a PEP has left office, FCL may decide to downgrade the risk category after having assessed the risks associated to the PEP or the Close

Associate/Family Member. The decision to downgrade the risk from "High" to "Medium" or "Low", subject to other applicable risk factors, of such customer during the course of the business relationship shall also be approved by Senior Management on the recommendation of the Governance, Risk and Compliance Committee. Nevertheless, FCL also considers that PEPs can benefit from their former position for years after leaving office and therefore, this risk should be taken into account in the customer's overall risk rating. FCL shall follow the guidance of the FATF with regard to time limit of PEP status, as detailed hereinafter.

12. If an existing customer turns out to become a PEP or is found at a later stage of the business relationship to be Close Associate or Family Member of a PEP, FCL shall take relevant EDD measures when dealing the said customer pending a decision is taken as to whether to cease or otherwise business relationship with the customer.
13. The PEP Register should be filled in with all the necessary information and it should be kept updated.

D. APPLICABLE EDD MEASURES

The EDD measures, in addition to obtaining senior management approval that may be applied are as follows:

1. Obtaining additional information on the customer, such as occupation, volume of assets, information available through publicly or commercially available databases, internet among others, and updating more regularly the identification information of the customer and the beneficial owner, such as updated customer due diligence information.
2. Obtaining additional information on the intended nature of the business relationship.
3. Obtaining information on and taking appropriate and reasonable measures to establish the source of funds and wealth of the customer, the beneficial owner and any underlying principal.
4. Obtaining information on the reasons ofr intended performed transactions.
5. Conducting enhanced monitoring of the business relationship, by increasing number and timing of controls applied, and selecting patterns of transactions that need further scrutiny and setting lower monitoring thresholds for transactions connected with such business relationships.
6. Where applicable, requiring first payment to be carried out through an account in the customer's name with a bank subject to similar standards.
7. Conducting regular review of the customer file, as defined under the Risk Management Policy of FCL and a close monitoring of every instruction/transaction, with the findings of the review being duly documented.

E. GUIDANCE TO TIME LIMIT OF PEP STATUS

A PEP is defined as being someone who has been (but may no longer be) entrusted with a prominent public function. This definition is consistent with a possible open-ended approach (*i.e.*, "once a PEP – could always remain a PEP"). The FATF Recommendations Guidance provides that the handling of a customer who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits.

The risk-based approach requires that FCL assesses the Money Laundering /Terrorist Financing risk of a PEP who is no longer entrusted with a prominent public function and take effective action to mitigate this risk. The potential risk factors are:

- The level of (informal) influence that the individual could still exercise; the seniority of the position that the individual held as a PEP; or
- Whether the individual's previous and current function are linked in any way (*e.g.*, formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

Politically Exposed Person Declaration Form

Please answer the questions/state the information requested below with regards to Politically Exposed Person ("PEP").

1. Do you currently hold or have you been entrusted in the past with a prominent public function (1), or are you a family member (2), or close associate (3) of a PEP?

☐No ☐ Yes - If yes, please specify (functions held, when and for how long, etc...)

_____

_____

Origin of the funds/ wealth

2. If you have answered yes to the question above, the origin of any current, and the expected origin of any future funds/ wealth, must be provided

☐ Business operations ☐ Returns on investments
☐ Loans ☐ Salaries
☐ Inheritance ☐ Other Please specify?

_____

I/We hereby confirm that the above-stated information is correct and complete.

I/We undertake to promptly inform you in writing if there is any change in the status as declared above.

Signature: _____
Customer's/ Principal's name: _____
For and on behalf of
Date:

Definitions relating to the term "Politically Exposed Person":

1) Prominent public function is:

a) Head of State or of Government.
b) Senior Politicians.
c) Senior Government/Judicial/Military Officials.
d) Senior Executives of State-Owned-Corporations,
e) Important Political Party Officials.

2) Family Member of a PEP means an individual related to a PEP either directly through consanguinity, or through marriage or similar civil forms of partnership

3) Close associate of a PEP means an individual closely connected to a PEP, either socially or professionally

14.3 APPENDIX 3
CDD CHECKLIST CDD Checklist

List A for individual

(1)	Personal details including name (including any former names and any aliases), permanent residential address (not a P.O. Box address), date of birth, place of birth and nationality	
(2)	Curriculum vitae (for any promoter, ultimate owner, settlor/contributor, director of financial services provider)	
(3)	Certified true copy of the current valid passports or current valid driving licences or armed forces identity cards or national identity cards	
(4)	A recent original utility bill or recent original bank or credit card statement or recent original bank reference to establish place of residential address	
(5)	Bank reference from a recognized banking institution which has known the person for at least two years (required as an EDD measure or as an additional proof of address)	
(7)	Self-Certification form (FATCA/CRS)	
(9)	eclaration & Evidence of Source of Fund and Wealth	

List B for Company

(1)	Certified true copy of the Certificate of Incorporation or Registration	
(2)	Checking with the relevant companies registry that the company continues to exist - Original Certificate of Good Standing	
(3)	Details of the registered office and place of business	
(4)	Copy of latest audited accounts or corporate profile or signed management accounts where audited accounts are not available	
(5)	List of directors and shareholders – certified true copy of Registers	
(6)	FATCA/CRS Self Certification Form	
(7)	Certified board resolution authorising the person who acts on its behalf (for corporate shareholder only)	

(8)	Declaration & Evidence of Source of Fund and Wealth	

List C for Trusts/Foundations

(1)	Certified true copy of the extract of the trust deed/Foundation Charter	
(2)	Certificate of registration, where applicable	
(3)	Details of registered office and place of business of the trustee/Council Member	
(4)	Complete set of document required on principals of the trust (Trustee, Beneficiaries, Settlor, Protector) as above for individuals or corporate/ Founder, Beneficiaries	
(5)	Declaration & Evidence of Source of Fund and Wealth	

List D for Partnerships

(1)	An original or certified copy of the partnership deed	

(2)	Certificate of registration	
(3)	Good standing of Partnership	
(3)	Copy of the latest report and accounts	
(4)	Confirmation of the nature of the business of the partnership to ensure that it is legitimate.	
(5)	Certified partner resolution authorising the person who acts on its behalf (for shareholder only)	
(6)	Declaration & Evidence of Source of Fund and Wealth	

14.4 APPENDIX 4

GUIDE TO SOURCE OF FUND AND SOURCE OF WEALTH

The Company's customers are required, at the commencement of the business relationship, to formally confirm their Source of Fund and Wealth by way of written Declaration confirming that their funds have not been derived from any criminal activities of any nature whatsoever.

The Company's Customer Acceptance Agreement also contains a section whereby customers confirm that their moneys and assets do not emanate from any criminal activity which is unlawful in their country of origin and specifically that none of the assets were derived from any of the activities characterized as criminal by any applicable legislation against money laundering.

Customers are also required to disclose and confirm their source of funds in respect of the proposed business activities in the Business Plan.

The objective of all above mentioned declarations is to give FCL information on where the income/wealth of the new customers has been generated and ascertain that there is consistency between the information it holds on the customers and the nature of transactions or proposed transactions.

This is in line with our statutory commitment to the domestic and international effort to detect and prevent FCL and financial services in general, being used to launder the proceeds of crime.

- **Source of Fund/Property & Source of Wealth – Definitions**

Pursuant to the its regulatory framework, FCL, in the identification of risk and prevention of money laundering and terrorist and proliferation financing, is required to understand the origin of funds or property underlying a business relationship with its customers.

- The **Source of Fund** is the activity or transaction which generates the funds for a customer.
- The **Source of Wealth** refers to the activities which have generated the total net worth of the customer.

FCL is additionally required to use a risk-based approach and take appropriate measures to establish the source of fund for each applicant for business and when third party funding is involved, it should make further enquiries as to the relationship between the person providing the fund and the applicant for business.

FCL must ensure that there is consistency between the information they hold on the applicant for business and the nature of transactions or proposed transactions.

Where there is any indication of abnormal or potentially suspicious activity within the context of the product or service being provided, FCL must take additional measures to verify the information obtained.

This document should only be used as guidance for understanding the information and verification required to support the application for new business as well as in the course of the business relationship.

Source of Fund & Wealth - Information & Evidential Guide

Hereunder is a list of potential documents/information which we may use to identify, verify and validate the source of fund & wealth of customers.

	Description of Source of Fund & Wealth	Details Required	Documentary evidence required (original or fully certified copy*)
1	**Income-savings from salary** **If self-employed or company shareholder, refer to 8 hereunder**	All of the following: - Salary per annum - Employer's name and address - Nature of business	One of the following: - Pay slip (or bonus payment) from the last three months - Letter from employer confirming salary on letter-headed paper - Bank statements clearly showing receipt of most recent regular salary payment from employer
2	**Maturity or surrender of life policy**	All of the following: - Amount received - Policy provider - Policy number/reference - Date of surrender	One of the following: - Closing statement - Letter confirming surrender from previous investment company paying the claim
3	**Sale of investments & Liquidation of investment portfolio**	All of the following: - Description of shares/units/deposits - Name of seller - How long held - Sale amount - Date funds received	One of the following: - Investment/savings certificates, contract notes, or surrender statements - Bank statement clearly showing receipt of funds and investment company name - Signed letter detailing funds from a regulated accountant on letter-headed paper
4	**Sale of property**	All of the following: - Sold property address - Date of sale - Total sale amount	One of the following: - Letter from Notary on letter head - Copy sale contract
5	**Company Sale**	All of the following: - Name and nature of the company - Date of sale - Total amount - Customer's share	- Signed letter from Notary - Copy of contract of sale, plus bank statement showing proceeds - Copies of media coverage (if applicable) as supporting evidence
6	**Inheritance**	All of the following: - Name of deceased - Date of death - Relationship to customer	One of the following: -Signed letter from Notary or estate trustees on Letter head -The will

		- Date received - Total amount - Notary's details	
7	**Divorce settlement**	All of the following: - Date received - Total amount received - Name of divorced partner	One of the following: - Copy of court order - Attorney's letter
8	**Company profits**	All of the following: - Name and address of company - Incorporation certificate - Nature of company - Amount of annual profit	- Copy of latest audited company accounts - Confirmation of the nature of business activity and turnover, detailed in a letter from a licensed accountant.
9	**Asset (share) exchange**	Please describe the origin and means of wealth generation used to acquire the assets (use this column here as your guide)	If the assets have been held for less than two years: - Provide evidence of the original source of wealth used to acquire the assets
10	**Gift**	All of the following: -Date received -Total amount -Relationship to customer -Letter from donor explaining the reason for the gift and the source of donor's wealth -Certified identification documents for donor -Donor's source of wealth	- Documentary evidence of the donor's source of wealth
11	**Employer paying premium**	All of the following: - Employer letter - Country of incorporation - Incorporation number	All of the following: - Employer letter (confirming what will be paid, that the customer is an employee, and a brief explanation as to why the employer is paying premium) - Certificate of incorporation - Copy of latest audited company accounts
12	**Retirement income**	All of the following: - Retirement date - Details of previous profession/ occupation - Name and address of last (final) employer - Details of pension income source	One of the following: -Pension statement -Letter from a regulated accountant -Letter from Annuity provider -Bank statement showing receipt of latest pension income and name of provider -Savings account statement
13	**Fixed deposit – savings**	All of the following: - Name of institution where savings account is held - Date the account was established - Details of how the savings were	All of the following: - Savings statement - Evidence of account start (letter from account provider or first statement)

		acquired should be provided	We may request additional evidential information, in relation to the origin of the savings held.

***Note:**

Certification of Documents – see rules for certification under 5.10.4

14.5 APPENDIX 5

NON-EXHAUSTIVE LIST OF SUSPICIOUS ACTIVITIES

An unusual or suspicious activity includes, but not limited to, anything that triggers doubt on the identity and/or the good faith of the customer. Situations that are likely to appear unusual include, inter alia:

a. Transactions or instructions which have no apparent legitimate purpose and appear not to have a commercial rationale;
b. Transactions, instructions or activity that involve apparent unnecessary complexity.
c. Where the transaction which is being requested by the customer is out of the ordinary range.
d. Where the size or pattern of transactions is out of line with expectations for a customer.
e. Where the customer is not forthcoming with information about their activities, reason for a transaction, source of funds, CDD documentation among others.
f. Where the customer who has entered into a business relationship and uses the relationship for a single transaction or for only a very short period of time where that was not expected.
g. The extensive use of offshore structures where the customer's needs are inconsistent with the use of such services.
h. Transfers to or from high risk jurisdictions which are not consistent with the customer's expected activity.
i. Unnecessary routing of funds through third party accounts.
j. Unusual investment transactions with no discernible purpose.
k. Extreme urgency in requests from the customer, particularly where they are not concerned by large transfer fees, early repayment fees among others.

The above is a non-exhaustive list of suspicious activities and the latter are likely to be detected during ongoing monitoring of transactions, when receiving an application from a new customer, when receiving an instruction to carry out a transaction or during other communications with the customer.

14.6 APPENDIX 6

POTENTIAL RED FLAGS FOR MONEY LAUNDERING & TERRORIST FINANCING ACTIVITIES

The following is a non-exhaustive list of possible ML and TF red flags that CMS and its employees should be mindful of when dealing with a business relationship or occasional transaction:

a. The deposit or withdrawal of unusually large amounts of cash from an account.
b. Unwillingness to provide CDD documentation on beneficial owners/ controllers.
c. Deposits or withdrawals at a frequency that is inconsistent with CMS's understanding of that customer and their circumstances.
d. Transactions involving the unexplained movement of funds, either as cash or wire transfers.
e. Payments received from, or requests to make payments to, unknown or un-associated third parties.
f. Personal and business related money flows that are difficult to distinguish from each other.
g. Financial activity which is inconsistent with the legitimate or expected activity of the customer.
h. An account or business relationship becomes active after a period of dormancy.
i. The customer is unable or reluctant to provide details or credible explanations for establishing a business relationship, opening an account or conducting a transaction.
j. The customer holds multiple accounts for no apparent commercial or other reason.
k. Bank drafts cashed in for foreign currency.
l. Frequent early repayment of loans.
m. Frequent transfers indicated as loans sent from relatives.
n. Funds transferred to a charity or NPO with suspected links to a terrorist organisation.
o. High level of funds placed on store value cards.
p. Insurance policy being closed with a request for the payment to be made to a third party.
q. Large amounts of cash from unexplained sources.
r. Obtain loan and repay balance in cash.
s. Purchase of high value assets followed by immediate resale with payment requested via cheque.

The above mentioned non exhaustive list of potential red flags for ML and TF activities is provided for guidance. The existence of one or more red flag does not automatically indicate suspicion and there may be a legitimate reason for which a customer has acted in the manner identified.

14.7 APPENDIX 7

INTERNAL SUSPICIOUS TRANSACTION REPORT

Internal Suspicious Transaction Disclosure Form to MLRO of FCL

1.	**REPORTING EMPLOYEE**	
a.	Full name	
b.	Position:	
c.	Telephone No.	
2.	**CUSTOMER**	
a.	Customer Name	
b.	Customer Address	
c.	Representative (Contact Person) Name	
d.	Representative Telephone No.	
e.	Date Customer Relationship Commenced	
f.	Customer Reference	
3.	**INFORMATION / SUSPICION**	
a.	Suspected Information/ Transaction	
b.	Reasons for Suspicion	

Please attach copies of any relevant documentation to this report.

Reporter's Signature: _____

Date :_____

NOTE: It is an offence to advise the Customer. The Reported Parted or anyone else of your suspicion and report.
This report will be treated in the strictest confidence.

For MLRO Use:

Date & Time Received:

Date & Time of Acknowledgement to Reporting Officer:

FIU ADVISED: **YES** **NO**

Comments:

If Yes, Date of External Filing:

Reference No.

Approved by the Board on: ……