ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING

POLICY AND PROCEDURES MANUAL

made and adopted in respect of

360 Capital Ltd

(the "Company" or "FSP")

Approved by the Board on 11 February 2021

1. INTRODUCTION

1.1. The purpose of this Manual is to assist all members of management and employees of 360 Capital Ltd (the "Company ") to understand:

1.1.1. the Company 's Policy towards money laundering;

1.1.2. the Company 's procedures;

1.1.3. the legal requirements and the different penalties for non-compliance; and

1.1.4. how to recognise money laundering.

1.2. It is our intention to ensure that all employees have an understanding of money laundering, of why the Company must be particularly cautious in maintaining an Anti-Money-Laundering procedure and of the legal framework governing anti money laundering protocols.

1.3. Every employee of the Company is required to read and comply with this Manual. Failure to do so could expose the relevant employee to disciplinary action.

1.4. Any changes to the AML Policy can only be made following an ordinary resolution of the Board Members authorising the adoption of such amendment.

1.5. In summary all members of management and employees are expected to:

1.5.1. **Be aware of and follow the Company's procedures**

Certain of the Company's operating procedures have been strengthened with money laundering in mind. ***These procedures are there to be followed***.

1.5.2. **Be alert for anything suspicious**

This means not only large cash sums offered over the counter but a whole range of possible circumstances or transactions – the key may be that something does not "fit". It may be a single request or transaction, or it may be a pattern that does not seem right.

1.5.3. **Report suspicions to the Money Laundering Reporting Officer (MLRO)**

If you are suspicious, the law requires that you report it. The Money Laundering Reporting Officer ("MLRO") will act as the local contact, collecting any reports from employees and liaising with the authorities.

If you have any suspicions, don't keep quiet – speak to the MLRO. The MLRO is Mr. Sanjeev Kumar Lutchumun and the Alternate to MLRO is Mrs. Aroona D. Lutchumun.

2. WHY WE MUST COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

2.1. Money laundering is necessitated by the requirement for criminals, be the drug traffickers, organised criminals, terrorists, arms traffickers, blackmailers, or credit card swindlers, to disguise the origin of their criminal money so that they can use it more easily. Money laundering generally involves a series of multiple transactions used to disguise the source of financial assets so that those assets may be used without compromising the criminals who are seeking to use the Company. Through this process the criminal tries to transform the monetary proceeds derived from illicit activities into Company with an apparently legal source.

2.2. Money laundering has devastating social consequences and is a threat to national security. It provides the fuel for drug dealers, terrorists, illegal arms dealers, corrupt public officials and other criminals to operate and expand their criminal enterprises. Crime has become increasingly international in scope, and the financial aspects of crime have become more complex, due to rapid advances in technology and the globalisation of the financial services industry. Modern financial systems, in addition to facilitating legitimate commerce, permit criminals to order the transfer of millions of dollars instantly, using personal computers and satellite dishes. The criminal's choice of money laundering vehicles is limited only by his or her creativity. Money is laundered through currency exchange houses, stock brokerage houses, gold dealers, casinos, automobile dealerships, insurance companies, and trading companies. Private banking facilities, offshore banking, shell corporations, free trade zones, wire systems, and trade financing all have the ability to mask illegal activities. In doing so, criminals manipulate worldwide financial systems.

2.3. Unchecked, money laundering can erode the integrity of a nation's financial institutions. Due to the high integration of capital markets, money laundering could also adversely affect currencies and interest rates as launderers reinvest in

companies where their schemes are less likely to be detected, rather than where rates of return are higher.

2.4. Ultimately, this laundered money flows into global financial systems where it could undermine national economies and currencies. Money laundering is thus not only a law enforcement problem but poses a serious national and international security threat as well.

2.5. There is now worldwide recognition that we must deal firmly and effectively with increasingly elusive, well-financed and technologically adept criminals who are determined to use every means available to subvert the financial systems that are the cornerstone of legitimate international commerce. The continued abuse of some offshore financial centers, the proliferation of on-line Internet banking and Internet gambling have further enhanced the need to scrutinize new technologies to combat money laundering schemes.

3. WHAT IS MONEY LAUNDERING?

3.1. **Money laundering** is the process by which criminals attempt to conceal the true ownership of the proceeds of their criminal activities. If successful, money laundering allows criminals to legitimise "dirty" money by mingling it with "clean" money so that the money will lose its criminal identity and appear legitimate.

3.2. Money laundering also includes acquiring, possessing or using the proceeds of criminal conduct.

3.3. There is no one way of laundering money. Methods can range from the purchase and resale of high value items (e.g. houses, cars or jewellery) to the passing of money through a complex web of legitimate businesses and "shell" companies.

3.4. Despite the variety of methods employed, the laundering process is usually accomplished in three stages, each of which has its own characteristics and each of which may comprise numerous transactions by the launderers that could alert financial institutions to criminal activity:

3.4.1. place the money in the financial system, the object of which is to convert cash to a financial instrument, without arousing suspicion (known as "**Placement**");

3.4.2. move the money around, often in a series of complex transactions crossing multiple jurisdictions, so it becomes difficult to identify its original source and thus serve the link with the original crime (known as "**Layering**"); and

3.4.3. then move the money back into the financial and business system so that it appears as legitimate or assets or using an apparently legitimate transaction to disguise the illicit proceeds (known as "**Integration**").

3.5. The three basic stages may occur as separate or distinct phases. They may occur simultaneously or more commonly, they may overlap. The way in which these basic stages are used will depend on the available laundering mechanisms and the requirements of the criminal organisations.

3.6. **Placement**

This is actually disposing of criminal proceeds so that they are not found on the criminal. Where the proceeds take the form of cash (which they often do) the first step is to get the Company into the financial system. Some examples of this include:-

3.6.1. depositing cash, along with the proceeds of some legitimate enterprise in a deposit taking institution;

3.6.2. physically carrying cash between jurisdictions;

3.6.3. making loans to legitimate or apparently legitimate businesses in order to convert illegally obtained cash into an apparently legitimate debt;

3.6.4. placing cash in the client account of a professional intermediary; and

3.6.5. various other ways of disposing of the cash e.g. purchasing expensive objects, employing expensive services, purchasing negotiable assets in one off transactions.

3.7. **Layering**

3.8. This is how the criminal separates himself and the money from its original source. Layers of transactions are created intended to confuse the audit trail. It is hoped that the money will ultimately have the appearance of legitimacy having been in the financial system for a period of time. Some examples of layering include:

3.8.1. rapid switching of the Company between deposit taking institutions and jurisdictions;

3.8.2. use of cash deposits as security to support legitimate transactions;

3.8.3. switching cash through a network of legitimate businesses and shell companies across several jurisdictions; and

3.8.4. resale of goods and assets.

3.9. **Integration**

3.9.1. Integration is bringing the money into use. If layering has succeeded, the criminal is able to deploy the proceeds within the economy as apparently legitimate. At this stage, it is of course unlikely that a transaction will necessarily appear suspicious. Examples of integration could include:

3.9.1.1. the purchase of a troubled business for a good price exceeding its book value, or

3.9.1.2. raising a loan on the security of an asset and using the loan to establish an investment account.

3.9.2. Certain factors will indicate that a transaction may be intended as part of a money laundering scheme. In general, it can be expected that the majority of potentially suspect transactions that will come to our attention will be part of the layering process. It is essential that all employees of the Company are particularly aware of circumstances which may be suspicious.

3.9.3. The Securities Act 2005, The Financial Services Act 2007, The Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA or Act), The Code on the Prevention of Money Laundering & Terrorist Financing dated March 2012 and the 2018 Regulations made under FIAMLA, and The Prevention of Terrorism Act 2002 (POTA), Anti Money Laundering and Countering The Financing of Terrorism Handbook 2020 (AML Handbook) form part of the legal framework in Mauritius. It is therefore essential that the principles as to what will constitute a suspicious transaction are well understood.

3.9.4. Historically, money laundering has been concentrated on the traditional banking sector. However, criminals have responded to the measures taken by

banks and have sought to convert illegally earned money or mix them with legitimate income before they enter the banking system, thus making them harder to detect. Non-bank financial institutions have become increasingly vulnerable to being used for money laundering.

3.9.5. Terrorist financing involving the raising, management and transmission of money to finance the illegal activities of terrorist organisations with the intent of subverting the rule of law in Mauritius and other countries. Money for terrorists can often originate in legitimate areas, yet the transactions ordered may have suspicious or uncommercial patterns.

3.9.6. The highest risk category relates to those products or services where unlimited third party money can be freely received, or where the money can be regularly paid to, or received from third parties without evidence of identity of the third parties being taken. Examples of products in the highest risk category are: products offering money transfer facilities through chequebooks, telegraphic transfers, deposits from third parties, cash withdrawals, credit and debit cards or other means.

3.9.7. There are points of vulnerability for the money launderer and terrorist financer, at which times suspicious activity may be more recognisable:-

3.9.8. cross border flows of cash;

3.9.9. entry of cash into the financial system;

3.9.10. transfers from and within the financial system;

3.9.11. acquisition of investments and other assets;

3.9.12. incorporation of companies; and

3.9.13. formation of trusts.

3.10. **How can financial institutions combat money laundering and terrorist financing?**

3.10.1. Financial institutions must adhere to the fundamental concept of good business practice: **Know Your Customer.** Knowing and understanding your customer's business and the patterns of financial transactions and

commitments is the core to developing a capacity to recognise efforts to launder illicit money.

3.10.2. It is acknowledged by the authorities that we may have difficulty identifying terrorist financing in cases other than where illicit organisations seek to invest in our Company by name, however we remain subject to our legal duty to adopt measures and procedures to detect and prevent the commission of money laundering and terrorist financing offences

4. POLICY

It is the Company's policy that:

4.1. FATF recommendations, Mauritius anti money laundering statutory and regulatory obligations are to be met in full, the fundamental principle of good business practice **'know your customer'** is observed, and that employees of the Company are trained in order to comply with these obligations.

4.2. Positive management action shall be exercised in order to minimise the risk of the Company's services being abused for the purposes of laundering money.

4.3. The Company will not continue established relationships with parties whose conduct gives rise to suspicion of involvement with illegal activities. The Company will seek to terminate any client relationship where the client conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities.

4.4. **Salient Definitions and Requirements**

4.4.1. Both FIAMLA and POTA are in keeping with worldwide trends aimed at curbing the proceeds of crime, money laundering and terrorism. POTA aims at combating terrorism and empowers our legal system to adequately deal with the phenomenon of terrorism.

4.4.2. POTA applies to "*acts of terrorism*" which is defined as an act which:

"*(a) may seriously damage a country or an international organisation; and*

(b) is intended or can reasonably be regarded as having been in- tended to—

(i) seriously intimidate a population;

(ii) unduly compel a Government or an international organisa- tion to perform or abstain from performing any act;

(iii) seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation; or

(iv) otherwise influence such Government, or international organisation; and

(c) involves or causes, as the case may be—

(i) attacks upon a person's life which may cause death;

(ii) attacks upon the physical integrity of a person;

(iii) kidnapping of a person;

(iv) extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an in- formation system, a fixed platform located on the continental shelf, a public place or private property, likely to endanger human life or result in major economic loss;

(v) the seizure of an aircraft, a ship or other means of public or goods transport;

(vi) the manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;

(vii) the release of dangerous substance, or causing of fires, explosions or floods, the effect of which is to endanger human life;

(viii) interference with or disruption of the supply of water, power or any other fundamental natural resource, the effect of which is to endanger life."

4.4.3. POTA also applies to "terrorist property" which means property that—

(a) has been, is being or is likely to be used for any act of terrorism;

(b) has been, is being or is likely to be used by a proscribed organi- sation;

(c) is the proceeds of an act of terrorism; or

(d) is gathered for the pursuit of, or in connection with, an act of terrorism.

4.4.4. It is an offence under POTA where **"***any person who enters into, or becomes concerned in, an arrangement which facilitates the retention or control by, or on behalf of, another person of terrorist property, in any manner, including—*

(a) by concealment;

(b) by removal from the jurisdiction; or

(c) by transfer to any other person".

4.5. FIAMLA complements POTA and is the principal money laundering legislation in Mauritius.

4.6. In terms of FIAMLA, rigorous compliance obligations are imposed on reporting institutions, of which the Company is one.

4.7. Reporting institutions are obliged to:-

4.7.1. identify and verify new and existing clients;

4.7.2. keep records of identities of clients and of transactions entered into with clients;

4.7.3. report suspicious transactions to the Financial Intelligence Unit;

4.7.4. formulate and implement internal rules;

4.7.5. train employees; and

4.7.6. appoint a responsible person to monitor compliance.

4.8. The person responsible for monitoring compliance at the Company is **the Compliance Officer**.

4.9. Terrorist financing is also a predicate offence for money laundering. The purpose of this manual is not to go into the detail on the criminal and civil forfeiture regime that exists. As an employee we are, however, expected to know how to deal with a client that has committed or has been suspected of committing the predicate offences.

4.10. The **money laundering** offences are, in summary:

4.10.1. 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 of money laundering.

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

4.10.2. It is an offence for a designated body to fail to maintain the records required by FIAMLA or to fail to adopt measures to prevent and detect money laundering.

4.10.3. It is an offence for a designated body, its directors, employees and officers to fail to make a report as required by FIAMLA.

4.10.4. The act of tipping off is an offence under FIAMLA. This may occur where a person who, knowing or suspecting that an investigation is taking place makes any disclosure likely to prejudice the investigation arising from a report under FIAMLA.

4.11. It is not necessary that the original activity from which the proceeds stem was committed in Mauritius.

4.12. There is no obligation on a financial institution to enquire into the specific criminal offence underlying the suspicious transaction.

5. RISK BASED APPROACH

5.1. In terms of the Financial Action task force guidelines, the Company will incorporate a risk based approach to identifying its clients. Although the Company clients are expected to be similar in nature, the Company will still consider the following risk indicators when differentiating between clients. The following factors may be applied to differentiate between high risk, medium risk and low risk clients:

- The nature and type of customer
- Commercial rationale of the relationship
- The geographical location of customer
- The geographical location of the customer's business interest and / or assets
- Product type and value of assets concerned in the relationship
- Source of funds and where necessary, source of wealth

5.2. After collection of all CDD documentation, the Company must make an initial assessment of the risk to which the business relationship will expose the company and evaluate the customer accordingly. In this exercise the Company must take into consideration a number of factor including but not limited to the above list in 5.1.

Following the risk assessment exercise, a review shall take place based on the rating below;

- Low : every year
- Medium : every 6 months
- High : every 3 months

Clients will be risk rated during the engagement process and will be tagged under under low, medium or high risk.

6. IDENTIFICATION PROCEDURES

6.1. The purpose of these procedures is to ensure that the Company is in a position to be able to say "We know our client". The procedures are aimed to ensure that our clients actually exist and that they are who they say they are. The overriding requirement is that the Company is satisfied that it has established the true identity of the prospective client/investor as far as it is reasonably possible.

6.2. The Code on Prevention of Money Laundering and Terrorist Financing is the principal source for developing appropriate procedures. However, they provide some room for the exercise of discretion in carrying out their recommendations. Such discretion must be exercised only by the MLRO and with great caution, as its exercise may well be the subject of subsequent review by persons armed with much more information than we had at the time of entering into the business relationship with the client.

6.3. **What is identity?**

6.3.1. An individual's identity comprises his/her name and all other names used and address at which he/she can be located. Date of birth is also a useful indicator of identity. In order to identify somebody, an official document bearing a photograph of the person (e.g. certified copy of a passport or driving licence) should be obtained.

6.3.2. Corporate identification should include obtaining of incorporation documents, independent verification of the existence of the corporate body and confirmation that it exists for a legitimate purpose. Any subsequent changes to a customer's identification that are brought to the attention of the Company should be recorded as part of the know your customer process.

6.4. **Timing and duration of identification**

6.4.1. Whenever the Company or client/investor enters into a business relationship, we must carry out procedures to establish the identification of that client/investor as soon as reasonably practicable. Unless there is an exemption available, we must perform these checks ourselves or rely on identification conducted by a designated body in certain circumstances.

6.4.2. We should always complete the identification process. If a client/investor declines to cooperate the matter must be reported to the MLRO, who will decide whether to continue with the transaction or what other steps to take.

6.4.3. No funds should be transferred for the benefit of an identification subject until the identification process is complete.

6.5. **Methods of identification**

6.5.1. In terms of FIAMLA, a reporting institution may **not** establish ***a business relationship***[1] or conclude ***a single transaction***[2] with a client or prospective client unless it has taken certain prescribed steps to establish and verify the identity of the client or prospective client, as the case may be. Identification of the "principal" and "agent" and proof of authority are required where the client is acting on behalf of someone, or someone is acting on behalf of the client.

6.5.2. When establishing and verifying identities, the Company will follow the guidelines as provided by the Code on Prevention of Money Laundering and Terrorist Financing**.**

6.6. **Identification and Verification Procedures – New Client**

6.6.1. As early as possible and preferably at or before the first meeting with a new client, the Company must ascertain what information and documentation is required from the client in order to establish and verify the client's identity. The process of verification of identity entails comparing the identifying particulars provided by the client with other available information in order to establish whether the particulars provided by the client accurately and correctly reflect the client's identity.

6.6.2. There are different identification and verification requirements depending on whether the client or prospective client is a natural or a legal person.

[1] "**A business relationship**" is defined as "*an arrangement between a person and a reporting person, where the purpose, or effect, of the arrangement is to facilitate the carrying out of transactions between the person and the reporting person on a frequent, an habitual or a regular basis;*".

[2] "**Transaction**" includes "
(a) opening an account, issuing a passbook, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, whether electronically or otherwise; and
(b) a proposed transaction or an attempted transaction".

6.6.3. Each employee will be responsible for ensuring that his or her client furnishes the required information and documentation and to take reasonable steps to maintain the correctness of particulars of a client which are susceptible to change.

6.7. **Individuals**

The following information should be obtained:-

6.7.1. **Identity**

6.7.1.1. notarised or certified copy[3] of signed identification papers with a photograph attached such as a passport, drivers licence or national identity card;

6.7.1.2. We must ensure that these papers remain valid and have not expired and that there is no variation in the signatures used on the identification papers and the client agreement.

6.7.2. **Address**

6.7.2.1. Any one of the following should be obtained:

6.7.2.1.1. original or certified copy of a recent utility bill issued,

6.7.2.1.2. original or certified recent bank or credit card statement dated;

6.7.2.1.3. original or certified recent bank reference;

6.7.2.1.4. original or a professional reference including residential address.

6.7.2.2. **In our procedure we seek to ascertain who the investor is, and therefore the following information is vital:**

6.7.2.2.1. full names used;

6.7.2.2.2. date of birth;

6.7.2.2.3. place of birth;

[3] Certification can be by a Commissioner of Oaths, police officer, Chartered or Certified Accountant, Notary Public or Practising Solicitor/Lawyer, Banker or Embassy/Consular Employees

6.7.2.2.4. nationality;

6.7.2.2.5. occupation;

6.7.2.2.6. specimen signature; and

6.7.2.2.7. current permanent residential address, including zip or postal code;

This information should be ascertained and verified.

6.8. **Legal Persons**

The use of legal persons raises specific issues in anti money-laundering procedures because the identity of the ultimate beneficial owner is obscured by the corporate or legal structure of the entity. The principal aim of our identification procedures here is to penetrate the corporate entities and identify those natural persons who have ultimate control over the assets. Particular attention should be paid to anyone who has contributed significant capital to the investing entity. Additionally, every effort must be made to ensure that the investing entity exists for a legitimate trading or economic purpose and that it is not merely a brass plate entity where controlling parties cannot be identified.

Therefore, whenever we deal with a legal person, we must –

(a) take reasonable measures to understand the ownership and control structure of the applicant for business;

(b) verify and establish the existence of the legal person; and

(c) determine the identity of the principals of the legal person.

6.9. **Companies**

6.9.1. Inspect the incorporation documents. This should include such of the following documents to satisfy yourself of the investor's *bona fides*:

6.9.1.1. certified copy of certificate of incorporation or registration;

6.9.1.2. certified copy of Certificate of Good Standing from Registrar of Companies;

6.9.1.3. certified copy of the memorandum of Incorporation (or equivalent);

6.9.1.4. obtaining details of the registered address and place of business;

6.9.1.5. an authorised signatory list of the Company ;

6.9.1.6. a list of directors names, including occupations, residential and business addresses and dates of birth with identity documents provided;

6.9.1.7. a certified copy of latest reports or accounts (audited, where possible).

6.9.1.8. a list of the shareholders, with identity documents provided.

6.10. **Partnerships**

The following documents should be obtained:-

6.10.1. a certified copy of the partnership agreement; and

6.10.2. a certified copy of the latest accounts;

6.10.3. verification of the nature of the business of the partnership to ensure that it is legitimate;

6.10.4. verifying the identity of the principals;

6.10.5. an authorised signatory list of the General Partner;

6.11. **Trusts**

In the case of trust accounts the following should be provided to establish the identity of the trustee, settlors or contributors of capital (whether named or otherwise), protectors, enforcers and the beneficiaries of the trust:

6.11.1. a list of trustees and licence to act as Trustee;

6.11.2. a certified copy of the Trust Deed;

6.11.3. an authorised signatory list;

6.11.4. KYC documents on Settlor;

6.11.5. a list of beneficiaries of the trust and certified ID documents for the beneficiaries; and

6.11.6. Obtaining details of the registered office and place of business of the Trustee;

6.11.7. Verify the identity of the principals of the Trustee.

6.12. **Politically Exposed Persons (PEPS)**

6.12.1. A PEP is a term used for an individual who is or has in the past performed prominent public functions in any particular country. The principles issued by the Wolfsberg group of leading international financial institutions give practical guidelines on these issues. These principles are applicable to both domestic and international politically exposed persons. The following are examples of such persons:

6.12.1.1. heads of states or of governments;

6.12.1.2. ministers;

6.12.1.3. influential functionaries in nationalised industries;

6.12.1.4. senior government, judicial and military officials;

6.12.1.5. senior politicians and political party officials;

6.12.1.6. military leaders;

6.12.1.7. members of royal families;

6.12.1.8. senior executives of state owned corporations; and

6.12.1.9. senior and/or influential representatives of religious organisations

6.12.2. The Company will conduct proper due diligence on the PEP's and any person acting on their behalf, and PEP's personally or acting on behalf of family members will be subject to scrutiny. In terms of FIAMLA, specific action should be taken in respect of PEP's as a category of high risk clients. The PEP is immediately a high risk client.

6.12.3. In addition to performing the usual risk management measures, The Company will put in place a proper risk management system to determine whether the client is a PEP. In addition, The Company's employees must obtain approval from the Board before approving the establishment of business relationship with a PEP and will take reasonable measures to establish the source of wealth and the source of funds and will conduct enhanced on-going monitoring of the relationship with the PEP.

6.13. **Establishment and verification of identities**

6.13.1. Once the identification procedures have been completed, evidence of identity will not be necessary for subsequent transactions of the client/investor, but the appropriate records must be kept.

6.13.2. Each client/investor file must show the steps taken and the results of the identification process in respect of every identification subject, including letters from reliable sources and regulated institutions. The file should also contain reasons for not completing the process, or why the investor was treated as being an exempt case.

6.14. **Implementation of Targeted Sanctions under the Financial Prohibitions against Listed Parties under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019**

6.14.1. The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 provides the legal framework for the Government of Mauritius to implement targeted sanctions, including financial sanctions, arms embargo and travel ban, and other measures imposed by the United Nations Security Council under Chapter VII of the Charter of the United Nations, with a view to addressing threats to international peace and security, including terrorism, the financing of terrorism and proliferation of weapons of mass destruction. The United Nations has established a list of parties ("Listed Parties") against which targeted sanctions have been imposed. The United Nations Security Council Consolidated List may be accessed at the following link: https://www.un.org/securitycouncil/content/un-sc-consolidated-list. Additionally, the list is also available on the FSC and FIU websites, and is disseminated to reporting persons, investigatory authorities, supervisory authorities and any other relevant public and private agencies, registered on the goAML platform.

A summary of the current UN sanctions regime may be consulted at the above link. As part of its AML/CFT obligations, the Company must therefore on a weekly basis (or each time before a customer is onboarded, whichever is the earlier) consult the Consolidated List and take immediate action with respect to any changes brought thereto. The Company must also regularly consult the newspapers for any notice which may be issued by the National Sanctions Secretariat (in addition to its website as well as those of the FSC and the FIU) and immediately act upon it.

6.14.2. Pursuant to Section 18 of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the National Sanctions Secretariat, established thereunder gave public notice of the Consolidated List. Simultaneously, it has issued an Explanatory Note on the implementation of United Nations Sanctions Measures which have been published in the Government Gazette of 5 October 2019.

6.14.3. As a result of this Notice, the following financial prohibitions under Sections 23 and 24 of the said Act apply immediately:

(a) Prohibition to deal with the funds or other assets of Listed Parties under section 23 which provides that no person shall deal with the funds or other assets of a listed party, including –

- all funds or other assets that are owned or controlled by the Listed Party;
- those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by the Listed Party;
- funds or other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by the Listed Party; and
- funds or other assets of a party acting on behalf of, or at the direction of, the Listed Party.

(b) Prohibition to make funds or other assets available to Listed Parties under section 24 which states that no person shall make any funds or other assets or financial or other related services available, directly or indirectly, or wholly or jointly, to or for the benefit of –

- a Listed Party;
- a party acting on behalf, or at the direction, of a Listed Party; or
- an entity owned or controlled, directly or indirectly, by a Listed Party.

6.14.4. The Company, as part of its reporting obligations, must:

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

(b) if there is a positive match, identify whether the customer owns any funds or other assets with it, including the funds or assets mentioned in section 23(1) of the said Act; and

(c) make a report to the National Sanctions Secretariat and the FSC where funds or other assets have been identified by it. Accordingly, in accordance with section 23(4) of the said Act any person who holds, controls or has in his custody or possession any funds or other assets of a Listed Party must, not later than 24 hours of any notice issued under section 18(1) of the said Act, notify the National Sanctions Secretariat 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;

(ii) the name and address of the Listed Party;

(iii) details of any attempted transaction involving the funds or other assets, including –

- 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.

(d) submit a nil report to the above authorities if no funds or other assets are identified;

(e) immediately submit to the FIU in accordance with section 14 of FIAMLA, any information relating to a Listed Party which is known to it. This is in addition to the above reporting obligations.

7. KEEPING OF RECORDS

7.1. In terms of FIAMLA, the Company is required to keep detailed records of its clients and the transactions entered into with them.

7.2. The duty to keep records arises whenever the Company establishes a business relationship or concludes a single transaction with a client.

7.3. FIAMLA requires the FSP to keep records of the following:

7.3.1. the identity of a client and, if applicable, the identity of the client's agent or principal;

7.3.2. the manner in which the identity of the client and the client's agent or principal was established;

7.3.3. the nature of the business relationship or transaction;

7.3.4. in the case of a transaction, the amount involved and the parties to that transaction;

7.3.5. all accounts that are involved in transactions concluded by the Company in the course of a business relationship or a single transaction, as the case may be;

7.3.6. the name of the person who obtained the information referred to above; and

7.3.7. any document or copy of a document obtained by the Company in order to verify a person's identity.

7.4. In order to comply with this requirement, hard copies of identifying documents received from clients must be kept for a period of at least seven years.

7.5. No person may delete or destroy any record pertaining to a client in respect of identity or verification of identity or in respect of any transaction recorded.

7.6. An authorised representative of the Company has access to any records kept by the Company and may examine, make extracts from or copies of any such records.

7.7. The Company must, except where such documents are protected by confidentiality, give to an authorised representative all reasonable assistance in this regard.

7.8. Any request for access to records, including by way of warrant, must be forwarded to the Compliance Officer and may not be dealt with by any member of employees.

The Company to advise whether a specified person is or has been a client whether a specified person is acting or has acted on behalf of any client; or whether a client is acting or has acted for a specified person. To the extent that some of this information may be protected by privilege and to keep the reporting process streamlined, no person other than the Compliance Officer may respond to such request. Accordingly, if any person at the Company receives such a request that person must immediately inform the Compliance Officer.

8. RESULTS OF IDENTIFICATION PROCEDURES

8.1. Once the identification procedures have been completed, evidence of identity will not be necessary for subsequent transactions of the client/investor, but the appropriate records must be kept.

8.2. Each client/investor file must show the steps taken and the results of the identification process in respect of every identification subject, including letters from reliable sources and regulated institutions. The file should also contain reasons for not completing the process, or why the investor was treated as being an exempt case.

8.3. **Unsatisfactory identification**

8.3.1. If the verification process is not completed in relation to every identification subject, funds held to the account of the investor should be retained until the issues are resolved. The MLRO should be informed. A written report should be

prepared, giving details of the company or client, the nature of the failure of the identification process and the reasons for its failure. It should be sent to the MLRO and a decision will be made as to the appropriate course of action. A copy of the report will be placed in the Company's file.

8.3.2. If the failure of the identification process gives rise to a suspicion of money laundering, submit an internal disclosure form together with the reasons for your suspicions and the nature of the transaction. The MLRO will consider the report and where appropriate, notify the FIU.

8.4. **Source of funds**

8.4.1. You should always confirm that the source of funds of the investment is consistent with the other information provided to you in the course of the identification procedure. The source of funds must be an account with a bank/credit institution where the name of the drawee bank/credit institution account is the same as that of the individual investor.

8.4.2. Payments from joint accounts are considered acceptable. Payments by bank or building society draft or from a general account are not considered acceptable unless they are certified by the financial institution as coming from an account held in the name of the individual investor.

9. GENERAL POINTS ON IDENTIFICATION

These procedures are intended to ensure that the Company is in complete compliance with the Act. Compliance with these procedures should provide a complete defence to any charges brought against the Company or any of its employees under the Act. However, if any employee becomes aware of any suspicious transaction after all the procedures are followed and the identification process is completed satisfactorily, a report should be made to the MLRO.

10. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

10.1. **There is a statutory legal obligation on all employees of the Company to report suspicions of money laundering. There can be criminal penalties for employees who do not report suspicious transactions.** However, in the case of any employee, once they have reported their suspicion in accordance with established internal reporting procedures they have satisfied this obligation.

10.2. The Act states that there is no liability for breach of confidentiality or otherwise by reporting suspicious transactions.

10.3. As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business of their account. Therefore the key to recognition is knowing enough about the customer's business to recognise that a transaction, or series of transactions, is unusual.

10.4. You should also be willing to rely on 'gut instinct' where a transaction does not seem to make commercial sense, if you feel that there is something suspicious about a transaction or investor you should contact the MLRO to discuss your concerns.

10.5. Questions that might be considered when determining whether an established customer's transaction might be suspicious are:

10.5.1. Is the size of the transaction consistent with the normal activities of the customer?

10.5.2. Is the transaction rational in the context of the customers business or personal activities?

10.5.3. Has the pattern of transactions conducted by the customer changed?

10.5.4. In the case of a transaction of an international nature, does the customer have any obvious reason for conducting business with the other country or counterparty involved?

10.6. **Reporting of Cash Transactions**

10.6.1. All cash transactions of MUR500,000 and above must be reported to the MLRO. This includes multiple cash payments of smaller amounts received over a period of 24 hours, which can be linked as fractions or parts of one transaction and which, when aggregated, amount to MUR500,000 or more. This must be done irrespective of whether or not it is a suspicious and/or unusual transaction.

10.6.2. Multiple cash payments of MUR500,000 and more received over a period of more than 24 hours and which are suspected of having being structured in

such a way as to evade a reporting requirement, must be reported as a suspicious or unusual transaction.

10.6.3. Cash is defined as coins and notes of Mauritius or another country, as well as any cheque which is neither crossed nor made payable to order whether in Mauritian currency or in any other currency;

10.6.4. The Cash transaction report is to be completed for reporting of cash transactions, identified above, and reporting must take place immediately after becoming aware of such a cash transaction.

10.6.5. The MLRO shall report this to the FIU, on the prescribed form, as soon as possible but not later than 15 (Fifteen) working days after becoming aware of such a cash transaction.

10.7. **Procedure for reporting a suspicious transaction**

10.7.1. The employee must take certain steps immediately:

10.7.1.1. File the internal disclosure form with the MLRO

10.7.1.2. Gather and keep safely all the files relating to that investor, in particular safeguarding all original material relating to the transaction in question.

10.7.1.3. Take no steps on any instructions to transfer funds or property out of or within the jurisdiction[4]**

10.7.1.4. Make no report to the client or any other person which could constitute a tipping-off.

10.7.2. The MLRO will take the following steps:-

10.7.2.1. Review the report and the file, discuss the transaction with the directors of the Company and the group manager;

10.7.2.2. If he is of the opinion that the matter does raise reasonable suspicion of money laundering he will notify the FIU;

[4] While transactions which are suspected to be related to money laundering must not be carried out until the reporting authority has been informed, where it is impossible in the circumstances to refrain from executing a suspicious transaction before making a report, the reporting authority should be informed immediately after the transaction has been executed

10.7.2.3. This Report will be made using the Form available from the FIU at http://www.fiumauritius.org/English/Reporting/Documents/STR%20FORM200114_310817.pdf .

10.7.3. If the MLRO and the directors of the Company are satisfied that the transaction is **NOT** a money laundering transaction he may instruct the responsible group manager to proceed with the transaction.

10.8. **Tipping off**

It is an offence where an employee knowing or suspecting that a report has been made to the FIU alerts the client or customer to the fact that a report has been made.

11. **TERRORIST FUNDS**

Where there is reason to believe that funds could be used to finance terrorism, the MLRO should inform law enforcement authorities.

12. **SCREENING AND TRAINING**

In order to ensure that the Company's personnel are of the required standard of competence (depending on the role of the employee within the Company), the Company must give consideration to the following prior to, 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 (as it would for a customer).

The Company must also carry out ongoing tallying of its personnel against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

The Act and the Code on Prevention of Money Laundering and Terrorist Financing require that all relevant employees of a financial institution must receive training in specific matters. The Company requires that all relevant employees are advised of their obligations under the Act and the Code on Prevention of Money Laundering and Terrorist Financing and will undertake compulsory refresher training for relevant employees on a periodic basis.

13. **RECORD KEEPING AND REPORTING**

13.1. The Act provides that a copy of all documents used to identify a client/investor must be kept for a period of at least 7 years after the relationship with the client/investor has ended. This obligation applies even if the person identified does not become a client/investor or the proposed transaction is not actually effected. The date on which the client relationship is deemed to have ended is the date of:

13.1.1. the completion of all activities in relation to a once-off transaction or the last in a series of transactions; or

13.1.2. the ending of the relationship e.g. closing of account or dissolution of a fund: or

13.1.3. the commencement of proceedings to recover debts payable on insolvency.

13.2. While the Laws does not specify the precise nature of the records to be retained in respect of a transaction or series of transactions, the objective of the Acts and Regulations is to ensure that in the event of an investigation the Company can assist in the creation of an audit trail. The original documents or copies admissible in legal proceedings relating to a transaction must be maintained.

13.3. The following information is relevant in the case of each transaction:

13.3.1. Name, address, age, occupation, passport number, nationality of client;

13.3.2. Personal references and identification;

13.3.3. Name and number of Fund and corporate documents of the Company; and

13.3.4. Particulars of the transaction or property including amount and currency of any funds, the date they were received, the known source of such funds.

14. **ADOPTION**

Adoption of this AML Manual incorporating FATF guidelines shall be brought into effect by approval of the Board of Directors of the Company

15. **CONCLUSION**

15.1. It is intended that these procedures will create an understanding of money laundering and awareness of money-laundering. They provide a systematic means of ensuring that neither the Company, its employees nor our clients find ourselves in breach of the legislation. They should enable us to provide a high quality service to our clients.

15.2. **However, it may be that certain of the procedures will have to be changed over time due to experience. FIAMLA and the Code on Prevention of Money Laundering and Terrorist Financing have been amended and will be again in the future as our authorities seek to combat money launderers. Accordingly these procedures will be kept under constant review. Amendments will be issued as required and the manual itself will be re-issued as required**

ANNEXURE A

Indicators of Potentially Suspicious Activity

This list of indicators is by no means an exhaustive list of indicators of suspicious activity.

a. Any activity that casts doubt over the true identity of an applicant for business or the principals thereof.
b. Any relationship or arrangement that appears not to have a clear commercial justification or rationale.
c. Any unusual or unexplained transaction in the context of the normal pattern of activity for a particular relationship.
d. Reluctance on the part of clients to respond to enquiries made by the Company.
e. Attempts to avoid standard processes.
f. Unusually linked transactions.
g. Unnecessarily complex arrangements.
h. Fund transfers to or from accounts in countries that are known to be associated with drug trafficking or other serious crime.
i. Fund remittances or fund transfers request to unknown third parties.
j. Receipt of large transfers in, which are immediately followed by withdrawal. Any activity that appears to be inconsistent with the due diligence information and profile of a particular client e.g. the client's apparent standing and means.
k. Receipt of funds from or transmission of funds to a shell bank.
l. Back to back deposit/loan transactions with subsidiaries of, or affiliates of, overseas financial institutions in non-cooperative, non-recognised banking jurisdictions or correspondent shell banks.
m. Clients who produce or demand for collection large quantities of cash.
n. The request for use of intermediary client accounts as bank accounts.
o. A complete disregard for investment risks, such as adverse tax treatment and transaction.
p. A willingness to accept frequent losses without question.
q. A complete disregard for due diligence / research in connection with investments.
r. No apparent investment strategy or conduct inconsistent with a stated investment strategy.
s. Use of an address, which is not a permanent or regular address.
t. Unusual concern for secrecy, particularly with respect to their Identity, type of business, and property held.