**SECUREFX CAPITAL LTD.**

# ANTI-MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM, COUNTER PROLIFERATION FINANCING AND TARGETED FINANCIAL SANCTIONS POLICIES & PROCEDURES MANUAL

Approved and adopted: January 2024
Last reviewed: February 2024

*The policies and procedures within this Manual have been written to assist compliance with the anti-money laundering and counter financing of terrorism laws of Saint Lucia.*

*Alternative measures to those set out in this Manual should not be applied without the agreement of the Compliance Officer.*

## A. INTRODUCTION TO THIS MANUAL

### 1. Overview and purpose

1.1 This anti-money laundering (**AML**), counter financing of terrorism (**CFT**), counter proliferation financing (**CPF**) and targeted financial sanctions (**TFS**) policies and procedures manual (this **Manual**) sets out the systems, policies and procedures adopted by SECUREFX CAPITAL LTD. (the **Entity**) with respect to AML, CFT, CPF and TFS. In particular, this Manual establishes the necessary policies and procedures required to ensure full compliance with the applicable laws and regulations of Saint Lucia (**St Lucia** or **Saint Lucia**).

1.2 This Manual is designed to assist the Entity in adhering to the laws of Saint Lucia and, if followed diligently, will protect the Entity, its customers, employees, facilities and activities from being used for money laundering (**ML**), terrorist financing (**TF**) and/or proliferation financing (**PF**), or breaching any TFS.

1.3 The consequences of the Entity being used to assist ML, TF and/or PF, or acting contrary to TFS, include:

(a) criminal and disciplinary sanctions for the Entity and its individual directors and other officers;

(b) civil and/or criminal prosecution of the Entity and its individual directors and other officers;

(c) financial sanctions against the Entity and its individual directors and other officers; and

(d) severe reputational damage to the Entity and its associates worldwide, together with a loss of business.

1.4 This Manual has been adopted by the board of directors (the **Management** or the **Board**) of the Entity and is effective immediately. Compliance with this Manual is integral to the Entity's overall commitment to combat ML, TF, PF and other crimes.

### 2. Policy

2.1 The policy of the Entity is to ensure full compliance with all applicable laws and regulations regarding AML procedures and TFS, in order to prevent and detect ML, TF, PF and other illegal activities.

2.2 It is the policy of the Entity to deal only with individuals and organisations of good standing and sound repute, so as to protect the reputation of the Entity and of Saint Lucia.

2.3 Directors, officers and employees of the Entity are required to familiarise themselves with the policies and procedures set out below. Directors, officers and employees of the Entity are expected to refer to and comply with the specific provisions of this Manual on every occasion that relevant circumstances arise, seeking appropriate advice or assistance in advance, if necessary. Failure to follow the requirements of this Manual is unacceptable and may result in action being taken in accordance with the terms of employment. Such a failure may, in some circumstances, also constitute a regulatory breach or criminal offence, which may result in the Entity being sanctioned and may also result in the relevant person being personally sanctioned.

### 3. Business of the Entity, Risks of Business and Risk Management Systems

3.1 The Entity was incorporated as a Saint Lucian international business company on 15 December 2023 by filing its memorandum and articles of association with the Registrar of International Business Companies of St Lucia[1]

3.2 The Entity is subject to the overall supervision by the Board. The activities of the company are the provision of broker-dealer services in Contracts For Difference whose underlying are foreign exchange pairs, commodities, indices, and other securities. The Board's role is to execute and supervise the activities of the Entity. The Board currently consists of 1 member VISHAL V. LIMBANI[2].

[1] Certificate of incorporation as international business company dated 15 December 2023.

[2] Register of Directors of the Entity dated 6 January 2023

## B. INTRODUCTION TO AML/CFT AND THE PURPOSE AND IMPORTANCE OF THE COMPLIANCE FUNCTION

### 1. What is money laundering?

1.1 Deception is the heart of money laundering. ML is the process by which the direct or indirect benefit of crime is channelled through the financial system in order to conceal the true origin and ownership of the proceeds of criminal activities. Generally, to launder criminal proceeds, a money launderer places the funds/proceeds in the financial system without arousing any suspicion, moves it in a series of complex transactions to disguise its original (criminal) source and finally, if successful, integrates it into the economy to make the funds appear to be derived legitimately.

1.2 There is no single method of laundering money. However, despite the variety of methods used, the laundering process is accomplished in three stages, as follows:

(a) *placement* – the physical placement of proceeds derived from criminal activity into the financial system;

(b) *layering* – separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity; and

(c) *integration* – the provision of apparent legitimacy to wealth derived from crime.

1.3 The three basic steps may or may not occur as separate and distinct phases; they may occur simultaneously or they may overlap. Some typical examples of the three stages are listed below.

| *Placement* | *Layering* | *Integration* |
|---|---|---|
| Cash paid into the account of a financial service provider, sometimes with employee complicity or mixed with legitimate funds | Wiring transfer abroad | False loan repayments and forged invoices are used as a cover for repayment of laundered money |
| Cash used to buy high value assets | Resale of goods or assets | Income from sale of assets appears legitimate |

1.4 Certain points in the laundering process have been identified as difficult for money launderers to avoid and, therefore, more susceptible to recognition as ML by legitimate businesses, including:

(a) entry of cash into the financial system;

(b) cross-border flows of cash;

(c) acquisition of financial assets;

(d) transfers within and from the financial system; and

(e) establishment of corporate and financial vehicles, including ostensible pooled investment funds.

1.5 Below are examples of suspicious behaviour or transactions which could occur during the course of a normal business day:

(a) a customer for whom verification of identity is unusually difficult and who is reluctant to provide details;

(b) an unwillingness to disclose the source(s) of funds;

(c) an unwillingness to disclose the identity of beneficial owners or beneficiaries;

(d) attempts to make cash deposits;

(e) frequent transfers into or from an account for no apparent commercial reason;

(f) transfers of assets to an apparently unrelated third party;

(g) a customer who is introduced by a third party based in a country noted for corruption or drug production;

(h) registration or delivery of securities to an unverified third party; and

(i) the use of a different mailing address.

## 2. What is terrorist financing?

2.1 A person commits the offence of financing of terrorism under the Anti-Terrorism Act, 2017 (As Amended (the **Anti-Terrorism Act**) if that person, directly or indirectly, wilfully and without lawful justification or reasonable excuse, provides or collects funds:

(a) intending that they be used, or knowing that they are to be used, in full or in part, in order to carry out one or more acts of a kind that, if they were carried out, would be one or more terrorist act; or

(b) intending that they benefit, or knowing that they will benefit, an entity that the person knows is an entity that carries out, or participates in the carrying out of, one or more terrorist act.

2.2 A 'terrorist act' (**terrorist act**) for the purpose of the Anti-Terrorism Act includes where a person conducts:

(a) an act or omission in or outside Saint Lucia which constitutes an offence within the scope of a counter terrorism convention;
(b) an act or threat of action in or outside Saint Lucia which—
  (i) involves serious bodily harm to a person,
  (ii) involves serious damage to property,
  (iii) endangers a person's life,
  (iv) creates a serious risk to the health or safety of the public or a section of the public,
  (v) involves the use of firearms or explosives,
  (vi) involves releasing into the environment or any part thereof or
  (vii) distributing or exposing the public or any part thereof—
    A. any dangerous, hazardous, radioactive or harmful substance,
    B. any toxic chemical,
    C. any microbial or other biological agent or toxin,
  (viii) is designed or intended to disrupt any computer system by the provision of services directly related to communications infrastructure, banking or financial services, utilities transportation
  (ix) or other essential infrastructure,
  (x) is designed or intended to disrupt the provision of essential emergency services such as police, civil defence or medical services,
  (xi) involves prejudice to national security or public safety, and is intended, or by its nature and context, may reasonably be regarded as being intended to—
    A. intimidate the public or a section of the public, or
    B. compel a government or an international organization to do, or refrain from doing, any act, and
    C. is made for the purpose of advancing a political, ideological, or religious cause;
(c) an act which—
  (i) disrupts any services, and
  (ii) is committed in pursuance of a protest, demonstration or stoppage of work, shall be deemed not to be a terrorist act within the meaning of this definition, so long and so long only as the act is not intended to result in any harm referred to in sub-paragraphs (i), (ii), (iii) or (iv) of paragraph (b);

2.3 Terrorist groups, like criminal organisations, must develop sources of funding, a means of laundering those funds and a way of using those funds to obtain materials and logistical items to commit terrorist acts. However, financial institutions (**FIs**) must be aware that funding for terrorist groups may be derived from legitimate sources. Indeed, terrorist financing frequently involves funds that, prior to being remitted, are unconnected to any illegal activity.

2.4 The Anti-Terrorism Act places a duty on a person to report to the Financial Intelligence Authority (**FIA**) suspicious activities and transactions which may relate to property owned or controlled by designated terrorist entities. The Anti-Terrorism Act provides for the exchange and mutual legal assistance in criminal matters in relation to terrorist groups or acts and empowers the Commissioner of Police to make account monitoring orders for the purposes of a terrorist investigation.

## 3. What is proliferation financing?

3.1 PF refers to the act of providing funds or financial services which are used, in whole or in part, for the development or production, or the facilitation of the development or production, of nuclear, radiological, biological of chemical weapons or systems for their delivery, in contravention of national or, where applicable, international laws.

3.2 PF differs from ML in that the pattern used by proliferators is a linear 'raise-obscure-procure & ship' pattern (rather than placement-layering-integration). The stages of this pattern are briefly described below:

(a) *raise* – funds are raised from overseas criminal activities, state budgets and overseas

commercial enterprises;

(b) *obscure* – proliferators rely on extensive networks of businesses (including front companies) and middlemen to obscure any connection on paper to sanctioned countries; and

(c) *procure & ship* – involves expenses associated with brokers, shippers, freight forwarders, insurance coverage for goods and technology that is intended to be delivered to conduit countries for final entry into a sanctioned country.

3.3 It is important to note that proliferation involves not only the purchase of weapons but also of individual goods and component parts that can be used to develop weapons or missiles, making proliferation activities more difficult to detect.

## 4. AML/CFT/CPF vulnerabilities

4.1 The continuing effort by governments globally to combat ML, TF and PF has made the work of the criminal more difficult. In part, as a means of circumventing AML/CFT/CPF measures, criminals have had to develop more complex schemes. This increase in complexity means that those individuals desiring to launder criminal proceeds – unless they have specialised professional expertise themselves – often turn to the expertise of legal professionals, accountants, financial consultants and other professionals to aid them in the movement of such proceeds.

4.2 The continuing ability of the finance industry to attract legitimate customers with funds and assets that are clean and untainted by criminality depends, in large part, upon Saint Lucia operating as a sound, well-regulated jurisdiction.

4.3 Any business that assists in laundering the proceeds of crime, or financing of terrorism, whether:

(a) with knowledge or suspicion of the connection to crime; or

(b) acting without regard to what it may be facilitating through the provision of its products or services,

will face the loss of its reputation, risk the loss of its licence or other regulatory sanctions (where regulated and supervised), damage the integrity of the finance industry as a whole, and may risk prosecution for criminal offences.

## 5. What are targeted financial sanctions?

5.1 Financial sanctions are restrictive measure put in place to limit the provision of certain financial services and/or restrict access to financial markets, funds or other assets to persons or entities. Determination of what is considered 'funds or other assets' has been defined by the FATF[3]. These are generally imposed to:

(a) coerce a regime, or individuals within a regime, into changing their behavior (or aspects of it) by increasing the cost on them to such an extent that they decide to cease the offending behavior;

(b) constrain a target by denying them access to key resources needed to continue their offending behavior, including the financing of terrorism or nuclear proliferation;

(c) signal disapproval, stigmatising and potentially isolating a regime or individual, or as a way of sending broader political messages nationally or internationally; and/or

(d) protect the value of assets that have been misappropriated from a country until these assets can be repatriated.

5.2 TFS are a specific type of financial sanction with stated objectives, one of which is the prevention of TF and PF. The term TFS refers to both asset freezing and restrictions and directions to prevent funds or other assets, including virtual assets, from being made available, directly or indirectly, for the benefit of designated persons and entities.

---

[3] According to the FATF, the term 'funds or other assets' means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds, or other assets, including, but not limited to, bank credits, travelers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.

5.3 There are two key international bodies which impose international sanctions measures; the United Nations through resolutions passed by the UN Security Council and the European Union through EU Regulations[4].

5.4 The Governor General through local designations can also impose domestic financial sanctions.

5.5 Once a person or entity has been designated in a sanctions order, there is a legal obligation not to transfer funds or make funds or other assets available, directly or indirectly, to that person or entity. FIs are required to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities.

5.6 The freezing of assets extends to all funds or other assets, including virtual assets, that are owned, held or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets that are wholly or jointly owned, held or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned, held or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

5.7 FIs are prohibited from making any funds, economic resources, other assets or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and/or entities; entities owned, held or controlled, directly or indirectly, by designated persons or entities; and persons and/or entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions.

[4] The EU Regulations do not apply to Saint Lucia but the Entity seeks to comply with them.

## C. Saint Lucia Legislative and Regulatory Framework

### 1. Introduction

1.1 Saint Lucia is committed to fighting ML, TF and PF. The competent authorities in Saint Lucia develop strategies to ensure that Saint Lucia responds to money laundering and terrorist financing threats and other issues in an effective manner and ensuring compliance with all relevant standards.

1.2 Saint Lucia is a member of the Caribbean Financial Action Task Force and has implemented the Financial Action Task Force's (**FATF**) 40 Recommendations on the Prevention of Money Laundering and the Countering of Terrorist Financing, which are international standards for effective AML and CFT regimes.

### 2. Key legislation

2.1 The key components of the AML/CFT/CPF and regulatory framework include:

(a) Money Laundering (Prevention) Act Cap.12.20 (as Amended) (the **MLPA**);

(b) Anti-Terrorism Act - Cap. 3.16 (as amended);

(c) Registration of Supervised Entities Act No.12 of 2023;

(d) Registration of Supervised Entities Regulations;

(e) Proceeds of Crime Act - Cap.3.04 (as amended) (the **PCA**);

(f) UN Sanctions (Counter-Proliferation Financing) Act No.29 of 2019

(g) Guidance to Reporting Entities on Suspicious Activity Reportin (May 2023)

(h) Guidance on the Identification & Verification of Beneficial Owners (May 2022)

(i) Guidance to MSBs (Class A-D) on their Sub-Agents (May 2022)

(j) Guidance on the Application of a RBA & Conduct of a Risk Assessment (March 2022)

(k) Guidance to Reporting Entities on CDD Measures (Oct 2021)

(l) Guidance to Reporting Entities on PEPs (Sept 2021)

(m) Guidance on Developing an AML/CFT/CPF Compliance Programme (March 2021)

(n) AML/CFT Guidelines for Money Remitters (Nov 2020)

(o) AML/CFT Guidelines for Attorneys-at-Law (Aug 2019)

(p) AML/CFT Guidelines for the Real Estate Sector (Aug 2019)

(q) Terrorist Disclosure Guidance to Reporting Entities

(r) AML/CFT/CPF Obligations of Reporting Entities

2.2 The Entity must familiarize itself and ensure that it complies with all relevant laws, regulations and other regulatory directives.

2.3 The MLPA is discussed in more detail in Part D (The MLPA, and other regulatory guidance) of this Manual below.

2.4 The AML/CFT legislation criminalises ML, TF and PF and imposes penalties and criminal sanctions for these offences. The commission of ML offences may lead to enforcement actions and/or prosecution. The main offences under the AML/CFT laws are summarised briefly below.

2.5 It is not necessary that the original offence from which the proceeds or property stems was committed in Saint Lucia if the conduct contravened the laws of the country in which it occurred and would also constitute an offence had it taken place in Saint Lucia. This is known as the concept of dual criminality.

---

[5] A list of the Orders in force in Saint Lucia is maintained by the FIA at https://www.slufia.com/. Whilst the sanctions programs maintained by the US Treasury Department's Officer of Foreign Assets Control (**OFAC**) do not have force of law in Saint Lucia, these sanctions should be taken into consideration where the Entity is connected to US persons or entities, or conducts business with any US persons or entities.

2.6 No duty is imposed on FIs to inquire into the criminal law of another country in which the conduct may have occurred. However, each FI should be aware of and understand the laws of the jurisdictions in which it operates. The relevant question is whether the conduct amounts to an indictable offence in Saint Lucia, or would if it took place in Saint Lucia. An FI is not expected to know the exact nature of criminal activity concerned or that the particular funds in question are definitely those that flow from the crime.

## 3. Outline of the offences

3.1 The main ML offences under the PCA are summarised briefly below.

(a) The PCA makes it an offence if a person enters into or is otherwise concerned in an arrangement which that person knows or suspects facilitates the acquisition, retention, use or control of proceeds of criminal conduct by or of that person or by or on behalf of another person.

(b) Under the PCA, a person commits an offence if that person acquires, transfers or uses any property or has possession of it which, in whole or in part, directly or indirectly represents the person's own proceeds of criminal conduct. It is also an offence if a person, knowing or suspecting that any property, in whole or in part, directly or indirectly, represents another person's proceeds of criminal conduct, acquires, transfers or uses that property or has possession of it.

(c) Under the PCA, it is an offence if a person conceals or disguises any property which is, or in whole or in part, directly or indirectly represents, the proceeds of criminal conduct, or converts or transfers that property or removes that property from Saint Lucia. It is also an offence if a person, knowing or having reasonable grounds to suspect that any property is, or in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct, conceals or disguises that property, or converts or transfers that property or removes it from Saint Lucia.

(d) The PCA creates the offence of failing to make a disclosure to the FIA as soon as reasonably practicable after it comes to the relevant person's attention where:

(i) a person knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and

(ii) the information on which the knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, came to that person's attention in the course of that person's trade, profession, business or employment.

(e) The PCA creates the offence of tipping off a target or third party about a suspicion, investigation or proposed investigation into ML, which is likely to prejudice such an investigation.

3.2 The main TF offences under the Anti-Terrorism Act are summarised briefly below.

(a) The Anti-Terrorism Act makes it an offence of TF for a person to, directly or indirectly, wilfully and without lawful justification or reasonable excuse, provide or collect funds:

(i) intending that they be used, or knowing that they are to be used, in full or in part, in order to carry out one or more acts of a kind that, if they were carried out, would be one or more terrorist act; or

(ii) intending that they benefit, or knowing that they will benefit, any entity that the person knows is an entity that carries out, or participates in the carrying out of, one or more terrorist act.

(b) The Anti-Terrorism Act, a person commits an offence if that person, without lawful justification or reasonable excuse, deals with any property knowing that the property is owned or controlled, directly or indirectly, by a designated terrorist entity, or derived or generated from that property.

(c) The Anti-Terrorism Act makes it an offence to make available, or cause to be made available, directly or indirectly, without lawful justification or reasonable excuse, any property, or any financial or related services, either to or for the benefit of an entity, knowing that the entity is a designated terrorist entity.

(d) The Anti-Terrorism Act, it is an offence if a person enters into or becomes concerned in an arrangement as a result of which terrorist property is made available or is to be made available to another, and that person knows or has reasonable cause to suspect that it will or may be used for the purposes of financing terrorism or the commission of one or more terrorist acts.

(e) The Anti-Terrorism Act, a person commits an offence if that person enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property by concealment, removal from the jurisdiction or transfer to nominees.

(f) Where an offence under the Anti-Terrorism Act committed by a body corporate is proved to have been committed with the consent or the connivance of an officer of the body corporate, or to be attributable to any act or default on the part of that officer, the officer as well as the body corporate will be guilty of an offence.

(g) The Anti-Terrorism Act imposes an obligation on a person, who knows or suspects, or has reasonable grounds for knowing or suspecting, through the course of that person's trade, profession, business or employment, that another person is engaged in the financing of terrorism or is seeking to engage in one or more terrorist acts, to report such information or other matter to the FIA as soon as reasonably practicable after it comes to that person's attention. Failure to make a disclosure is an offence. It is also an offence if a person knows or suspects that a report of suspicious information is being or had been made to the FIA and that person discloses to any other person information or any other matter which is likely to prejudice any investigation which might be conducted.

3.3 PF is an offence which takes place when a person makes available an asset, provides a financial service, or conducts a financial transaction, and the person knows that, or is reckless as to whether, the asset, financial service or financial transaction is intended, in whole or in part, to facilitate any of the following activities, regardless of whether such activity occurs or is attempted:

(a) the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, export, transhipment or use of (i) nuclear weapons; (ii) chemical weapons; (iii) biological weapons; or (iv) materials related to nuclear weapons, chemical weapons, biological weapons or radiological weapons that are prescribed by regulations or restricted or prohibited under any enactment relating to export or import controlled measures; and

(b) the provision of technical training, advice, service, brokering or assistance related to any of the activities mentioned in paragraph (a) above.

3.4 The other PF offences include the following:

(a) it is an offence if a person deals with an asset knowing that, or reckless as to whether, the asset is owned, controlled or held, directly or indirectly, wholly or jointly, by a designated person or entity[6], on behalf of a designated person or entity, or at the direction of a designated person or entity.

(b) it is an offence if a person makes an asset available knowing that, or reckless as to whether, it is being made available, directly or indirectly, wholly or jointly, to a designated person or entity, a person or entity owned or controlled by a designated person or entity, a person or entity acting on behalf of a designated person or entity, or for the benefit of a designated person or entity.

3.5 There is an obligation is imposed on any person who holds an asset of a designated person or entity to report the holding of such asset to the FIA as soon as reasonably practicable and, in any case, within five wording days from the date that person received notification of the designation or the date of publication of the designation in accordance with the PFPA, or the date when that person became aware that the asset belongs, or is connected, to the designated person or entity (whichever occurs first).

3.6 The designation of a person or entity by the United Nations Security Council or its Committees under a UN Security Council Resolution which will apply in Saint Lucia pursuant to the UN Sanctions (Counter-Proliferation Financing) Act No.29 of 2019[7].

3.7 The FIA has issued Financial Sanctions Guidelines for the public, which can be accessed at https://www.slufia.com/

## 4. Outline of the defences

4.1 There are general defences enabling a defendant to prove, for example, that the defendant did not suspect that an arrangement related to the proceeds of criminal conduct or that it facilitated retention or control of the proceeds by the criminal. There are also specific defences provided by reporting a suspicious transaction. It will not be an offence to act in accordance with an arrangement which would otherwise be a crime if a report is made of the suspicion about the source of the funds of investment. If a disclosure of the arrangement is made before the action

---

6 'Designated person or entity' is a person or entity designated by the competent authorities in St Lucia or by the United Nations Security Council or its Committees pursuant to a resolution in relation to a designated country.

7 See UN Sanctions (Counter-Proliferation Financing) Act No.29 of 2019

in question or volunteered as soon as it reasonably might be after the action, no offence is generally committed.

4.2 An employee who makes a report to his employer in accordance with established internal procedures is specifically protected by the PCA.

4.3 To avoid tipping off, caution must be adopted in determining what may be disclosed to a customer in the event that a Suspicious Activity Reporting (**SAR**) is made to the FIA or information is obtained regarding an ML investigation.

**5. Making a suspicious activity report to the FIA**

5.1 A report of a suspicious activity made to the FIA does not give rise to any civil liability to the customer or others and does not constitute, under St Lucia law, a breach of confidentiality. There are statutory safeguards governing the use of information received by the FIA.

5.2 A SAR must be made to the CO in all circumstances where there is knowledge or suspicion or reasonable grounds for suspicion of ML and/or TF, or that any property constitutes or represents the proceeds of criminal conduct or is or may be of terrorist property.

5.3 The full policy and procedures can be located at Part J (CO and Internal Controls) of this Manual. Contact the CO for further details or information on reporting obligations.

**D. The MLPA, and other regulatory guidance**

**1. Who do the MLPA apply to?**

1.1 The MLPA have the force of law and lay down the general compliance requirements relating to conduct to be taken by a reporting entity.

**2. Requirements of the MLPA**

2.1 The MLPA require relevant persons to establish and maintain systems to detect ML/TF, and therefore assist in the prevention of abuse of their financial products and services. This is in the commercial interests of those businesses and it also protects the reputation of Saint Lucia.

2.2 In order to comply with the requirements of the MLPA, the relevant person must:

(a) establish and maintain prescribed measures to prevent and detect ML and TF (including identification and verification procedures in respect of an applicant for business[10], record keeping procedures, internal reporting procedures and internal controls and communication procedures which are appropriate for the purposes of forestalling and preventing money laundering);

(b) provide training to all of the relevant person's directors (or partners), all other persons involved in the relevant person's management and all key staff to ensure that they are aware of the relevant laws and regulations, the relevant regional and international conventions and standards of compliance established by relevant organisations on ML and TF; their personal and the relevant person's obligations and liabilities on ML and TF under the relevant laws and regulations; and the AML/CFT manual of compliance procedures or internal control systems, and training with respect to the relevant person's AML/CFT systems, policies and procedures;

(c) establish and maintain prescribed measures where the relevant person relies on the introduction of an applicant for business by a third party;

(d) appoint a Compliance Officer (**CO**);

(e) maintain a register of all reports made by the relevant person to the FIA and all inquiries relating to ML made of the relevant person by the FIA; and

(f) establish written internal SAR procedures.

**3. AML/CFT/CPF Manual**

3.1 This Manual is designed to assist the Entity in complying with its obligations under Saint Lucia AML/CFT/CPF legislative and regulatory framework. This Manual must be maintained and reviewed periodically in relation to the entry, verification and recording of customer information and reporting procedures. The frequency of review should be based on the size, nature and complexity of the Entity. However, as a minimum, this Manual should be reviewed at least annually or where there are significant changes to the AML/CFT/CPF systems and obligations.

3.2 This Manual has been adopted by the Management of the Entity. It should be read by all directors, officers and employees of the Entity (as applicable) and read in conjunction with legislation and guidance issued by the relevant Saint Lucian competent authorities.

3.3 The CO will periodically review this Manual to ensure its appropriateness.

## 4. Key contact for AML questions

For further guidance and information in respect of either the interpretation of the policies and procedures contained in this Manual or the regulatory AML/CFT requirements, please consult the CO.

## E. AML/CFT Strategy

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. AML/CFT strategy

1.1 The Entity recognises and acknowledges the importance of the need to forestall and prevent money laundering and to counter the financing of terrorism and therefore a formal strategy has been established and is set out below.

*1.2 General*

The Entity will:

(a) have the highest regard for the protection of its business against any involvement in ML or TF, ensuring that it understands the relevant regulations and enactments, including the duties of the CO;

(b) ensure that this Manual is adopted and reviewed in accordance with the laws of Saint Lucia;

(c) ensure that the AML/CFT policies and procedures set out in this Manual are developed and maintained in line with St Lucia statutory and regulatory obligations;

(d) actively promote the importance and need for systems and controls to forestall, prevent and detect ML or TF; and, wherever possible, ensure that the Entity is able to keep ahead of new methodologies of ML or TF;

(e) be accountable for identifying the Entity's risks and adopting and documenting systems and controls (including policies and procedures) to manage those risks;

(f) ensure that the Entity considers and meets its AML/CFT requirements on a regular basis. This will include, but not be limited to, the receipt of regular compliance reports, ensuring any failings identified are addressed promptly and appropriately;

(g) appoint a designated CO;

(h) report through the CO to the FIA where there are reasonable grounds to suspect that an offence of ML, financing terrorism or financing criminal activity (including engaging with property which constitutes or represents the proceeds of criminal conduct, or is or may be terrorist property) has been or is being committed;

(i) take all reasonable steps to establish the identity of any person for whom it is proposed to provide any products or services and verify the identity where necessary;

(j) retain identification, transactional and any other documentation as required by the laws of Saint Lucia; and

(k) provide initial and ongoing AML/CFT/CPF training to ensure that all employees are aware of their personal responsibilities and the AML/CFT/CPF procedures in respect of identifying applicants for business/customers[8], record-keeping, remaining vigilant at all times and reporting any suspicious activity or transactions.

*1.3 Communications with the regulator/supervisory authorities*

(a) The Entity will maintain a positive and open relationship with the supervisory authorities in Saint Lucia, based upon mutual trust and co-operation. The Entity will maintain clear communication lines to ensure that the supervisory authorities receive an appropriate and consistent message.

(b) The Entity's Management will be informed immediately of non-routine or material communications from the regulator or other regulatory/enforcement authorities. This also applies to all proposed outward communications, including planned meetings or telephone calls or written communications.

---

[8] References to an 'applicant for business' or 'applicant' relate to a prospective customer or/investor in the Entity, and references to a 'customer' relate to a person with whom a business relationship has been formed by the Entity.

*1.4 Legal advice*

Whenever required, the CO may obtain advice from legal counsel, as and where they deem appropriate.

*1.5 Training*

(a) Employees will receive appropriate AML training within a prescribed period following the commencement of their employment and at regular intervals thereafter.

(b) The Entity will provide, at regular intervals, further relevant AML and CFT awareness training to all those deemed applicable.

## 2. Purpose of the strategy

2.1 This strategy has been adopted to:

(a) forestall, detect and report any known or suspected involvement in or with ML, TF, PF, criminal activity or activities or persons subject to TFS, by the Entity;

(b) reduce the risk that funds managed or received by the Entity are being used in or for ML, TF, PF, criminal activity or activities or persons subject to TFS;

(c) ensure appropriate scrutiny is exercised when establishing business relationships to identify ML, TF, PF, criminal activity or activities or persons subject to TFS;

(d) ensure increased scrutiny is exercised when establishing relationships involving connections with those countries known for ML, terrorism, corruption, financial crime and financial irregularity;

(e) mitigate the risk of and protect the Entity against being used for the purpose of ML, TF, PF, criminal activity or activities or persons subject to TFS; and

(f) ensure identification and compliance with the statutory and regulatory requirements that govern the provision of financial services as they relate to AML, CFT, CFP, criminal activity and TFS.

## F. CPF Strategy

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. CPF strategy

1.1 The Entity recognises and acknowledges the importance of the need to forestall and prevent proliferation financing and therefore a formal strategy has been established and is set out below.

*1.2 General*

The Entity will:

(a) carry out appropriate CDD on applicants for business/customers in accordance with this Manual, which includes screening names of clients and related parties, counterparties against sanctions lists;

(b) implement risk based systems and controls to detect PF; and

(c) carry out risk assessments to determine the Entity's exposure to PF risk, which will (amongst other things) consider risks relating to geography, customers and products and services (each of which are considered below).

*1.3 Customers*

The Entity will:

(a) determine the exposure of applicants for business/customers to the manufacture, trade or provision of expertise or consulting services relating to sensitive or dual use goods or technology;

(b) given the potential difficulties of identifying applicants/customers that are involved with sensitive goods and technology, identify the applicants/customers that pose a smaller risk of PF and concentrate on gathering more information from the customers that remain;

(c) be aware of the transactions of the Entity's applicants/customers, particularly paying attention to payments being made to the importers/exporters, shipping agents, brokers and freight forwarders, especially where controlled and dual use goods are being shipped to conduit countries (those near sanctioned countries).

*1.4 Geography*

The Entity will:

(a) determine its level of business (including applicants/customers and beneficial owners) with sanctioned countries as well as with countries that are known to have ties with sanctioned countries;

(b) remain informed about the countries that present a higher risk for PF;

(c) identify its business relationships, including correspondent banking relationships with partners and financial services providers located in the above-noted jurisdictions; and

(d) identify applicants/customers with payments to importers/exporters, shipping agents, brokers and freight forwarders that export to countries and ports near the border of sanctioned countries.

*1.5 Products and services*

The Entity will:

(a) be aware of its exposure to proliferation; for example, shipping insurance and insurance against certain risks in the trading process is a financial product highly sought by proliferators;

(b) to avoid proliferators using trade finance to assist with the procurement and movement of goods, determine the amount of business conducted in loans or credit facilities to facilitate export transactions, purchasing promissory notes or bills of exchange from foreign banks to exporters, purchase of discounted foreign accounts receivable and provisions of guarantees to or on behalf of exporters; and

(c) consider whether the Entity provides loans, financing or credit to applicants/customers in sensitive industries or to entities in higher risk jurisdictions; noting that loan repayments may be made from corporate structures linked to jurisdictions near, but not necessarily in, sanctioned jurisdictions like Iran and North Korea.

**2. Controls and ongoing monitoring**

In accordance with this Manual, the Entity will:

2.1 implement risk-based anti-proliferation and PF policies and procedures, including internal escalation and external reporting procedures; and

2.2 screen all incoming and outgoing transactions against lists of entities and persons designated under the relevant international sanctions regime.

## G. TFS Strategy

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. TFS strategy

1.1 The Entity recognises and acknowledges the importance of the need to comply with the sanctions regimes applicable in Saint Lucia and therefore a formal strategy has been established and is set out below.

*1.2 Compliance with obligations*

The Entity will comply with its legal obligations to:

(a) regularly monitor the sanctions in place including the local designations made by the the competent authorities;

(b) review applicants/customers against the lists of designated persons or entities and the consolidated lists maintained by the competent authorities;

(c) freeze any accounts, other than funds or economic resources belonging to, owned, held or controlled by designated persons or entities;

(d) refrain from dealing with funds or assets or making them available to designated persons or entities, unless licensed by the competent authorities;

(e) report to the FIA, as soon as practicable, if it knows or has reasonable cause to suspect that a person is a designated person or has committed an offence under the legislation; and

(f) disclose to the FIA, via the designated Compliance Reporting Form available at the FIA's website[9], details of any frozen funds or other assets or actions taken in compliance with the prohibition requirements of all applicable sanctions, including attempted transactions.

*1.3 Sanctions hits*

(a) The Entity will maintain a record of any potential matches (or 'hits') to names on sanctions lists and related actions, whether the match turns out to be a true match or a false positive.

(b) Such records of sanctions hits will contain, as a minimum:

(i) the basis or other grounds which triggered the match;

(ii) any further checks or enquiries undertaken;

(iii) the associated sanctions regime;

(iv) the person(s) involved, including any members of compliance or senior management who authorized treatment of the match as a false positive;

(v) the nature of the relationship with the person or entity involved, including attempted or refused transactions; and

(vi) subsequent action taken (eg freezing of funds).

[9] See https://www.slufia.com/document-categories/downloadable-forms

## H. Risk Assessment Policy

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. Risk assessment policy

1.1 The possibility of being used to assist with ML, TF, PF or activities or persons subject to TFS poses many risks for businesses which invest, administer or manage funds or money on behalf of other persons, including criminal and disciplinary sanctions, civil action and damage to reputation. These risks must be identified, assessed and mitigated.

1.2 The Entity is obliged to identify, assess and understand its ML, TF and PF risks, taking into account:

(a) the type of applicants for business/customers;

(b) their countries or geographic areas of residence or operation;

(c) the Entity's products, services or transactions; and

(d) the delivery channels[10] of the Entity.

1.3 Accordingly, the Entity will:

(a) conduct and document an AML/CFT/CPF business risk assessment in line with the requirements of the MLPA;

(b) ensure that each new business relationship entered into is assessed for risk, which will include a review of the applicant/customer and the nature of transaction or relationship concerned;

(c) ensure that all applicants, customers and associated parties are assessed in accordance with the risk assessment procedures set out in this Manual; and

(d) risk assess third party introducers or intermediaries where reliance is placed upon such parties for the purpose of customer due diligence (**CDD**).

1.4 The Entity has developed CDD procedures that take into account risk, and require the application of enhanced customer due diligence (**EDD**) procedures to higher risk applicant/customer relationships and to applicant/customer relationships where risk factors have been identified and ongoing monitoring of such relationships.

1.5 This policy is to be read in conjunction with the MLPA.

1.6 This policy has been adopted to:

(a) comply with legal obligations;

(b) determine the Entity's exposure to AML/CFT/CPF risk at overall business relationship level and at applicant/customer level;

(c) determine the extent and nature of the CDD measures to be undertaken and the level of ongoing monitoring required;

(d) establish the frequency of applicant/customer and business relationship reviews and CDD information updates based upon the applied risk rating; and

(e) mitigate risk and protect the Entity being used for the purpose of ML, TF, PF, financial crime or activities or people subject to TFS.

### 2. The risk based approach explained

2.1 A risk based approach is aimed at providing flexibility, ensuring that businesses identify and understand the risks associated with undertaking their particular business and allowing for greater focus on those areas of higher risk.

2.2 A risk based approach requires all FIs to have appropriate and consistent policies and procedures, which should be designed and maintained with specific reference to the risks that FI may be exposed to during the course of conducting its business. For systems and controls

---

[10] 'Delivery channel' in this context means the way or means whereby the Entity carries on its business relationship with a customer, ie directly or through other means such as email, internet, intermediary or any correspondent institution.

(including policies and procedures) to be adequate and effective in preventing and detecting ML, TF and PF, and ensuring compliance with TFS, they will need to be appropriate to the circumstances and business of the Entity.

2.3 The regulatory authorities in Saint Lucia will be looking at the adequacy of the Entity's policies, procedures and controls, including how such policies, procedures and controls have been maintained and how successful they have been.

## 3. Business risk assessments

3.1 The Entity shall conduct a risk assessment to identify and assess the risks of ML, TF and PF to the business and to ensure that its policies, procedures and controls are effective and appropriate to the assessed risks as a whole.

3.2 The Entity must regularly review the business risk assessment, so as to keep it up to date and must have regard to risk, taking into account but not limited to:

(a) the Entity's risk appetite;

(b) the nature, scale and complexity of the Entity's business;

(c) applicant/customer base;

(d) applicant/customer geography;

(e) cultural barriers;

(f) AML/CFT/CPF technological developments; and

(g) business and operating AML risks, including (where applicable) considering the risk that is involved in placing reliance on third parties to apply identification measures.

3.3 The Entity may demonstrate that its business risk assessment is kept up to date where it is reviewed when events (internal and external) occur that may materially change ML, TF and PF risk.

## 4. Customer risk assessments

4.1 As well as conducting a business risk assessment, the Entity is also required to conduct risk assessments of its applicants and customers, including risk posed by the:

(a) combination and complexity or products, services and delivery channels that the applicant/customer uses;

(b) geographical location of the applicant/customer (eg the countries in which the applicant/customer (and its beneficial owner(s)) reside or from which they operate); and

(c) applicant/customer's characteristics, nature and purpose of the relationship or nature of the transaction.

4.2 Each person who is responsible for accepting new business from an applicant or customer must ensure that there is sufficient information available to conduct a risk assessment in relation to that individual applicant/customer and the overall nature of the business relationship to be commenced. The gathering of identification and verification of identity information is to be completed at the commencement of a business relationship or within a reasonable timeframe thereafter.

4.3 The scope and nature of identification, verification and due diligence information to be collected on a particular customer will be determined by the level of risk associated with the customer, as high, medium or low.

4.4 The category of **low risk** factors may include the following:

(a) *customer risk factors* - where the customer is:

(i) a person which is subject to and required to comply with the MLPA, or a majority-owned subsidiary of such a person;

(ii) a central or local government organization, statutory body or agency of government in a country assessed as having a low degree of risk of ML and TF;

(iii) acting in the course of a business (or is a majority-owned subsidiary of the business) in relation to which an overseas regulatory authority exercises regulatory functions and is based, incorporated or formed in a country assessed as having a low degree of risk of ML and TF and

(iv) a company which is listed on a recognised stock exchange and subject to disclosure requirements imposing requirements to ensure adequate transparency of beneficial ownership, or a majority-owned subsidiary of such a company; and

(b) *country/geographic risk factors* - countries or geographic areas which have been assessed as having a low degree of risk of ML and TF.

4.5 There can never be a finding of low risk where there is knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of ML or TF.

4.6 The category of **high risk** factors includes the following:

(a) *customer risk factors* - where the customer, any connected entity or intermediary, or a counterparty is:

(i) a sanctioned individual/entity;

(ii) a PEP;

(iii) involved in any sanctioned activity;

(iv) a company with nominee shareholders or bearer shares; and

(v) the subject of an adverse search,

or where the ownership structure of the customer appears unusual or excessively complicated given the nature of the customer's business;

(b) *country/geographic risk factors (including corruption risk)* - where the customer, any connected entity or intermediary, or a counterparty is incorporated or resident in, or operates from, a jurisdiction which:

(i) is identified by credible sources[11] as not having adequate AML/CFT systems;

(ii) has high levels of organised crime;

(iii) has strong links (such as funding or other support) with terrorist activities, or that are known to have designated terrorist organisations operating within their borders;

(iv) is vulnerable to corruption; and

(v) are the subject of embargos, sanctions or similar measures by, for example, the UN, EU, the United Nations or OFAC[12]; and

(c) *product, service, transaction or delivery channel risk factors*:

(i) anonymous transactions (which may include cash);

(ii) non-face-to-face business relationships or transactions; and

(iii) payments received from unknown or un-associated third parties.

4.7 The MLPA provides additional risk classification factors.

## 5. Risk tolerance and residual risk

5.1 Risk tolerance is the amount of risk that the Entity is willing and able to accept. The Entity's Management will establish and, on an ongoing basis, consider the Entity's risk tolerance and appetite.

5.2 In establishing the risk tolerance, the extent of the Entity's exposure to ML and TF risks must be considered 'in the round' or as a whole by reference to its organisational structure, its applicants/customers, the countries and territories with which its applicants/customers are connected, its products and services, and how it delivers those products and services. The assessment must consider the cumulative effect of risks identified, which may exceed the sum of each individual risk element.

---

11 Such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, the International Monetary Fund, the World Bank, the OECD, the UN and MoneyVal.

12 A list of the Orders in force in Saint Lucia is maintained by the FIA. Details of the sanctions programs administered by OFAC can be found at https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.

5.3 When the Entity's risk tolerance has been established, the Entity's Management must also consider the residual risk faced by the Entity. Residual risk is the risk remaining after taking into consideration the mitigation measures and controls put into place to address the AML/CFT/CPF risks facing the Entity.

## 6. Suspicious activity reporting and the risk based approach

The risk based approach does not apply to the reporting of suspicious activity. See Part J (CO and Internal Controls) of this Manual below.

## 7. New products and technologies

7.1 All new products, services and systems will be subject to a risk assessment to assess whether the product, system or service can be used to improve controls, reduce risks and whether the new service, products or system exposes the Entity, its directors, officers or employees (as applicable) or its applicants/customers to any risks of ML, TF or PF.

7.2 Where the Entity has identified a risk that may arise in relation to new products, services, business practices or technology, including where developed at group level or by outside developers (locally and elsewhere), the Entity will:

(a) take steps to ensure that those involved in their development or implementation have a basic awareness of ML and the financing of terrorism and proliferation, and of current money laundering techniques, methods and trends; and

(b) identify any additional steps or actions required to mitigate the risk(s) identified; and

(c) take steps to implement those steps or actions.

7.3 The Entity will record each risk assessment undertaken in relation to a new product, system or service and provide evidence supporting the conclusions reached and any actions taken to mitigate the risks identified.

## I. Risk Assessment Procedures

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. Business risk assessments

1.1 The Entity is required to identify and assess the ML/TF risks that it faces with regard to:

(a) its customers and the countries or geographic areas from which they reside or operate; and

(b) the products/ services that it offers and the delivery channels by which those products/services are delivered to the customers/investors.

1.2 To assist with risk assessments and their documentation, the Entity has adopted the forms of risk assessment questionnaire contained at Schedule 1 (Form of Risk Assessment Questionnaire) and the risk assessment record at Schedule 2 (Form of Risk Assessment Record).

1.3 The CO has completed a risk assessment and has chosen to assess the Entity's risk or susceptibility to ML or TF as high. This risk assessment has been recorded by the CO using a risk assessment record.

1.4 The CO will review the risk assessment described above on at least an annual basis, or in the event of major changes which are likely to affect the Entity's AML/CFT risks. A risk assessment record will be completed by the CO in respect of each annual review.

### 2. Customer risk assessments

2.1 The Entity is also required to conduct risk assessments of its customers, including risk posed by the:

(a) combination and complexity or products, services and delivery channels that the customer uses;

(b) geographical location of the customer (eg the countries in which the customer (and its beneficial owner(s)) reside or from which they operate); and

(c) customer's characteristics, nature and purpose of the relationship or nature of the transaction,

2.2 To assist with customer risk assessments and their documentation, the Entity has adopted the form of customer risk assessment questionnaire contained at Schedule 3 (Form of Customer Risk Assessment).

2.3 Each person who is responsible for accepting business from a new applicant/customer must:

(a) review all information/documentation provided by the applicant/customer;

(b) conduct a risk assessment in the form set out at Schedule 3 (Form of Customer Risk Assessment); and

(c) determine the level of risk associated with the applicant/customer, as high, medium or low.

2.4 Where a customer or business relationship is assessed as presenting a higher risk, or where specific scenarios are identified, appropriate EDD must be performed.

2.5 Where a lower risk finding has been reached in respect of a customer or business relationship, AML/CTF Legislation allows SDD to be applied.

### 3. Updating CDD and customer risk assessments

3.1 Risk assessment is an ongoing process both for the Entity generally and for each business relationship. A comprehensive understanding of the risk presented by a customer/business relationship may only become evident at a later stage following the establishment of a relationship. The information gathered initially and that acquired during the course of the business relationship will inform the risk assessment and enable risks to be re-assessed.

3.2 If, following completion of identification procedures as part of the periodic review of a customer's risk and CDD documentation, the risk rating of a customer has changed from low to medium or medium to high, a copy of the updated customer risk assessment and accompanying materials must be sent to the CO for review.

3.3 In the case of a business relationship assessed as presenting higher risk:

(a) that relationship shall be placed on a high risk customer and transaction register; and

(b) the CDD information (including all documents, data and information obtained under identification measures) gathered in relation to each customer/business relationship placed on the high risk register shall be reviewed on at least an annual basis for the life of that relationship, to ensure that it remains up to date.

3.4 Where a customer/business relationship is considered higher risk due to a PEP connection:

(a) the PEPs shall be recorded on a PEP register; and

(b) ongoing monitoring of the PEP shall be required throughout the life of the business relationship.

3.5 CDD for an existing customer/business relationship shall be reviewed upon the entry by the Entity into a new transaction with that customer, regardless as to when that last transaction occurred. The CDD status date will not however be updated unless any material updates are required.

3.6 In the case of other relationships, the Entity may demonstrate that its CDD information remains up to date where it is reviewed and updated on a risk sensitive basis, including where additional factors to consider (see risk factors to consider above) become apparent.

**4. Trigger events for new and existing customers**

4.1 Certain trigger events, eg upon entering into a new business transaction with a customer, notification of a change of address, CDD held over 3 years old or in accordance with the relevant risk rating, change of name or meeting with a customer may also present a convenient opportunity to update CDD information.

4.2 Where the Entity becomes aware of any of the following issues relating to an existing customer (irrespective of risk rating), identification procedures must be applied, always under the advice or guidance of the CO:

(a) where there is a suspicion of ML, TF or PF; or

(b) where there are doubts about the veracity or adequacy of documents, data or information that the Entity has previously obtained for the purposes of CDD measures.

4.3 Where it is identified that there has been a change to any of the following relating to an existing customer, identification procedures must be applied:

(a) the identification information of a customer (ie name, residential address, nationality);

(b) the beneficial ownership or control of a customer; or

(c) changes to third parties (ie the underlying person on whose behalf a customer acts).

4.4 Where the Entity becomes aware of any of the following relating to an existing customer, it is necessary to review and consider the adequacy of documents held on file prior to proceeding with the transaction or business relationship, irrespective of whether the CDD status of the customer is verified:

(a) where a high risk factor is identified which was not previously identified (eg the customer has become a PEP, adverse information is obtained or the customer has become connected with a high risk country or business);

(b) when an existing standard or lower risk customer is involved in a new higher risk transaction; or

(c) where the CDD on file was last verified more than three years ago or in accordance with the relevant risk rating.

4.5 If, following completion of identification procedures following a trigger event, the risk rating of a customer has changed from low to medium or medium to high, the updated customer risk assessment and accompanying materials must be sent to the CO for review and for entry into the high risk customer and transaction register in accordance with Part M (Record Retention Policies and Procedures) of this Manual.

## J. CO and Internal Controls

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. CO

1.1 The Entity is required to designate a person of sufficient seniority to act as the CO. The Entity is exempt from the requirement to appoint a person to act as the Compliance Officer and has not elected to appoint a Compliance Officer. The CO will perform the applicable functional responsibilities of a Compliance Officer.

1.2 The name and contact details of the CO designated by the Entity are set out below:

Limbani Vishal Vallabhbhai

Telephone: +1 519 330 4688

Email: Limbanivishal1991@gmail.com

The CO shall:

(a) be the Entity's point of contact with the supervisory and other competent authorities in Saint Lucia;

(b) respond promptly to any requests for information from such authorities;

(c) review, develop and maintain the AML/CFT systems and procedures set out in this Manual in line with the requirements of this Manual and the evolving requirements of Saint Lucia's AML/CFT regime;

(d) ensure the high risk customer and transaction register and the PEP register are maintained in line with the policies and procedures set out in this Manual;

(e) ensure regular audits of the Entity's AML/CFT programme in accordance with the internal control procedures set out in this Manual;

(f) advise the Entity's Management of any AML/CFT compliance issues that need to be brought to their attention;

(g) report periodically (and, in any event, at least annually) to Management on the Entity's AML/CFT systems and controls, including by preparing and submitting an annual compliance report to the Entity's board of directors.

1.3 The CO shall be responsible for the following:-

(a) employee screening (where applicable);
(b) anti-money laundering training (where applicable);

1.4 The Compliance Officer has functional responsibility for:

(a) ensuring that the Entity complies with its obligations with respect to the establishment and maintenance of compliance systems and controls (to the extent applicable to the Entity);

(b) identifying, measuring and assessing the compliance risks associated with the Entity's business, including the compliance risks associated with the material changes or the development of new, products, types of business or customer relationships;

(c) keeping the regulatory obligations of the Entity and the compliance systems and controls under review, identifying any deficiencies, making regular assessment reports to the Entity's board of directors and senior management and making recommendations for any updates or revisions;

(d) establishing and maintaining this Manual and keeping this Manual under regular review and current;

(e) maintaining a register of compliance breaches containing information on the date, nature and extent of each compliance breach and whether the breach has been reported;

(f) ensuring that the Entity's staff are aware of the need for and the objectives of compliance and that they are familiar with, and understand, to the extent

necessary to undertake their responsibilities;

(i) the regulatory regime, and any changes to it; and

(ii) this Manual;

(g) ensuring that the Entity complies with its reporting obligations;

(h) establishing and maintaining procedures for the monitoring and handling of complaints, and keeping the complaints procedures under review.

1.5 In addition to the above, where there are further anti-money laundering precautions that need to be taken into consideration, the CO will ensure:-

(a) implementation and monitoring of the day-to-day operations and internal controls of the anti-money laundering programme; and overseeing the implementation of the requirements of this Manual.

(b) appropriate reporting to the board of directors on anti-money laundering and compliance issues;

(c) reflection in the supervisory policies and procedures of the Entity any applicable changes in the law, reporting rules, and industry best practices; and

(d) an annual review and monitoring of client information

1.6 The CO is responsible for:

(a) ensuring that any incidents of suspicious activity are reported to the Financial Intelligence Authority (the **FIA**) and are filed in accordance with the applicable legislation; and

(b) maintenance of a register listing reports made to the FIA and inquiries received from the FIA.

1.7 The CO of the Entity will monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non cooperative" are involved, or any of the "red flags" identified below.

1.8 The CO is responsible for monitoring and reviewing the Entity's transactions, including reviewing trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual strategy for that client. The CO will be responsible for this monitoring, will document when and how it is carried out and will report suspicious activities. The CO on an ongoing basis will identify, measure and assess the compliance risks associated with the Entity's business including the compliance risks associated with material changes in, or the development of, new products, types of business or customer relationships.

## 2. Suspicious Activity Indicators

2.1 During the course of a relationship with a client, the Entity, employees, the CO should be wary of certain risk indicators, these generally fall into two categories:-

(a) suspicious client behaviour, and

(b) suspicious transactions.

2.2 Examples of client behaviour suspicious activity indicators include:-

(a) activity that is inconsistent with the business or financial background, investment strategy or stated business strategy;

(b) refusal or delays in producing requested client identification documentation;

(c) no concern for investment risks, performance, commissions or other transaction costs;

(d) where the client has been the subject of significant regulatory or governmental inquiries;

(e) where the client source of funds information is false, misleading, or substantially incorrect; and

(f) where the client appears to be acting as an agent for an undisclosed principal but declines to provide information regarding that person's identity.

2.3 Examples of transactional suspicious activity indicators include:-

(a) frequent large purchases or movement of funds, especially to or from foreign banks or third parties;

(b) investing a significant amount of money into a long-term investment and then liquidating it within a short time period, this demonstrates a lack of concern for penalties or associated fees;

(c) conducting a transaction with the goal of moving along funds or securities, rather than obtaining a favourable return; and

(d) engaging in transactions involving cash and cash equivalents that appear structured to avoid any government reporting requirements.

## 3. Review of the AML/CFT/CPF policies and procedures

3.1 On at least an annual basis, the CO will ensure that a complete review of the Entity's AML/CFT/CPF systems, policies and procedures is undertaken.

3.2 The annual review will include a review of each policy to determine the following:

(a) adequacy;

(b) effectiveness;

(c) accuracy;

(d) appropriateness for the Entity's current activities;

(e) current regulatory requirements;

(f) any prior policy issues, violations or sanctions; and

(g) any changes or updates that may otherwise be required or appropriate.

3.3 The annual review process should also consider and assess the risk areas for the Entity and review and update any risk assessments in view of any changes in services, customer base, regulatory developments or any other relevant factors.

3.4 The CO will coordinate the review of each policy with an appropriate person, to ensure that each of the Entity's policies and procedures is adequate and appropriate for the business activity covered.

3.5 The CO will revise or update the policies and/or procedures set out in this Manual as necessary or appropriate and obtain the approval of the Entity's Management as part of the review.

3.6 The CO will maintain hardcopy or electronic records of the Entity's AML/CFT/CPF policies and procedures as in effect at any particular time following the adoption of this Manual.

3.7 The CO will maintain an annual compliance review file for each year which will include and reflect any revisions, changes, updates and materials supporting such changes and approvals, of any of the firm's policies and/or procedures.

3.8 The CO will also conduct more frequent reviews of the Entity's AML/CFT/CPF policies and procedures, or any specific policy or procedure, in the event of any change in business activities, personnel, regulatory requirements or developments, or other circumstances requiring a revision or update.

## 4. Testing of the AML/CFT/CPF systems, policies and procedures

4.1 The CO has overall responsibility for monitoring and testing compliance with the Entity's AML/CFT/CPF policies and procedures.

4.2 The Entity has adopted various procedures to implement their policies, reviews and internal controls to monitor and ensure the policies and procedures are observed, implemented properly and amended or updated, as appropriate, which include the following:

(a) designating the CO as responsible for overseeing the implementation and monitoring of the Entity's AML/CFT/CPF policies and procedures;

(b) ensuring the establishment of written policies and procedures with statements of policy, designated persons responsible for the policies and procedures and procedures designed to implement and monitor the Entity's policies;

(c) conducting an annual review of the Entity's AML/CFT/CPF policies and procedures to determine that they are adequate, effective current, meet regulatory requirements and are consistent with the Entity's business; and

(d) maintaining appropriate records of the annual review and changes to the policies and procedures set out in this Manual.

## 5. Compliance Committee

The Entity may also establish a compliance committee at such times as may be considered necessary or expedient with such function(s) as shall be determined by the directors acting with the advice of the CO.

## 6. Compliance Organisational Chart

6.1 A Compliance Organisational Chart is set out at Schedule 11.

## K. Customer Due Diligence Policy and Procedures

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. Customer due diligence policy

1.1 It is the policy of the Entity to:

(a) inquire into and identify the applicant for business, or the intended customer, and verify the identity;

(b) obtain information on the purpose and intended nature of the business relationship;

(c) use reliable evidence through such inquiry as is necessary to verify the identity of the applicant for business or intended customer;

(d) categorize such measures as are necessary to understand the circumstances and business of the applicant for business or the intended customer, including obtaining information on the source of wealth and funds, size and volume of the business, and expected nature and level of the transaction sought;

(e) conduct, where a business relationship exists, an on-going monitoring of that relationship and the transactions undertaken for purposes of making an assessment regarding consistency between the transactions undertaken by the customer and the circumstances and business of the customer; and

(f) inquire into and identify a person who purports to act on behalf of an applicant for business or a customer, which is a legal person or a partnership, trust or other legal arrangement, is so authorised and to verify the person's identity

(g) where required to do so, ensure that the source of funds is understood and documented;

(h) where required to do so, understand and document source of wealth (see paragraph 10 (Enhanced customer due diligence) below); and

(i) where identification or verification procedures (including EDD measures) cannot be concluded within a reasonable timeframe:

(i) not commence business relations or perform the transaction;

(ii) if the business relationship has been established, terminate the business relationship or refuse to complete the one-off transaction;

(iii) assess whether the circumstances surrounding the failure to identify or verify identity provide grounds for suspicion of ML, TF or PF; and

(iv) in such circumstances, the person concerned must consider making an internal SAR to the CO based on the information in their possession (remaining aware of the tipping off obligations).

1.2 Unless complete and satisfactory evidence of the identification and verification of identity is obtained within a reasonable period (considered to be thirty (30) days), the business relationship or transaction must not proceed.

1.3 These policies are to be read in conjunction with the AML/CFT Legislation.

### 2. Identification and Verification

(a) Identification and verification (**IDV**) shall be completed at the commencement of every business relationship.

(b) In addition, IDV must be completed:

(i) when effecting a one-off transaction (including a wire transfer) which involves funds of or above $1,500;

(ii) when there is a suspicion of money laundering or terrorist financing, irrespective of any exemption or threshold that may be referred to in this Manual including where an applicant for business or a customer is considered by an entity or a professional as posing a low risk;

(iii) where a business relationship or transaction presents any specific higher risk scenario; and

(iv) if there are doubts as to the veracity or adequacy of any previously obtained CDD information.

2.1 There may be instances when it might not be feasible to conduct and complete a verification process at the time of establishing a business relationship in order to ensure the smooth and normal conduct of business. In such a situation, it is permissible to complete the verification process following the establishment of the business relationship. This is permissible provided that:

(a) it is essential necessary in order not to disrupt the normal conduct of business;

(b) the verification is completed within a reasonable period not exceeding 30 days from the date of the establishment of the business relationship;

(c) prior to the establishment of the business relationship, the entity or professional adopts appropriate risk management processes and procedures, having regard to the context and circumstances in which the business relationship is being developed; and

(d) following the establishment of the business relationship, the money laundering or terrorist financing risks that may be associated with the business relationship are properly and effectively monitored and managed.

However, this is not best practice and the policy of the Entity is to undertake IDV at the commencement of a business relationship.

2.2 In addition:

(a) all business relationships which the Entity assesses to present a higher risk will undergo a review at least annually, where consideration must be given to the adequacy of the CDD being held in light of any changes that have occurred since last verified; and

(b) all business relationships which the Entity assesses to present normal or low risk will be reviewed at least once every four years to keep the CDD information up-to-date and periodically review/adjust the risk profile of any customers, where necessary.

## 3. Client Introductions

3.1 Certain clients may be introduced to the Entity by a third party. An "introduced" client is one where the third party introducer may withdraw from the relationship and it is the *introduced client* that becomes the direct client of the Entity. Where a third party introduces the client, the Entity shall satisfy itself that:

(a) The third party has a business relationship with the introduced client;

(b) The third party has taken measures to comply with the requirements of the MLPA or, if the third party resides outside Saint Lucia, their equivalent in the third party's jurisdiction; and

(c) The requirements of the MLPA or, if the third party resides outside Saint Lucia, their equivalent in the third party's jurisdiction, have been complied with;

3.2 Prior to establishing the business relationship with the introduced client, the Entity shall ensure that:

(a) the third party introducer has in place a system of monitoring any change in risk with respect to the introduced client and of reviewing and keeping up-to-date at least once every 4 years the relevant customer due diligence information on the introduced client where such client is assessed to present a low risk; or every year where such client is assessed to present a higher risk; and

(b) it enters into a written agreement with the third party in the terms set out in the MLPA.

## 4. Client Identification Documentation

4.1 The following IDV checklists (each, an **IDV Checklist**), sample forms of which are provided at the Schedule identified below, identify the appropriate information to be obtained for each applicant/customer. Based on the nature of the transactions and or risk posed by the client, the Entity will use some of the documents below as a basis for

identification. It should be noted that the lists below are not exhaustive and other 'equivalent' documents might be used where appropriate. It should not be expected that each of the documents listed below will be used to identify every single client.

| | **Sample IDV Checklist** | **Schedule** |
|---|---|---|
| (a) | IDV Checklist – Individual | Schedule 4 |
| (b) | IDV Checklist – Legal person (company/LLC) | Schedule 5 |
| (c) | IDV Checklist – Limited Partnership | Schedule 6 |
| (d) | IDV Checklist – Partnership | Schedule 7 |
| (e) | IDV Checklist – Trust/Unit Trust | Schedule 8 |

4.2 The IDV Checklists set out the minimum verification requirements for different types of applicants/customers[13] and their verifiable entities and also provide reminders regarding the standards of documentation required.

## 5. Who is a verifiable entity?

5.1 Where the Entity is dealing with an applicant/customer who is a natural person, it is the identity of that person which must be established and verified in accordance with Saint Lucian law, this Manual and the AML/CFT Legislation.

5.2 Where the Entity is dealing with an applicant/customer which is a corporate entity, a limited partnership, partnership, trust or unit trust, then the following must be established:

(a) the 'identity' of the corporate, partnership, limited partnership or trust; and

(b) the beneficial owner(s) of that entity.

*5.3* Beneficial owner is defined as *'the natural person who ultimately owns or controls an applicant for business or a customer or on whose behalf a transaction or activity is being conducted and includes but is not restricted to:*

*(a) in the case of a legal person other than a company whose securities are listed on a stock exchange, a natural person who ultimately owns or controls, whether through direct or indirect ownership or control, 10% or more of the shares or voting rights in the legal person;*

*(b) in the case of any legal person, a natural person who otherwise exercises ultimate effective control over the management of the legal person; or*

*(c) in the case of a legal arrangement:*

*(i) the partner or partners who control the partnership;*

*(ii) the trustee or other person who controls the applicant for business or customer; and*

(iii) *the settlor or other person by whom the legal arrangement is made*.'

## 6. Which IDV Checklist to use

6.1 If the applicant/customer is an individual, refer to or complete an IDV Checklist – Individual.

6.2 If the applicant/customer is a company or LLC, then:

(a) you must ensure that the information/documentation identified in the IDV Checklist – Legal person (company/LLC) is obtained in respect of the applicant/customer:

(b) you must ensure that the information/documentation identified in the IDV Checklist – Individual is obtained in respect of each of the directors/managers;

---

[13] The client's form(s) of DDQ should be reviewed against these requirements to ensure that all requisite information is being requested and verified.

(c) to the extent that any direct shareholder/member of the applicant/customer holds 10% or more of the shares/voting rights/ownership interests in the company or LLC and is:

(i) a company/LLC, obtain the information/documentation identified at paragraphs 1 to 5 (inclusive) of an IDV Checklist – Legal person (company/LLC) in respect of that company/LLC;

(ii) a limited partnership, obtain the information/documentation identified at paragraphs 1, 2, 4 and 5 of an IDV Checklist – Limited Partnership in respect of that limited partnership;

(iii) a partnership, obtain the information/documentation identified at paragraphs 1 to 5 (inclusive) of an IDV Checklist –Partnership in respect of that partnership; and/or

(iv) a trust/unit trust, obtain the information/documentation identified at paragraphs 1, 2, 3 and 4 of an IDV Checklist – Trust/Unit Trust in respect of that trust/unit trust;

(d) to the extent any individual directly or indirectly owns or otherwise controls 10% of more of the shares/voting rights/ownership interests in the company or LLC, you must obtain the information/documentation identified at paragraphs 1, 2, 3 and 4 of an IDV Checklist – Individual; and

(e) see paragraph 6.6 below.

6.3 If the applicant/customer is a limited partnership, then:

(a) you must ensure that the information/documentation identified in the IDV Checklist – Limited Partnership is obtained in respect of the applicant/customer:

(b) to the extent the general partner of the limited partnership is:

(i) a company/LLC, you must obtain the information/documentation identified at paragraphs 1 to 5 (inclusive) of an IDV Checklist – Legal person (company/LLC) in respect of that company/LLC;

(ii) a limited partnership, you must obtain the information/documentation identified at paragraphs 1, 2, 4 and 5 of an IDV Checklist – Limited Partnership in respect of that limited partnership;

(iii) an individual, you must obtain the information/documentation identified at paragraphs 1, 2, 3 and 4 of an IDV Checklist – Individual;

(c) to the extent any limited partner holds 10% or more of the ownership interests in the limited partnership and is:

(i) a company/LLC, you must obtain the information/documentation identified at paragraphs 1 to 5 (inclusive) of an IDV Checklist – Legal person (company/LLC) in respect of that company/LLC;

(ii) a limited partnership, you must obtain the information/documentation identified at paragraphs 1, 2, 4 and 5 of an IDV Checklist – Limited Partnership in respect of that limited partnership;

(iii) a partnership, you must obtain the information/documentation identified at paragraphs 1, 2, 4 and 5 of an IDV Checklist –Partnership in respect of that partnership; and/or

(iv) a trust/unit trust, you must obtain the information/documentation identified at paragraphs 1, 2, 3 and 4 of an IDV Checklist – Trust/Unit Trust in respect of that trust/unit trust;

(d) to the extent any individual directly or indirectly owns or otherwise controls 10% of more of the ownership interests in the limited partnership, you must obtain the information/documentation identified at paragraphs 1, 2, 3 and 4 of an IDV Checklist – Individual; and

(e) see paragraph 6.6 below.

6.4 If the applicant/customer is a partnership (but not a limited partnership), then:

(a) you must ensure that the information/documentation identified in the IDV Checklist – Partnership is obtained in respect of the applicant/customer:

(b) to the extent any partner[14] holds 10% or more of the ownership interests in the partnership and is:

(i) a company/LLC, you must obtain the information/documentation identified at paragraphs 1 to 5 (inclusive) of an IDV Checklist – Legal person (company/LLC) in respect of that company/LLC;

(ii) a limited partnership, you must obtain the information/documentation identified at paragraphs 1, 2, 4 and 5 of an IDV Checklist – Limited Partnership in respect of that limited partnership;

(iii) a partnership, you must obtain the information/documentation identified at paragraphs 1, 2, 4 and 5 of an IDV Checklist –Partnership in respect of that partnership; and/or

(iv) a trust/unit trust, you must obtain the information/documentation identified at paragraphs 1, 2, 3 and 4 of an IDV Checklist – Trust/Unit Trust in respect of that trust/unit trust;

(c) to the extent any individual directly or indirectly owns or otherwise controls 10% of more of the ownership interests in the partnership, you must obtain the information/documentation identified at paragraphs 1, 2, 3 and 4 of an IDV Checklist – Individual; and

(d) see paragraph 6.6 below.

6.5 If the applicant/customer is acting in its capacity of a trust or unit trust, then:

(a) you must ensure that the information/documentation identified in the IDV Checklist – Trust/Unit Trust is obtained in respect of the applicant/customer;

(b) to the extent any trustee, settlor, beneficiary[15], protector (if any), enforcer (if any), unit holder or any other natural person exercising effective ultimate control over the trust/unit trust (including through a chain of ownership) (as applicable) of the trust is:

(i) a company/LLC, you must obtain the information/documentation identified at paragraphs 1 to 5 (inclusive) of an IDV Checklist – Legal person (company/LLC) in respect of that company/LLC;

(ii) a limited partnership, you must obtain the information/documentation identified at paragraphs 1, 2, 4 and 5 of an IDV Checklist – Limited Partnership in respect of that limited partnership;

(iii) a partnership, you must obtain the information/documentation identified at paragraphs 1, 2, 4 and 5 of an IDV Checklist –Partnership in respect of that partnership; and/or

(iv) the trustee of another trust/unit trust, you must obtain the information/documentation identified at paragraphs 1, 2, 3 and 4 of an IDV Checklist – Trust/Unit Trust in respect of that other trust/unit trust; and/or

(v) an individual, you must obtain the information/documentation identified at paragraphs 1, 2, 3 and 4 of an IDV Checklist – Individual; and

(c) see paragraph 6.6 below.

---

[14] Identification evidence must be obtained for at least two partners (paragraph II.4.B.43).

[15] This is only required if the trust is a nominee relationship so that the beneficiaries have substantive control over the trust assets.

6.6 If any individual exercises control of an applicant/customer through other means[16], or acts or provides instructions on behalf of an applicant/customer, you must:

(a) obtain the information/documentation identified in the IDV Checklist – Individual in respect of that person, to the extent not already completed in accordance with the above; and

(b) (where applicable) verify that the person acting on the applicant/customer's behalf is properly authorised to do so.

Examples of an individual giving instructions on behalf of an applicant/customer include:

(i) a director/manager of a customer company/LLC;

(ii) a director/manager of a company/LLC which is the general partner of a customer limited partnership;

(iii) authorised signatories;

(iv) a shareholder/member of a customer company/LLC;

(v) a partner of a customer partnership; and

(vi) an attorney appointed under a power of attorney by the applicant/customer and authorised to give instructions.

1.1 If the applicant/customer is a non-profit organisations (including charities), then there may be a potential risk of money laundering, as there are some difficulties in verifying the source of funds (in some cases there may have been anonymous donations). It has been that there is a clear distinction between the risks involved with local not for profits and those that make distributions overseas. You must:-

(a) treat the identification process on not for profit organisations as they would for any other corporate entity or trust;

(b) obtain an explanation of the proposed purpose and operation of the organization;

(c) obtain the identification documents on at least two of the signatories of the organization;

(d) where the organization is registered in an overseas jurisdiction, it is prudent to contact the appropriate charity commission or equivalent body to confirm registration of the charity; and

(e) undertake a basic vetting of foreign organisations in relation to known money laundering and terrorist activities.
(i)

---

16 **Through other means** may, for example, mean through partnership agreements, power to appoint senior management, where any outstanding debt is convertible into voting rights, through personal connections, by participation in financing, because of close of intimate family relationships, historical or contractual associations or as a result of default on certain payments.

## 2. Certification of CDD documentation

2.1 Where the Entity, in the establishment of a business relationship or conduct of a one-off transaction with an applicant for business or a customer, relies on a copy of a document presented by the applicant or customer which the Entity, having regard to appropriate risk assessment, considers may not be authentic or may be doubtful or generally has concern with, the Entity must ensure that the copy of the document is properly certified.

2.2 When used in the context of CDD documentation and, in particular, the IDV Checklists, a **certified document** means a document which:

(a) is certified by a person who is competent and has authority to certify the document (see paragraphs 2.3 and 2.4 below for more details); and

(b) bears (i) the name and address of the person certifying the document; (ii) the date of the certification; and (iii) the signature or seal of the person certifying the document.

2.3 The onus is on the Entity to determine whether the person making a certification is competent and has the authority to provide reliable certification. A person that is acting in a professional capacity and is subject to some rules of professional conduct promulgated and enforced by the professional body to which he or she belongs, is most likely to provide reliable certification. This is also the case for a person operating within a statutory system in his or her jurisdiction that provides for specific compliance measures and the application of penalties for breaches of those measures.

2.4 Examples of persons that are competent and have the authority to certify reliable documents are as follows:–

(a) a judicial officer or a senior public officer, including a senior police officer, customs officer or immigration officer with responsibility within his or her for issuing certified documents (for example, a registrar responsible for deeds, land matters, etc.);

(b) an officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity;

(c) a legal practitioner or medical practitioner, or an accountant, actuary or other professional who belongs to a professional body with established rules of professional conduct;

(d) a notary public who is governed by established rules of professional conduct or statutory compliance measures;

(e) a director, manager or senior officer of a licensed entity, or of a branch or subsidiary of a group headquartered in a well-regulated jurisdiction that applies group standards to subsidiaries and branches worldwide and tests the application of and compliance with such standards.

2.5 To the extent that any document is not in English, that document may need to be translated into English. Please discuss exactly what will be required (eg certified translation) with the CO.

## 3. CDD procedures

3.1 The following procedures must be adhered to in respect of each applicant or customer:

(a) Distribute a DDQ to the applicant/customer. Standard CDD information is requested via the DDQ.

(b) Obtain email or hard copy DDQ (and accompanying information/documentation) containing the relevant information required to commence CDD.

(c) Determine the verifiable entities in relation to the customer/applicant (see paragraph 5 (Who is a verifiable entity?) above).

(d) Conduct screening checks and searches on each verifiable entity.

(e) Risk assess each applicant or customer, using the form set out at Schedule 3 (Form of Customer Risk Assessment) as a guide.

(f) Review all information/documentation provided and check against/complete an IDV Checklist for each verifiable entity.

(g) File the customer risk assessment and all relevant information, which may include the IDV checklist(s), DDQ and all accompanying documentation electronically.

(h) If any deficiencies are noted in the CDD process, notify the CO and/or, where deficiencies provide grounds for suspicion of ML or TF, the CO as a matter of priority.

3.2 The CDD status of an applicant or customer will be found in the records maintained by the CO.

## 4. Low Risk Customers or Transactions

4.1 The AML/CFT Legislation allows the Entity to conduct simplified or reduced customer due diligence (**SDD**) procedures where the Entity makes a determination that a customer poses low risk. Any SDD measures adopted must be in accordance with this Manual and the AML/CFT Legislation and proportionate to the risks involved in any particular relationship or transaction.

4.2 It is the policy of the Entity to conduct SDD only:

(a) in the circumstances, and in accordance with the procedures, identified below; and

(b) with the concurrence of the CO, which shall be documented in the applicable customer risk assessment form.

4.3 Adopting the risk-based approach, the Entity may determine customers or transactions that it considers carry low risk in terms of the business relationship, and to make such a determination the Entity may take into account such factors as:

(a) a source of fixed income (such as salary, superannuation and pension);

(b) in the case of a financial institution, the institution is subject to anti-money laundering and terrorist financing requirements that are consistent with the FATF Recommendations and are supervised for compliance with such requirements;

(c) publicly listed companies that are subject to regulatory disclosure requirements;

(d) Government statutory bodies;

(e) beneficial owners of pooled accounts held by non-financial businesses and professions if they are subject to anti-money laundering and terrorist financing requirements and are subject to effective systems for monitoring and compliance with the anti-money laundering and terrorist financing requirements;

(f) in the case of a body corporate that is part of a group, the body corporate is subject to and properly and adequately supervised for compliance with anti-money laundering and terrorist financing requirements that are consistent with the FATF Recommendations; and

(g) the entity considers, in all the circumstances of the customer, having regard to the Entity's anti-money laundering and terrorist financing obligations, to constitute little or no risk.

4.4 Where the Entity makes a determination that a customer poses low risk, the entity may carry out SDD in accordance with this Manual and the AML/CFT Legislation.

4.5 Where SDD is applied in accordance with the foregoing paragraphs:

(a) the rationale behind the decision should be documented in writing on the relevant customer risk assessment form;

(b) the customer risk assessment form must be counter-signed by the CO; and

(c) evidence supporting the decision should be documented and retained in the relevant CDD record. By way of example, such evidence may include:

(i) a print out of the relevant stock exchange to evidence a listing;

(ii) online searches on a listed or regulated entity; and

(iii) online searches or other identity checks on all verifiable entities in relation to that applicant/customer.

## 5. Enhanced customer due diligence

5.1 The Entity shall consider the applicant for business or customer to present a higher risk in respect of whom EDD shall be performed where the business relationship or transaction involves:

(a) a politically exposed person;

(b) a business activity, ownership structure, anticipated, or volume or type of transaction that is complex or unusual, having regard to the risk profile of the applicant for business or customer, or where the business activity involves an unusual pattern of transaction or does not demonstrate any apparent or visible economic or lawful purpose; or

(c) a person who is located in a country that is either considered or identified as a high risk country or that has international sanctions, embargos or other restrictions imposed on it,

(d) where any person conducting CDD measures is dissatisfied as to the veracity or accuracy of any evidence of identity provided;

(e) where an applicant/customer or transaction is identified as presenting a higher risk of ML or TF;

(f) in the event of any unusual or suspicious activity being identified.

5.2 Where EDD measures are to be applied, the relevant person must make further enquiry or investigation, and/or take such further steps as considered appropriate to ensure that there is no suspicion of ML or TF (eg, by obtaining and verifying further details on the transactions to be undertaken and their underlying purposes and the parties involved).

5.3 EDD measures must be in addition to the measures to be taken in circumstances presenting a lower or medium risk, and must address the particular risk(s) presented.

5.4 EDD measures may include but not be limited to:

(a) obtaining further CDD information (identification information and relationship information, including further information on the directors/controllers of the entity, source of funds and source of wealth), from either the applicant/customer or independent sources (such as the internet, public and commercially available databases);

(b) taking additional steps to verify the CDD information obtained;

(c) commissioning due diligence reports from independent experts to confirm the veracity of CDD information held;

(d) requiring higher levels of management approval for higher risk business relationships or transactions;

(e) requiring more frequent review of business relationships;

(f) requiring the review of business relationships to be undertaken by the CO, or other person not directly involved in managing the business relationship; and

(g) setting lower monitoring thresholds for transactions connected with the business relationship.

5.5 For further guidance concerning EDD measures, contact the CO.

## 6. Breaches in Compliance

If due diligence cannot be performed adequately, the Entity should consider not opening the account, suspending the transaction activity, filing a report with the CO or closing the account.

## K. Politically Exposed Persons (PEPs) Policy and Procedures

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. AMLR requirements

1.1 The MLPA require the Entity, to:

(a) have, as part of its or his internal control systems, appropriate risk-based policies, processes and procedures for determining whether an applicant for business or a customer is a politically exposed person;

(b) in dealings with a politically exposed person, take such reasonable measures as are necessary to establish the source of funds or wealth respecting such person

(c) ensure that senior management approval is sought for establishing or maintaining a business relationship with a politically exposed person;

(d) ensure a process of regular monitoring of the business relationship with a politically exposed person;

(e) in circumstances where junior staff deal with politically exposed persons, ensure that there is in place adequate supervisory oversight in that regard; and

(f) ensure that the requirements of paragraphs (a) to (d) apply in relation to a customer who becomes a politically exposed person during the course of an existing business relationship.

1.2 Pursuant to the AML/CTF Legislation, a politically exposed person means an individual who is or has been entrusted with prominent public functions and members of his immediate family, or persons who are known to be close associates of such individuals. The AML/CTF Legislation provides that politically exposed persons and generally comprise persons who are Heads of State/government, cabinet ministers/secretaries of state, judges (including magistrates where they exercise enormous jurisdiction), senior political party functionaries and lower political party functionaries with an influencing connection in high ranking government circles, military leaders and heads of police and national security services, senior public officials and heads of public utilities/corporations, members of ruling royal families, senior representatives of religious organizations where their functions are connected with political, judicial, security or administrative responsibilities.

1.3 The Entity should also act in accordance with the Financial Action Task Force (the **FATF**) recommendation on dealings with PEP's. The FATF recommends that a higher degree of vigilance be applied when a regulated entity such as the Entity is dealing with a PEP.

### 2. PEPs policy

2.1 For the purposes of this Manual, a reference to a **politically exposed person** or **PEP** shall mean a person who is a politically exposed person, or members of his immediate family, or persons who are known to be close associates of such individuals.

For the purposes of determining whether a person is a close associate of an individual entrusted with a prominent public function, a relevant person need only consider information that it holds or is publicly known.

2.2 Prior to the establishment of a business relationship with a PEP, or entry into a transaction or business relationship where there is a connection to a PEP, the identity, background to the proposed business relationship, source of funds and wealth must be established.

2.3 All PEP relationships must be approved by the Entity's Management and monitored appropriately.

2.4 PEP status automatically puts a customer, business relationship or transaction into a higher risk category.

2.5 PEP status automatically requires that EDD measures be applied using a risk based approach.

2.6 Unless satisfactory evidence of these requirements is obtained, the business relationship must not proceed.

2.7 A register of PEPs must be maintained.

2.8 This policy is to be read in conjunction with the AML/CTF Legislation.

## 3. Purpose of the PEPs policy

This policy has been adopted to:

3.1 identify and verify the identity of PEPs;

3.2 ensure that funds managed by the Entity on behalf of PEPs are not the proceeds of criminal activity for bribery, corruption and financial irregularity;

3.3 ensure greater care is exercised when considering establishing a PEP relationship with those countries known for bribery, corruption and financial irregularity;

3.4 mitigate risk and protect the Entity being used for the purpose of ML, TF or corruption; and

3.5 ensure compliance with the requirements of Saint Lucia legal system regarding the provision of financial services as they relate to PEPs and anti-corruption.

## 4. PEPs procedures

4.1 These procedures must be followed if a PEP is identified at any point during a business relationship.

4.2 The identification of a PEP may occur at any time during a relationship, including but not limited to the following:

(a) during the verification of identity of a customer and all connected entities; and

(b) as a result of new information being obtained on existing relationships.

4.3 PEP status itself does not, of course, incriminate individuals or entities. It will mean, however, that the customer will be subject to EDD measures.

4.4 Upon identification of a PEP:

(a) a higher risk rating must be applied to that customer, transaction or business relationship;

(b) the CO must be informed and provided with all relevant information and supporting materials on request;

(c) the source of funds and source of wealth of the PEP should be established;

(d) the nature of EDD measures applied will be commensurate with the risk that is identified and nature of the PEP connection;

(e) additional online searches as determined by the CO will be undertaken using AML-specific tools, such as World Check or Accuity Online;

(f) a general internet search must also be undertaken to enhance the CDD information, corroborate source of wealth and funds and to uncover any other information available in the public domain; and

(g) approval to enter into or to continue the business relationship with the PEP is required from the Entity's Management.

4.5 In determining whether a customer is a PEP and the risk they may pose, the Entity will:

(a) assess those countries and territories with which the customer is connected and consider:

(i) which pose the highest risk of corruption and other criminal activities such as abduction and kidnapping for ransom;

(ii) whether the country of origin of the customer is cash based;

(iii) whether the country of origin of the customer has in place adequate AML/CTF measures, including "know your customer" (KYC)

requirements; and

(iv) whether the country of origin is under any established sanction, embargo or other restriction or whether any such sanction, embargo or restriction is specifically imposed on the customer (entities and professionals are encouraged to conduct regular checks of Saint Lucia Gazette to note any new lists on the UN and EU sanctions and embargo regimes, including modifications thereto);

(b) consider who are the current and former holders of prominent public functions within those higher risk countries and territories and determine, as far as is reasonably practicable, whether or not the customer has any connections with such individuals (including through immediate family or close associates); and

(c) exercise vigilance where customers are involved in business sectors that are vulnerable to corruption such as, but not limited to, oil or arms sales.

(d) conduct enhanced monitoring of the relationship.

4.6 The degree of scrutiny that the Entity will apply will depend on various risk factors, including, but not limited to:-

(a) proof that the clients source of funds or wealth do not emanate from criminal activity;

(b) whether the home jurisdiction of the PEP is one in which current or former political figures have been implicated in corruption; and

(c) the length of time that a former political figure has been in office.

4.7 In a case where a PEP is a director (or equivalent) of a customer, or person acting, or purporting to act for a customer, and where no property of that PEP is handled in the particular business relationship or one-off transaction, the Entity may demonstrate that it applies specific and adequate measures under where it considers the nature of the PEP's role and reason why the PEP has such a role.

4.8 Similarly, where a PEP is a trustee or a general partner that is a customer, or is a beneficiary or object of a power of a trust, and where no property of that PEP is handled in the particular business relationship or one-off transaction, the Entity may demonstrate that it applies specific and adequate measures where it considers the nature of the PEP's connection and reason why the PEP has such a connection.

4.9 This does not discharge the Entity from its other AML obligations where there is a PEP involvement:

(a) requiring any new business relationship or continuation of such a relationship or any new one-off transaction to be approved by the Board of the Entity; and

(b) undertaking measures to establish the source of the wealth of the PEP and source of the funds involved in the business relationship or one-off transaction

4.10 If any adverse information is identified in respect of a PEP, the following action must be taken:

(a) obtain all necessary information where relevant (including, without limitation, where the PEP is the customer, beneficial owner or controller of the customer) and provide details of source of wealth/funds;

(b) forward the relevant information/documents to the CO and to Management for review and, if considered appropriate, sign off; and

(c) flag the entity and related entities in the Entity's internal books and records as a PEP, as appropriate.

4.11 The approval process detailed above also applies to existing customers who are identified as a PEP during the course of their business relationship with the Entity.

**5. PEP register**

5.1 On receipt of information and documentation relating to a PEP or a customer or business transaction with a PEP connection which has been risk assessed and signed off by the Entity's Management, full details must be included within the PEP register by the CO.

5.2 The PEP register is maintained by the CO and all relationships are monitored/reviewed

and assessed in accordance with their risk categorization to ensure that the CO is satisfied that each relationship remains satisfactory.

5.3 The PEP register will be presented to Management on a periodic basis.

## 6. Meetings/communications with PEPs

Any proposed physical meetings with PEPs, particularly in higher risk jurisdictions, must be communicated with the CO and to Management prior to the meeting.

## 7. Ongoing monitoring

The CO is responsible for the review of ongoing monitoring of any relationship with a PEP.

## 8. PEP relationship termination or reassessment

8.1 The decision to terminate a relationship with a PEP due to a concern or suspicion being raised must be referred to the Entity's Management and the CO.

8.2 Where there is a suspicion of ML or TF, the CO must be notified and an internal SAR made immediately and no further action taken (see Part N (Suspicious Activity Reporting (SAR) Policy) of this Manual below).

8.3 Where a PEP is considered no longer to be in a politically exposed role, the CO will determine an appropriate period for them to remain on the PEP register.

## 9. Reputational damage

9.1 There is a significant risk involved with institutions providing financial services to persons such as government ministers and their officials where they are from countries with known problems of bribery, corruption and financial irregularity. There have been a number of high profile cases where persons in power have illegally benefited from their senior positions by 'stealing' their country's money or accepting bribes often described as commission or consultancy. The funds illegally acquired are often transferred into companies, trusts and other structures designed to hide the connection with the individual(s) concerned.

9.2 Persons or entities who have a relationship with individuals involving the proceeds of corruption, risk severe reputational damage as well as the possibility of criminal sanction, should they have assisted in laundering the proceeds of crime.

## 10. Source of wealth and source of funds

10.1 Source of wealth is gaining an understanding of how the PEP has accumulated their overall wealth, to gain comfort that it has been obtained by legitimate means, whether or not those funds are used in the business relationship or one-off transaction.

10.2 Source of funds is gaining an understanding of the activity which has accumulated the specific funds for the transaction being undertaken, provided to the Entity by the PEP.

## L. Record Retention Policies and Procedures

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. Retention Periods of Record

1.1 The Entity shall retain the following records for a period of 7 years following the closing of the account, or termination of the business relationship.

(a) the records required by the MLPA for purposes of establishing customer due diligence, compliance auditing, law enforcement, facilitating the strengthening of the Entity's systems of internal control and facilitating responses to requests for information pursuant to the provisions of the regulations, or any other enactment or for regulatory or investigative purposes;

(b) the policies and procedures of the Entity regarding relevant internal control measures;

(c) the internal suspicious activity reports made and the supporting documentation;

(d) the decisions of the CO in relation to suspicious activity reports and the basis for the decisions;

(e) the activities relating to complex or unusual large or unusual patterns of transactions undertaken or transactions which do not demonstrate any apparent economic or visible lawful purpose or, in relation to a customer, are unusual having regard to the customer's pattern of previous business or known sources of business;

(f) the activities of customers and transactions that are connected with jurisdictions which do not or insufficiently apply the FATF Recommendations;

(g) the activities of customers and transactions which relate to jurisdictions on which sanctions, embargos or other restrictions are imposed; and

(h) the account files and business correspondence with respect to transactions.

1.2 These records are stored at the principal office of the Entity and will be made available to governmental regulatory agencies upon request.

### 2. CDD records

2.1 To comply with its AML/CFT obligations, the Entity shall establish and retain the following records in relation to identification data obtained through the CDD process in relation to each customer:

(a) information regarding the source from which the evidence can be obtained; or

(b) information that is sufficient to enable the details of identity to be obtained, in circumstances where it is not reasonably practicable to obtain or retain a copy of the evidence.

2.2 The Entity shall ensure that the manner in which customer due diligence and, where applicable, enhanced customer due diligence information is recorded and kept facilitates the unhindered monitoring of its or his business relationships and transactions.

### 3. Transaction records

The Entity shall establish and retain records in relation to each business relationship entered into by the Entity, which shall incorporate the following details as a minimum:

(a) the name and address of the customer;

(b) in the case of a monetary transaction, the kind of currency and amount involved;

(c) the beneficiary of the monetary transaction or product, including his or her name and address;

(d) where the transaction involves a customer's account, the number, name or other identifier with respect to the account;

(e) the date of the transaction;

(f) the nature of the transaction and, where the transaction involves securities and investment, the form in which funds are offered and paid out;

(g) in the case of a transaction involving an electronic transfer of funds, sufficient detail to enable the establishment of the identity of the customer remitting the funds and compliance with paragraph (c);

(h) account files and business correspondence with respect to a transaction; and

(i) sufficient details of the transaction for it to be properly understood.

## M. Suspicious Activity Reporting (SAR) Policy

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. Suspicious Activity Reporting

1.1 All employees of the Entity are required to be familiar with the anti-money laundering procedures. In the event that an employee receives any enquiry from a law enforcement agency, that inquiry shall immediately be referred to the CO.

### 2. SAR policy

2.1 The Entity and all directors, officers, partners or employees (as applicable) shall report (to the CO or, if the CO is unavailable, any deputy CO), as soon as practicable where they have any knowledge, suspicion or reasonable grounds to know or suspect that another person is engaged in money laundering.

2.2 AML Legislation creates the offence of failing to make a disclosure to the FIA as soon as reasonably practicable after it comes to the relevant person's attention where:

(a) a person knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and

(b) the information or other matter on which the knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, came to that person's attention in the course of that person's trade, profession, business or employment.

2.3 There are criminal offences for a **failure to report** where there is knowledge, suspicion or reasonable grounds to know or suspect.

2.4 This policy is to be read in conjunction with the AML/CTF Legislation.

### 3. Purpose of the SAR policy

3.1 This policy has been adopted to:

(a) ensure that the Entity and all other relevant persons understand and comply with their statutory and regulatory obligations;

(b) assist the supervisory and competent authorities in the detection and prevention of ML, TF or any criminal conduct investigations;

(c) provide, as requested, evidential documentation to assist in AML, CFT or any criminal conduct investigations;

(d) protect the reputation of the Entity, its customers and Saint Lucia; and

(e) mitigate risk and protect the Entity being used for the purposes of ML, TF and financial crime.

3.2 This policy will also protect against:

(a) regulatory sanction against the Entity and principal persons;

(b) criminal sanctions against the Entity and its directors, officers, partners or employees (as applicable);

(c) financial sanctions against the Entity and its directors, officers, partners or employees (as applicable); and

(d) disciplinary action against any employee of the Entity who fails, without reasonable excuse, to make an internal SAR where he/she has knowledge, suspicion or reasonable grounds for knowledge or suspicion, or does not do so as soon as is reasonably practicable.

### 4. Guidance on SARs

*4.1 What constitutes knowledge or suspicion?*

(a) What may constitute reasonable grounds for knowledge or suspicion will be determined from the facts and circumstances of each case. Generally speaking,

knowledge is likely to include:

(i) actual knowledge;

(ii) deliberately refraining from making inquiries or asking questions, on the basis that one does not want to know the results of the inquiries or the answers to the questions;

(iii) deliberately deterring another person from making disclosures, the content of which one might not care to have;

(iv) knowledge of circumstances which would indicate the facts to an honest and reasonable person; and

(v) knowledge of circumstances which would put an honest and reasonable person on inquiry and failure to make the reasonable inquiries which such a person would have made.

(b) For a person to have knowledge, or be suspicious, they do not need to know the exact nature of the criminal activity underlying the money laundering, or that the funds themselves were definitely those arising from the criminal offence.

(c) In contrast, suspicion is more than speculation but it falls short of proof or knowledge. Suspicion is personal and subjective but will generally be built on some objective foundation.

*4.2 Examples of suspicious activities or transactions*

(a) There is no standard definition of what constitutes a suspicious activity or transaction. However examples are available at the FATF ML typologies webpage (www.fatf-gafi.org).

(b) It is important to differentiate between the terms "unusual" and "suspicious" and note that activities (or attempted activities or transactions) may be recognizable as falling into one or more of the following categories (which is not an exhaustive list):

(i) any unusual financial activity of the customer in the context of the customer's own usual activities;

(ii) any unusual transaction in the course of some usual financial activity;

(iii) any unusually linked transactions;

(iv) any unusual engagement of an intermediary in the course of a usual transaction or financial activity;

(v) an unusual method of settlement;

(vi) any unusual or disadvantageous early redemption of an investment product; and

(vii) any unwillingness to provide information requested.

(c) The following factors should be considered when seeking to identify a suspicious transaction (this is not an exhaustive list):

(i) Is the customer known personally?

(ii) What are the customer's economic/financial status, employment history, behaviour and general background?

(iii) Does the transaction or activity make sense for that particular customer?

(iv) Is the transaction in keeping with normal practice in the market to which it relates (ie with reference to the market, size and frequency)?

(v) Is the transaction to be settled in the normal manner?

(vi) Is the role of any agent involved in the transaction unusual?

(vii) Are the reasons for the transaction or activity or transaction transparent and understandable ie. Is there a cheaper, easier, or more convenient method available?

(viii) Are the client's instructions structured in a way that the economic or

lawful purpose of the instruction is not apparent or is absent entirely?

(ix) When asked to explain the circumstances or the transaction is the client or customer evasive or do they give explanations which do not stand up to reasonable scrutiny?

*4.3 The Objective Test of Knowledge or Suspicion*

An offence is committed where there are reasonable grounds to know or suspect that another person is engaged in money laundering. That is, a person would commit an offence even if he/she did not know or suspect that another person is engaged in money laundering, if he/she had reasonable grounds for knowing or suspecting that they words. In other words, if another 'reasonable' person in the same position would have been suspicious and made a report, a person who does not make a report may have committed an offence.

**5. Tipping off**

5.1 The offence of tipping off a target or third party about a suspicion, investigation or proposed investigation into ML, which is likely to prejudice such an investigation.

5.2 The effect of this is that no director, officer, partner or employee (as applicable) of the Entity may:

(a) at the time, tell a customer that a transaction or activity is being delayed because an internal SAR is about to be made or has been made to the CO;

(b) at the time, tell a customer that a transaction or activity is being delayed because an external SAR is about to be made to or is awaiting consent from the FIA;

(c) later tell a customer that a transaction or activity was delayed because an internal or external SAR had been made; or

(d) tell a customer that law enforcement is conducting an investigation.

5.3 For the avoidance of doubt and to avoid any tipping off offence being committed, the only disclosure which should be made by any director, officer or employee (as applicable) of the Entity should be to the CO.

## N. Reporting and Procedures

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. Compliance Officer

1.1 The Entity is required to appoint persons at managerial level to act as the CO.

1.2 The name and contact details of the CO designated by the Entity are set out below:

*Compliance Officer*

Limbani Vishal Vallabhbhai

Telephone: +1 519 330 4688

Email:

Limbanivishal1991@gmail.com

### 2. Suspicious activity reporting procedures (AML/CFT)

*2.1 Internal reporting procedures*

(a) The Entity and all directors, officers or employees (as applicable) shall report (to the CO or, if the CO is unavailable, any deputy CO), as soon as practicable where they have any knowledge, suspicion or reasonable grounds to know or suspect that another person is engaged in money laundering by way of an file an internal suspicious activity report (**SAR**).

(b) A form of internal SAR form is provided at Schedule 9 and is also available from the CO. The internal SAR form should be completed electronically and emailed to the CO.

(c) The CO must be advised where an internal SAR relates to an urgent transaction.

(d) Reporting requirements extend to business relationships and one-off transactions that are declined (ie, where no business relationship is established or transaction carried out).

(e) Each person who holds the knowledge, suspicion or reasonable grounds for knowing or suspecting that a person is engaged in money laundering must make their own internal SAR. However, where exactly the same reason for suspicion is held by another person dealing with the same customer, party or transaction, they can be added on the internal SAR form as a joint reportee and may rely on the one report made.

(f) It is not sufficient to rely on an internal SAR which is known to have been raised by another individual.

(g) An internal SAR made in respect of a customer, business relationship or one-off transaction does not remove the need to make further reports in respect of any knowledge or suspicion that subsequently arises in respect of that customer, relationship or one-off transaction (or a series of linked transactions). The reportee must keep the CO abreast of any pertinent developments in relation to the customer, relationship or transaction which is the subject of a SAR, including any adverse or relevant media attention. Relevant copy correspondence must be forwarded to the CO as necessary.

(h) An internal SAR should not be discussed with anyone apart from the CO or a person designated by the CO. The internal SAR (or a copy thereof) should not be disclosed in any circumstances, other than those disclosures which have been sanctioned by the CO and are in accordance with Saint Lucian legislation.

(i) Where an internal SAR is made to the CO:

(i) the CO shall, as soon as possible, provide the reportee with an acknowledgement receipt by email, which shall include a reminder of the reportee's obligation not to disclose details of the internal SAR or a copy of the internal SAR;

(ii) all correspondence and documentation relating to the internal SAR must be retained separately from any other customer, correspondence or transaction files or records;

(iii) the CO shall have access to, and shall review, all relevant information, records and files as may be required, in the CO's opinion, to consider whether the knowledge or suspicion identified in the internal SAR requires a disclosure to be made to the FIA in accordance with the MLPA;

(iv) the CO shall determine whether or not the information contained in the internal SAR does give rise to knowledge or suspicion of ML or TF activities requiring a disclosure to be made to the FIA in accordance with the MLPA; and

(v) the CO shall record details of that internal SAR and the CO's decision making process as required by these procedures, the MLPA and the Entity's records retention policy.

(j) It is a criminal offence not to file an internal SAR with the CO where there is knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that a person might be concerned in an illegal money laundering, terrorist financing activity or any criminal conduct, or requesting services to assist them. Reporting, in good faith, as soon as is reasonably practicable, and in accordance with these internal SAR procedures, is a defence.

(k) Guidance will be provided by the CO if any person is unsure how to deal with a customer, relationship or transaction which is under investigation.

*2.2 Making an external SAR to the FIA*

(a) If the CO determines that the information provided in relation to an internal SAR substantiates a suspicion of ML or TF, they must promptly make a disclosure to the FIA in the form prescribed by the FIA.

(b) If the CO considers that a SAR report should be made to the FIA urgently, initial notification to the FIA should be delivered in accordance with the procedure prescribed by the FIA.

(c) When an acknowledgement is received from the FIA, the CO shall:

(i) provide the reportee(s) with a copy of any acknowledgement by email;

(ii) provide guidance in respect of any instructions given by the FIA;

(iii) carry out any requested actions or take legal advice, if required;

(iv) record the SAR in the SAR register (including the date of the report and supporting documentation); and

(v) retain copy correspondence in accordance with the Entity's records retention policy.

*2.3 Ongoing responsibilities*

(a) Having made an internal SAR, the reportee is still obliged to report any further concerns they have, as well as any pertinent developments in relation to the subject of the SAR.

(b) The CO must:

(i) inform the FIA where relevant information relating to an external SAR is subsequently discovered;

(ii) provide guidance where a reportee is unsure how to deal with a customer under investigation; and

(iii) keep SARs (whether internal or external) securely in accordance with the provisions of the MLPA.

(c) The CO must also consider on a periodic basis:

(i) the period of time between information on a matter coming to the attention of the original reporter and the date on which the internal SAR is made to ensure that this is reasonable; and

(ii) the number and content of internal SARs to ensure that these are consistent with the Entity's risk assessments.

**3. SAR register**

3.1 The SAR register must contain the following details in relation to each SAR made to the FIA:

(a) the date of the report;

(b) the person who made the report;

(c) the person(s) to whom the report was forwarded; and

(d) a reference by which supporting evidence is identifiable.

3.2 The SAR register shall be maintained by the CO.

## 4. Tipping off

4.1 Section 31 of the PCA creates the offence of tipping off a target or third party about a suspicion, investigation or proposed investigation into ML, which is likely to prejudice such an investigation.

4.2 The PCA does provide defences to tipping off. However, for the avoidance of doubt and to avoid any tipping off offence being committed, the only disclosure which should be made by any director, officer or employee (as applicable) of the Entity should be to the CO.

4.3 The CO will work with the reportee on a suitable response to the customer. The FIA may provide guidance on what, if any, information can be provided to the customer.

4.4 A customer, business relationship or transaction which is the subject of a SAR should not be terminated without speaking to the CO, who will contact the FIA for guidance.

## O. Anti-money Laundering Training Policies

| | | | |
|---|---|---|---|
| Date approved: | January 2024 | Original issue date: | January 2024 |
| Last revised date: | January 2024 | Next review date: | As determined by the CO |

### 1. Training Policy

1.1 The Entity does not currently have any employees. However, if the Entity employs any employees in the future:

(a) it will provide each employee with a copy of this Manual;

(b) the CO shall implement a programme to train employees in connection with:

(i) anti-money laundering policies and procedures;

(ii) current Saint Lucia anti-money laundering regulation; and

(iii) rules and guidelines with respect to money laundering. Anti-money laundering training will be conducted on at least an annual basis.

1.2 The MRLO should pay particular attention to the following:-

(a) the necessity to be pro-active in training employees to recognize money laundering activities;

(b) the severity of the regulatory exposure due to lack of such a pro-active stance;

(c) the suspicious activity indicators to look for and the procedures in place regarding the vigilance required when establishing a new relationship; and

(d) any other anti-money laundering issues that the CO believes would be educational.

1.3 The Entity has circulated all of the aforementioned policies as part of its anti-money laundering efforts and the policies and procedures are designed to enable the Entity to satisfy the anti-money laundering regulations currently in force in Saint Lucia.

**Schedule 1 – Form of Risk Assessment Questionnaire[17]**

| Our customer types and locations | Rarely | Some times | Often |
|---|---|---|---|
| Do we act for customers whom we do not meet, or otherwise whom we do not know well? | | | |
| Do we act for entities with a complex or obscure ownership structure? | | | |
| Do we act for entities that have nominee shareholders or shares in bearer form? | | | |
| Do we work for customers who are believed to have criminal associations or low standards of honesty? | | | |
| Do we act for politically exposed persons? | | | |
| Do we act for customers who have connections with countries which are high risk for money laundering? | | | |
| Do we act for customers who have connections with countries or geographic areas which are identified by credible sources as providing support or funding for terrorist activities, or that have designated terrorist organisations operating within their borders? | | | |
| Do we act for customers who may have terrorist sympathies? | | | |
| Do we act for customers who have connections with countries which are high risk for corruption or other criminal activity? | | | |
| Do we act for customers who are, or who have connections with countries which are, subject to embargoes, sanctions or similar measures issued by the United Nations, the European Union or the United States? | | | |
| Do we carry-out transactions for customers in high-risk industries[18]? | | | |
| Do we act for customers who for some other reason present a substantial money laundering risk? | | | |

[17] The questions posed in this questionnaire are examples only and should be tailored to the business activities of the Entity.

[18] High-risk industries include those involving the manufacture, supply or transportation of arms, weapons or other military or defence equipment, involvement (directly or indirectly) in mining, drilling or quarrying for natural resources, dealing in precious metals or gems, pornography or other adult entertainment, involvement (directly or indirectly) with religious or political organisations, customers handling funds raised directly from the public (eg, crowd funding or charities) that are not subject to oversight by a regulator, involvement in football or other sports sectors and cash-intensive activities including those that originate from casinos, betting shops and other activities related to gambling. This is not a definitive list.

| **Our services** | **Rarely** | **Some times** | **Often** |
|---|---|---|---|
| Do we act in complex or high value transactions? | | | |
| Do we act in cross-border transactions (particularly involving high risk countries)? | | | |
| Do we act for companies, trusts or other entities with structures which could be used to obscure ownership or control? | | | |
| Do we conduct non-face-to-face business relationships or transactions? | | | |
| Do we accept funds in cash? | | | |
| Do we receive payments from unknown or un-associated third parties? | | | |
| Do we provide services which for some other reason involve a substantial money laundering risk? | | | |

| **Internal issues** | **Rarely** | **Some times** | **Often** |
|---|---|---|---|
| Does any director, partner or member of staff display ignorance of or indifference to their AML/CFT obligations? | | | |
| Do we lack appropriate oversight of anyone in the Entity (particularly regarding customers or transactions)? | | | |
| Is there reason to doubt the reliability or strength of character or any director, partner or member of staff? | | | |
| Are we dependent on one source of work or person who could unduly influence any director, partner or member of staff? | | | |
| Have we had experience of any money laundering or financial crime in the past? | | | |

## Schedule 2 – Form of Risk Assessment Record[19]

*Note: the paragraphs included within the form of Risk Assessment Record are examples only. Each client should use this form as a guide only and must consider their own risks regarding their own business practices.*

The Entity has taken steps appropriate to the nature and size of its business to identify, assess and understand its money laundering and terrorist financing risks in relation to:

(a) the customers of the Entity;

(b) the countries or geographic areas in which those customers reside or operate;

(c) the products, services and transactions of the Entity; and

(d) the delivery channels of the Entity.

This has been considered in light of:

(a) the nature, scale and complexity of the Entity's business operations;

(b) the diversity of the Entity's operations, including its geographical diversity;

(c) the profile of the Entity's customers, products, services and activities;

(d) the distribution channels utilized by the Entity;

(e) the size and volume of the transactions engaged in by the Entity;

(f) the degree of risk associated with each area of the operations of the Entity;

(g) the extent to which the Entity is dealing directly with its or his customers or is dealing through intermediaries, third parties, correspondents or non-face to face channels; and

(h) the measure of regulatory compliance which has effect on AML/CFT compliance.

### A. Steps taken

The risk assessment was carried out by the Entity's Compliance Officer on___.

| |
|---|
| Checking the history of money laundering issues and compliance at the Entity, including considering the results of file reviews over the previous [two] years, the Entity's record or regulatory failures maintained by me as officer responsible, or the Compliance Officer, so far as they relate to AML issues and the history of suspicious activity reports. |

[19] The MLPA require risk assessments to be documented and to be kept current, and for financial institutions to have appropriate mechanisms in place to provide risk assessment information to the supervisory authorities (and competent authorities and self-regulatory bodies, if required).

Considering the risk factors identified by the regulatory and supervisory authorities in the Saint Lucia.

Reflecting on my personal experience of the services, customers, systems and personnel of the Entity.

Completing a Risk Assessment Questionnaire.

Leading a discussion of money laundering and terrorist financing risks at a meeting of the board of directors of the Entity on [*date*][20].

[20] Keep records of such meetings or other consultations held with senior management.

## B. The risks to which the Entity is subject[21]

### Overview[22]

Overall the Entity is considered to be [ ] [ ] [ ] risk.

| Country/geographic risk factors |
| --- |
| [*Insert*] |

21 Edit and expand the lists of risk factors as appropriate to reflect the business practices of and risks relevant to the Entity.

22 All relevant risk factors for each risk category should be considered before determining the overall risk classification (eg, high, medium or low) and the appropriate level of mitigation to be applied. The Entity should make its own determination as to the risk weights to be given to the individual risk factors or combination of risk

| Customer risk factors |
| --- |
| [*Insert* |

| **Product, service, transaction or delivery channel risk factors** |
| --- |
| [*Insert*] |

| **Risk management and mitigation[23]** |
| --- |
| [*Insert*] |

[23] The Entity should establish its risk tolerance, identifying the risks that it is willing to accept and the risks that it is not willing to accept. The Entity should consider the consequences, such as legal, regulatory, financial and reputational consequences, of an AML/CFT compliance failure. Dependent upon the level of risk which the Entity is willing to accept, it should then have mitigation measures and controls in place commensurate with those risks. Any such controls should be monitored and enhanced as and when necessary. Risk tolerance and any changes to mitigation measures and controls should be approved by senior management

## C. Review

This record reflects the Entity's current risks. It will be reviewed annually, or sooner in the event of major changes which are likely to affect the Entity's AML/CFT risks[25].

*Identify any reasons why the AML/CFT risks may have increased or reduced, or are likely to do so in the foreseeable future. This may include such things as the Entity providing new business services, the recruitment of new staff, restructure or changes in the Entity's customer profile, etc.*

| |
|---|
| Signature Date |

[24] Each risk assessment should be documented in order that the Entity can provide risk assessment to Saint Lucia supervisory authority and other competent bodies, if required.

[25] Identify any reasons why the AML/CFT risks may have increased or reduced, or are likely to do so in the foreseeable future. This may include such things as the Entity providing new business services, the recruitment of new staff, restructure or changes in the Entity's customer profile, etc.

**Schedule 3 – Form of Customer Risk Assessment**

*The risk factors included below should be considered when assessing the risk of an applicant/customer and/or a transaction. Please use the notes column to summarise observations/assessment of risks involved where the issue is applicable to the applicant/customer/transaction being considered.* ***Not all questions will be relevant or applicable to all situations. Conversely, the questions outlined are non-exhaustive– there may be other pertinent risk factors which should be taken into account, dependent upon the nature of the applicant/customer/transaction being considered.***

**Customer Risk Assessment**

| | | |
|---|---|---|
| **Name of applicant/customer:** | | |
| **Address of applicant/customer:** | | |
| **Contact details:** | **T** | |
| | **F** | |
| | **E** | |
| **Name and position of contact(s):** | | |
| **Brief description of transaction:** | | |

| **Risk factor** | **Yes/No** | **Notes** |
|---|---|---|
| ***Status of applicant/customer*** | | |
| 1. Is the applicant/customer known to you personally or an existing customer? | | |
| 2. Is the applicant/customer a new business relationship? | | |
| 3. Is the instruction from the applicant/customer channelled through a third party? If so, why? | | |
| 4. Is the applicant/customer a politically exposed person? | | |
| 5. If the applicant/customer is not a natural person but a legal entity, do you have full visibility and identification and verification of the beneficial owners and directors/controllers? | | |
| ***Face to face contact*** | | |
| 6. Have you met the applicant/customer face to face? | | |

| | | |
|---|---|---|
| 7. If this is a non face to face transaction/relationship, are you comfortable that there is a legitimate reason for this? | | |
| 8. If this is a non face to face transaction/relationship, is all communication effected via a regulated/listed/licenced intermediary? | | |
| ***Location of applicant/customer*** | | |
| 9. Where is the applicant/customer based? | --- | |
| 10. Are you aware of the applicant/customer having any links to criminality? | | |
| 11. Is the applicant/customer based in a high risk country or territory, or resident in/links to a sanctioned jurisdiction? | | |
| ***ID & address verification*** | | |
| 12. Has the applicant/customer provided acceptable standard ID and address verification? | | |
| 13. Has the applicant/customer provided acceptable non-standard ID and address verification? | | |
| 14. If reliant upon obtaining certified copies of ID & address verification, have you been able to confirm the authenticity/professional status of the certifier? | | |
| 15. Has the applicant/customer been co-operative in the process or have thy delayed providing ID & address verification or appeared reluctant to do so? | | |
| ***Financial profile of applicant/customer*** | | |
| 16. Does the stated source of wealth / source of funds and the amount of money involved stack up with what you know of the applicant/customer, for example given their age and occupation? (**Evidence** of source of wealth is required for high risk applicants/customers/transactions.) | | |
| 17. Is the applicant/customer involved in/run a high risk or high cash turnover business? | | |
| ***Type of transaction/activity*** | | |

| | | |
|---|---|---|
| 18. Could the type of transaction be used for the purposes of money laundering or terrorist financing, or is it at a higher risk of money laundering or terrorist financing? | | |
| 19. Does the transaction make sense or is it overly complex given the nature of the business being conducted? | | |
| 20. Does it make sense that the applicant/customer has asked the Entity to carry out this transaction? | | |
| ***Value of transaction*** | | |
| 21. Does the value of the transaction appear to fall within the financial means of the applicant/customer? | | |
| ***Source of funds*** | | |
| 22. Is the source of funds clear and identifiable? | | |
| 23. Are funds coming from a recognised financial/credit institution or are they personal funds? | --- | |
| 24. Is any funding coming from overseas? Where from? Who from? Connection to applicant/customer? | | |
| 25. Are any of the funds being paid by a third party otherwise unconnected to the transaction? | | |
| 26. Does the applicant/customer seek to change the source of funds at the last minute? | | |
| 27. Has the applicant/customer paid excess funds into the relevant account? Why/how? | | |
| ***Destination of funds*** | | |
| 28. Has the applicant/customer requested that any funds payable to it be paid to someone other than themselves or a lender? | | |
| 29. Are any such funds to be pad to an overseas account? | | |

| **Initial Customer Risk Assessment:** | **Low** (standard CDD) | **Medium** (standard CDD) | **High** (EDD) |
|---|---|---|---|
| *Insert the reasons for the assessment* | | | |
| Signed _____ by:<br>Name:<br>Position: | | Date: | |

| **Further Risk Assessment:**<br>**Have any risk factors changed?** | **Low** (standard CDD) | **Medium** (standard CDD) | **High** (EDD) |
|---|---|---|---|
| *Insert the reasons for the assessment*<br><br>*(If no, quick note stating as such, signed and dated, evidences that a review has been undertaken and consideration has been made)* | | | |
| Signed _____ by:<br>Name:<br>Position: | | Date: | |

**Schedule 4 – Sample Form of IDV Checklist - Individual**

| **Identification and Verification Checklist - Individual** | |
|---|---|
| **Name of individual:** | |
| **Name of applicant/customer: (if different)** | |

| | | |
|---|---|---|
| **1.** | **Verification of identity** | |
| | A certified copy* of one of**: | |
| | (a) a passport; | ☐ |
| | (b) a government-issued, photo bearing identity card; | ☐ |
| | (c) an armed forces identity card; or | ☐ |
| | (d) a driving licence. | ☐ |
| **2.** | **Proof of residence*** ** | |
| | (a) A certified copy* (dated not more than 3 months previously) of one of: | |
| | (i) a utility bill (other than a mobile telephone bill); | ☐ |
| | (ii) a bank/credit card statement; | ☐ |
| | (iii) correspondence from a Government Department; | ☐ |
| | **OR** | |
| | (b) An original letter of introduction from a business regulated by the FSRA | ☐ |
| | **OR** | |
| | (c) Written communication from a business regulated by the FSRA | |
| **3.** | **Systems & internet checks** | |
| | Google [*insert details of other searches which will be completed*] search(es) on the individual. | ☐ |
| **4.** | **Risk assessment** | |
| | (a) If this person is the applicant/customer, has a customer risk assessment form been completed? | ☐ / N/A |
| | (b) If this person is not the applicant/customer: | ☐ |

| | | |
|---|---|---|
| | (i) Are there any links to high risk countries or territories? | ☐ |
| | (ii) Is the person engaged in a high risk activity? | ☐ |
| | (iii) Is the person a PEP or connected to a PEP? | |
| **5. Source of wealth (where high risk)** | | |
| [*Insert details*] | | ☐ / N/A |
| **6. Source of funds (where high risk and applicable)** | | |
| [*Insert details*] | | ☐ / N/A |
| **7. Enhanced due diligence** | | |
| [*Where this is a high risk applicant/customer, insert details of the additional measures taken/documentation obtained to satisfy EDD requirements*] | | ☐ / N/A |
| **8. Simplified due diligence** | | |
| [*Insert explanation of the reason why SDD measures have been applied*] | | ☐ / N/A |
| **9. Attestation** | | |
| **Signature:** | | |
| **Name:** | | |
| **Date:** | | |
| **10. CO concurrence (where high risk or SDD is applied)** | | |
| **Signature:** | | |
| **Name:** | | |
| **Date:** | | |

*Notes*

* *Certifications – the following must be adhered to for a certified document to be acceptable:*

- *Persons approved to certify documents are members of a judiciary, senior civil servants, serving police or customs officers, lawyers, notaries, accountants, actuaries and officers of an embassy or high commission.*
- *Where specifically approved by the CO, directors, officers or managers of a regulated entity may also certify.*
- *Certifiers must not be related to the underlying individual.*

- *Certifiers must ensure that the following information is included with all certified documents:*
  - *Name and address of certifier.*
  - *Date on which certification is made.*
  - *Signature of certifier.*
  - *Where applicable, certifiers should affix their stamp or seal.*

** *Photo ID - the following must be checked to ensure photographic identity documents are acceptable:*

- *Ensure photograph in document is clear and image is plainly visible.*
- *Ensure the document contains the name of the individual;*
- *Ensure the document has not expired*
- *If the document is not in English, then a certified translation must be obtained.*
- *Ensure the document is properly certified.*

*** *Proof of residence - the following must be checked to ensure that proof of residence documents are acceptable:*

- *Ensure the document is dated within the past 3 months.*
- *Ensure the document is not a mobile telephone bill.*
- *Ensure that the document contains the individual's name and residential address (note that a PO Box may be included, but the residential address must also appear).*
- *Ensure the document contains activity (as opposed to a blank statement).*
- *If the document is not in English, then a certified translation must be obtained.*
- *Ensure the document is properly certified.*

**Schedule 5 – Sample Form of IDV Checklist - Company/LLC**

| **Identification and Verification Checklist – Company/LLC** | |
|---|---|
| **Name of company/LLC:** | |
| **Name of applicant/customer: (if different)** | |

| | | |
|---|---|---|
| **1.** | **Documents confirming incorporation/organisation** | |
| | (a) Certified copies* of: | |
| | (i) a certificate of incorporation/organisation (or equivalent); | ☐ |
| | (ii) (where possible) the memorandum and articles of association (or equivalent constitutional document)[26]; and | ☐ |
| | (iii) (where available) the audited accounts of the company, dated not more than 12 months previously and confirming that the company is incorporated/organised. | ☐ |
| | (b) An original or certified copy certificate of good standing. | ☐ |
| **2.** | **Business information** | |
| | Certified copies* of documents showing: | |
| | (a) unless provided under 1 above, the address of the registered office of the company and, if different, its main place of business; | ☐ |
| | (b) if relevant, any trading names of the company; and | ☐ |
| | (c) unless provided under 1 above, the principal business of the company. | ☐ |
| **3.** | **Ownership and management documents** | |
| | (a) If this company is the applicant/customer or where the applicant/customer is a limited partnership and this company is the general partner, certified copies* of: | |
| | (i) an up-to-date register of directors (or, in the case of an LLC, register of managers) of the company; | ☐ |
| | (ii) an up-to-date register of members of the company; | ☐ |
| | (iii) CDD documents (ie, the documents specified in the relevant IDV Checklist) in respect of: | ☐ |
| | (A) each entity (if any) directly holding 10% or more of the shares or voting rights in the company; | |

[26] Best practice is to obtain the constitutional documents of the company.

| | |
|---|---|
| (B) each individual (if any) holding 10% or more of the shares or voting rights in the company; | ☐ |
| (C) each individual (if any) exerting control over the company through other means; and | ☐ |
| (D) all directors (or in the case of an LLC, managers) of the company. | ☐ |
| (b) Where possible, a certified copy* ownership or structure chart setting out the up-to-date ownership chain of the company[27]. | ☐ |
| **4. Systems & internet checks** | |
| Google [*insert details of other searches which will be completed*] on each of: | |
| (a) the company; and | ☐ |
| (b) if the company is the applicant/customer or the general partner of a limited partnership which is the applicant/customer: | |
| (i) all directors/managers of the company; | ☐ |
| (ii) all direct shareholders/members of the company; and | ☐ |
| (iii) all individuals holding 10% or more of the ownership interests in the company. | ☐ |
| **5. Risk assessment** | |
| (a) If this entity is the applicant/customer, has a customer risk assessment form been completed? | ☐ / N/A |
| (b) If this entity is not the applicant/customer: | |
| (i) Are there any links to high risk countries or territories? | ☐ |
| (ii) Is the entity engaged in a high risk activity? | ☐ |
| (iii) Is the entity a PEP or connected to a PEP? | ☐ |
| **6. Source of wealth (where high risk)** | |
| [*Insert details*] | ☐ / N/A |
| **7. Source of funds (where high risk and applicable)** | |
| [*Insert details*] | ☐ N/A |
| **8. Enhanced due diligence** | |

[27] A structure chart may be certified by a director/manager of the company/LLC.

| | |
|---|---|
| [*Where this is a high risk applicant/customer, insert details of the additional measures taken/documentation obtained to satisfy EDD requirements*] | ☐ / N/A |
| **9. Simplified due diligence** | |
| [*Insert explanation of the reason why SDD measures have been applied*] | ☐ / N/A |
| **10. Attestation** | |
| **Signature:** | |
| **Name:** | |
| **Date:** | |
| **11. CO concurrence (where high risk or SDD is applied)** | |
| **Signature:** | |
| **Name:** | |
| **Date:** | |

*Notes*

* *Certifications – the following must be adhered to for a certified document to be acceptable:*

- *Persons approved to certify documents are members of a judiciary, senior civil servants, serving police or customs officers, lawyers, notaries, accountants, actuaries and officers of an embassy or high commission.*
- *Where specifically approved by the CO, directors, officers or managers of a regulated entity may also certify.*
- *Certifiers must not be related to the underlying individual.*
- *Certifiers must ensure that the following information is included with all certified documents:*
  - *Name and address of certifier.*
  - *Date on which certification is made.*
  - *Signature of certifier.*
  - *Where applicable, certifiers should affix their stamp or seal.*

**Schedule 6 – Sample Form of IDV Checklist – Limited Partnership**

| **Identification and Verification Checklist – Limited Partnership** | |
|---|---|
| **Name of limited partnership:** | |
| **Name of applicant/customer: (if different)** | |

| | | |
|---|---|---|
| **1.** | **Documents confirming registration** | |
| | (a) Certified copies* of: | |
| | (i) a certificate of registration (or equivalent) of the limited partnership; and | ☐ |
| | (ii) the limited partnership agreement/deed (including all supplements/amendments, etc). | ☐ |
| | (b) An original or certified copy certificate of good standing. | ☐ |
| **2.** | **Business information** | |
| | Certified copies* of documents showing: | |
| | (a) unless provided under 1 above, the address of the registered office of the limited partnership and, if different, its main place of business; | ☐ |
| | (b) if relevant, any trading names of the limited partnership; and | ☐ |
| | (c) unless provided under 1 above, the principal business of the limited partnership. | ☐ |
| **3.** | **Ownership and management documents** | |
| | (a) If this limited partnership is the applicant/customer, certified copies* of CDD documents (ie, the documents specified in the relevant IDV Checklist) in respect of: | |
| | (i) each entity (if any) directly holding 10% or more of the ownership interests in the limited partnership; | ☐ |
| | (ii) each individual (if any) holding 10% or more of the ownership interest in the limited partnership; | ☐ |
| | (iii) each individual (if any) exerting control over the limited partnership; through other means; and | ☐ |
| | (iv) the/each general partner of the limited partnership. | ☐ |
| | (a) Where possible, a certified copy* ownership or structure chart setting out the up-to-date ownership chain of the limited partnership. | ☐ |

| | | |
|---|---|---|
| **4.** | **Systems & internet checks** | |
| | Google [*insert details of other searches which will be completed*] on each of: | |
| | (a) the limited partnership; | ☐ |
| | (b) each partner of the limited partnership; and | ☐ |
| | (c) each individual holding 10% or more of the ownership interests in the limited partnership. | ☐ |
| **5.** | **Risk assessment** | |
| | (a) If this entity is the applicant/customer, has a customer risk assessment form been completed? | ☐ / N/A |
| | (b) If this entity is not the applicant/customer: | |
| | (i) Are there any links to high risk countries or territories? | ☐ |
| | (ii) Is the entity engaged in a high risk activity? | ☐ |
| | (iii) Is the entity a PEP or connected to a PEP? | ☐ |
| **6.** | **Source of wealth (where high risk)** | |
| | [*Insert details*] | ☐ / N/A |
| **7.** | **Source of funds (where high risk and applicable)** | |
| | [*Insert details*] | ☐ / N/A |
| **8.** | **Enhanced due diligence** | |
| | [*Where this is a high risk applicant/customer, insert details of the additional measures taken/documentation obtained to satisfy EDD requirements*] | ☐ / N/A |
| **9.** | **Simplified due diligence** | |
| | [*Insert explanation of the reason why SDD measures have been applied*] | ☐ / N/A |
| **10.** | **Attestation** | |
| **Signature:** | | |
| **Name:** | | |
| **Date:** | | |

| **11. CO concurrence (where high risk or SDD is applied)** | |
|---|---|
| **Signature:** | |
| **Name:** | |
| **Date:** | |

*Notes*

* *Certifications – the following must be adhered to for a certified document to be acceptable:*

- *Persons approved to certify documents are members of a judiciary, senior civil servants, serving police or customs officers, lawyers, notaries, accountants, actuaries and officers of an embassy or high commission.*
- *Where specifically approved by the CO, directors, officers or managers of a regulated entity may also certify.*
- *Certifiers must not be related to the underlying individual.*
- *Certifiers must ensure that the following information is included with all certified documents:*
  - *Name and address of certifier.*
  - *Date on which certification is made.*
  - *Signature of certifier.*
  - *Where applicable, certifiers should affix their stamp or seal.*

**Schedule 7 – Sample Form of IDV Checklist – Partnership**

| **Identification and Verification Checklist – Partnership (not limited partnership)** | |
|---|---|
| **Name of partnership:** | |
| **Name of applicant/customer: (if different)** | |

| | | |
|---|---|---|
| **1.** | **Establishment documents** | |
| | A certified copy* of the partnership agreement/deed (including all supplements/amendments, etc). | ☐ |
| **2.** | **Business information** | |
| | Certified copies* of documents showing: | |
| | (a) unless provided under 1 above, the address of the registered office of the partnership and, if different, its main place of business; | ☐ ☐ |
| | (b) if relevant, any trading names of the partnership; and | ☐ |
| | (c) unless provided under 1 above, the principal business of the partnership. | |
| **3.** | **Ownership and management documents** | |
| | (a) If this partnership is the applicant/customer, certified copies* of CDD documents (ie, the documents specified in the relevant IDV Checklist) in respect of[28]: | |
| | (i) each entity (if any) directly holding 10% or more of the ownership interests in the partnership; | ☐ ☐ |
| | (ii) each individual (if any) holding 10% or more of the ownership interests in the partnership; and | ☐ |
| | (iii) each individual (if any) exerting control over the partnership through other means. | ☐ |
| | (b) Where possible, a certified copy* ownership or structure chart setting out the up-to-date ownership chain of the partnership. | |
| **4.** | **Systems & internet checks** | |
| | Google [*insert details of other searches which will be completed*] on each of: | |
| | (a) the partnership; | ☐ ☐ |
| | (b) each partner of the partnership; and | ☐ |

[28] CDD documents are required in respect of at least two partners.

| | |
|---|---|
| (c) each individual holding 10% or more of the ownership interests in the partnership. | |
| **5. Risk assessment** | |
| (a) If this entity is the applicant/customer, has a customer risk assessment form been completed? | ☐ / N/A |
| (b) If this entity is not the applicant/customer: | |
| (i) Are there any links to high risk countries or territories? | ☐ |
| (ii) Is the entity engaged in a high risk activity? | ☐ |
| (iii) Is the entity a PEP or connected to a PEP? | ☐ |
| **6. Source of wealth (where high risk)** | |
| [*Insert details*] | ☐ / N/A |
| **7. Source of funds (where high risk and applicable)** | |
| [*Insert details*] | ☐ / N/A |
| **8. Enhanced due diligence** | |
| [*Where this is a high risk applicant/customer, insert details of the additional measures taken/documentation obtained to satisfy EDD requirements*] | ☐ / N/A |
| **9. Simplified due diligence** | |
| [*Insert explanation of the reason why SDD measures have been applied*] | ☐ / N/A |
| **10. Attestation** | |
| **Signature:** | |
| **Name:** | |
| **Date:** | |
| **11. CO concurrence (where high risk or SDD is applied)** | |
| **Signature:** | |
| **Name:** | |
| **Date:** | |

*Notes*

* *Certifications – the following must be adhered to for a certified document to be acceptable:*

- *Persons approved to certify documents are members of a judiciary, senior civil servants, serving police or customs officers, lawyers, notaries, accountants, actuaries and officers of an embassy or high commission.*
- *Where specifically approved by the CO, directors, officers or managers of a regulated entity may also certify.*
- *Certifiers must not be related to the underlying individual.*
- *Certifiers must ensure that the following information is included with all certified documents:*
  - *Name and address of certifier.*
  - *Date on which certification is made.*
  - *Signature of certifier.*
  - *Where applicable, certifiers should affix their stamp or seal.*

**Schedule 8 – Sample Form of IDV Checklist – Trust/Unit Trust**

| **Identification and Verification Checklist – Trust/Unit Trust** | |
|---|---|
| **Name of trust/unit trust:** | |
| **Name of applicant/customer: (if different)** | |

| **1.** | **Documents confirming establishment** | |
|---|---|---|
| | One of the following: | ☐ |
| | (a) a certified copy* of the trust deed (including all supplements/amendments, etc); or | |
| | (b) a certified copy* of some other document showing: | |
| | (i) the name of the trust/unit trust; | |
| | (ii) the date and place of establishment of the trust/unit trust; | |
| | (iii) the general nature of the trust/unit trust; | |
| | (iv) the full name(s) and address(es) of each trustee of the trust/unit trust; and | |
| | (v) in relation to a unit trust, the full name(s) and address(es) of each unit holder of the unit trust; or | |
| | (vi) in relation to a trust: | |
| | (A) the full name(s) and address(es) of the settlor of the trust; | |
| | (B) the full name(s) and address(es) of each beneficiary of the trust; and | |
| | (C) the full name(s) and address(es) of any protector of the trust. | |
| **2.** | **Parties involved with the trust/unit trust** | |
| | If the applicant/customer is a trustee of a trust/unit trust, CDD documents (ie, the documents specified in the relevant IDV Checklist) in respect of: | ☐ |
| | (a) each trustee of that trust/unit trust; and | |
| | (b) in relation to a unit trust: | ☐ |
| | (i) each unitholder holding 10% or more of the units of that unit trust; | ☐ |
| | | ☐ |

| | |
|---|---|
| (ii) each individual (if any) ultimately holding 10% or more of the units of the unit trust or who exert control through other means; and<br><br>(iii) each individual (if any) exercising control through other means; or<br><br>(c) in relation to a trust:<br><br>(i) the settlor of that trust;<br><br>(ii) the beneficiaries of that trust;<br><br>(iii) the protector of that trust; and<br><br>(iv) each individual (if any) who exercises control over the trust through other means. | ☐<br>☐<br>☐<br>☐ |
| **3. Systems & internet checks** | |
| Google [*insert details of other searches which will be completed*] on each of:<br><br>(a) the partnership;<br><br>(b) each partner of the partnership; and<br><br>(c) each individual holding 10% or more of the ownership interests in the partnership. | ☐<br>☐<br>☐ |
| **4. Risk assessment** | |
| (a) If this entity is the applicant/customer, has a customer risk assessment form been completed?<br><br>(b) If this entity is not the applicant/customer:<br><br>(i) Are there any links to high risk countries or territories?<br><br>(ii) Is the entity engaged in a high risk activity?<br><br>(iii) Is the entity a PEP or connected to a PEP? | ☐ / N/A<br><br>☐<br>☐<br>☐ |
| **5. Source of wealth (where high risk)** | |
| [*Insert details*] | ☐ / N/A |
| **6. Source of funds** | |
| [*Insert details*] | ☐ / N/A |
| **7. Enhanced due diligence** | |

| | |
|---|---|
| [*Where this is a high risk applicant/customer, insert details of the additional measures taken/documentation obtained to satisfy EDD requirements*] | ☐ / N/A |
| **8. Simplified due diligence** | |
| [*Insert explanation of the reason why SDD measures have been applied*] | ☐ / N/A |
| **9. Attestation** | |
| **Signature:** | |
| **Name:** | |
| **Date:** | |
| **10. CO concurrence (where high risk or SDD is applied)** | |
| **Signature:** | |
| **Name:** | |
| **Date:** | |

*Notes*

* *Certifications – the following must be adhered to for a certified document to be acceptable:*

- *Persons approved to certify documents are members of a judiciary, senior civil servants, serving police or customs officers, lawyers, notaries, accountants, actuaries and officers of an embassy or high commission.*
- *Where specifically approved by the CO, directors, officers or managers of a regulated entity may also certify.*
- *Certifiers must not be related to the underlying individual.*
- *Certifiers must ensure that the following information is included with all certified documents:*
  - *Name and address of certifier.*
  - *Date on which certification is made.*
  - *Signature of certifier.*
  - *Where applicable, certifiers should affix their stamp or seal.*

**Schedule 9 – Form of Internal Suspicious Activity Report (SAR)**

*This form should be completed and submitted when appropriate, and as soon as is practicable to the CO, in accordance with Part O of this Manual.*

**Section A: For completion by the CO following receipt of the SAR**

| | |
|---|---|
| **Date SAR received** | |
| **Unique SAR reference**<br>**From the SAR register** | |

**Section B: For completion by the person(s) of the Entity who submits the SAR (the 'reportee')**

| **Reportee Information** | | |
|---|---|---|
| **Reportee name(s)** [29] | | |
| **Reportee practice area** | | |
| **Reportee position(s)**<br>eg Director/ Officer/ Employee | | |

| **Disclosure Subject - Personal Information**<br>Please copy and paste this section as necessary if more than one individual is involved | | |
|---|---|---|
| **Individual's full name** | | |
| **Other names** if applicable / known | | |
| **Gender** | | |
| **Date & place of birth** | | |
| **Nationality** | | |
| **Identification details**<br>ID type (ie passport) & number etc, if known | | |
| **Full residential address** | | |
| **Telephone / fax number(s)** | Home: | Work: |
| | Mobile: | Fax: |
| **Occupation, employer & business address** if known | | |
| **Has verification been undertaken?** | | |

[29] If a reportee is aware that the reportee shares the same reasons for suspicion as another reportee they may jointly submit a SAR should they wish to rely on the same disclosure content. If reportees have differing reasons for suspicion they should each complete and submit their own SAR in order to meet their reporting obligations. Each co-reportee should review and agree the content prior to submission and the submitter should copy their co-reportee on the submission email to the CO. It is not 'tipping off' to discuss/prepare this SAR with a reportee who intends to rely on its submission to the CO.

| **Disclosure Subject - Personal Information**<br>Please copy and paste this section as necessary if more than one individual is involved | | |
|---|---|---|
| **Individual's full name** | | |
| **Other names** if applicable / known | | |
| **Gender** | | |
| **Date & place of birth** | | |
| **Nationality** | | |
| **Identification details**<br>ID type (ie passport) & number etc, if known | | |
| **Full residential address** | | |
| **Telephone / fax number(s)** | Home: | Work: |
| | Mobile: | Fax: |
| **Occupation, employer & business address** if known | | |
| **Has verification been undertaken?** | | |

| **Disclosure Subject - Personal Information**<br>Please copy and paste this section as necessary if more than one individual is involved | | |
|---|---|---|
| **Individual's full name** | | |
| **Other names** if applicable / known | | |
| **Gender** | | |
| **Date & place of birth** | | |
| **Nationality** | | |
| **Identification details**<br>ID type (ie passport) & number etc, if known | | |
| **Full residential address** | | |
| **Telephone / fax number(s)** | Home: | Work: |
| | Mobile: | Fax: |
| **Occupation, employer & business address** if known | | |
| **Has verification been undertaken?** | | |

| **Disclosure Subject - Legal Entity Information**<br>Please copy and paste this section as necessary if more than one legal entity is involved | |
|---|---|
| **Type of legal entity**<br>ie company / trust / partnership etc | |
| **Full legal entity name** | |
| **Registration number** if any | |
| **Date & place of formation** | |
| **Registered office address** | |

| | |
|---|---|
| if applicable | |
| **Operating address** | |
| **Telephone number** | |
| **Beneficial owner(s)** Full ownership chain down to ultimate beneficial owner; include full names & percentages, if known; structure chart may be attached if available | |
| **Has verification been undertaken?** | |

| **Other Associated Person(s) or Legal Entity(ies)** | |
|---|---|
| **Full relevant details** ie name, address, relationship with disclosure subject, anything else pertinent to the situation | |

| **Relationship Details** | |
|---|---|
| **Relevant date** | |
| **Services provided by the Entity** or sought if SAR relates to prospective client or declined business | |
| **Source of Funds / Source of Wealth information held** if any | |
| **Details of any assets held or controlled by the Entity** ie type of assets, where held, current value (actual or estimated) | |
| **Details of intermediary** if any | |

| **Client Money Bank Details**[30] If any client money is held / controlled by the Entity | |
|---|---|
| **Bank name** | |
| **Bank address** | |
| **Account name** | |
| **Account number** | |
| **Is it a "pooled" account?** | |
| **Currency, value and source of funds** | |

[30] If client money is held in an account with one of the Entity's bankers the CO may request authorisation from the FIA to disclose information regarding the matter of concern to that bank. In order to not commit a tipping off offence you must not inform the bankers or any other party yourself.

| | |
|---|---|
| **Nature of transaction** ie why held | |
| **Related transaction details** if any | |

| **Reasons for Suspicion** | | |
|---|---|---|
| **Describe the circumstances and reasons for your suspicion, including details and status of any transaction or activity of concern**<br>– Please be detailed and clear in order to provide the CO with sufficient and relevant information to determine whether or not to make an external SAR to the FIA.<br>– Please attach any relevant supporting documents to your covering email which might be of assistance, such as a structure chart if multiple (5 or more) entities are involved.<br>– Make it clear if a transaction is pending and / or urgent and put the work and transaction on hold until the CO advises how to proceed.<br>– The CO may seek further information in order to assist with their determination. | | |
| **What prompted submission of this SAR**<br>ie monitoring / periodic review / open source information / transaction | | |
| **Date the knowledge / suspicion (or reasonable grounds for such knowledge / suspicion) came to your attention** | | |

- **Submit the completed form by email to the CO**.
- **Avoid committing a tipping off offence:** do not discuss the SAR with its subject or a third party unless the CO advises otherwise. Refer to Part N and Part O of this Manual for tipping off guidance.
- **Do not place a copy of the SAR or related correspondence on any client file.** The CO will advise you of the relevant processes. Refer to Part M and Part O of this Manual for record keeping requirements.

## Schedule 10 – Glossary

| | |
|---|---|
| **AML** | Anti-money laundering |
| **CDD** | Customer due diligence |
| **EDD** | Enhanced customer due diligence |
| **SDD** | Simplified customer due diligence |
| **CFT** | Counter financing of terrorism |
| **CO** | Compliance Officer |
| **CPF** | Counter proliferation financing |
| **FATF** | Financial Action Task Force |
| **FI** | Financial Institution |
| **KYC** | Know Your Client |
| **ML** | Money laundering |
| **PEP** | Politically exposed person, including (for the purposes of this Manual) a family member or close associate of a politically exposed person |
| **PF** | Proliferation financing |
| **SAR** | Suspicious activity report |
| **TF** | Terrorist financing |
| **TFS** | Targeted financial sanctions |