Your Private Broker

Doo Prime

Anti-Money Laundering And Counter-Terrorism Financing Policy

Doo Prime Mauritius Limited

Updated on 21 December 2020

1. INTRODUCTION

1.1 Doo Prime Mauritius Limited (referred to as “Doo Prime”, “we”, “us” or “our”) combats against any forms of money laundering, terrorism financing or criminal activities by strictly comply with the laws and regulations on Anti-Money Laundering (“AML”), Financial Intelligence and Anti-Money Laundering Act 2002 (“Act”), Financial Intelligence and Anti-Money Laundering Regulation 2018 (“Regulation”), Mauritius Financial Services Commission (“MFSC”)’s Code on Anti-Money Laundering and Counter-Terrorist Financing (“Code”), MFSC’s Handbook on Anti-Money Laundering and Counter-Terrorist Financing (“Handbook”), Prevention of Terrorism Act 2002, Prevention of Corruption Act 2002, Financial Action Task Force Recommendations and other relevant applicable regulatory regulation as required by the Mauritius government and the MFSC.

1.2 Our Money Laundering Reporting Officer (“MLRO”) and other Compliance Officer (“CO”) are employed to implement the appropriate Anti-Money Laundering and Counter-Terrorism Financing (“AML and CTF”) policies and procedures.

1.3 Doo Prime has established a series of AML procedures for the compliance of the Act and will apply our AML and Know-Your-Client (“KYC”) procedures in all securities transactions. We shall take all reasonable measures to prevent and mitigate Money Laundering and Terrorism Financing (“ML and TF”) activities.

1.4 We adopt a risk-based approach in the implementations of our AML and CTF systems and for the purposes of detecting ML and TF risks. We shall update our AML and CTF systems and policies at least once annually to take into account new and emerging risks, considering:

(a) the nature and level of money laundering and terrorism financing risk that we may reasonably expect to face in the course of our business;

(b) the nature, size and complexity of our business;

(c) development of new products and new business practices, including new delivery mechanisms; and

(d) use of new or developing technologies for both new and pre-existing products.

2. DEFINITIONS AND INTERPRETATIONS

2.1 The following terms shall carry the following meaning:

(a) “Act” means Anti-Money Laundering, Financial Intelligence and Anti-Money Laundering Act 2002.

(b) “CO” means compliance officer.

(c) “Code” means Mauritius Financial Services Commission’s Code on Anti-Money Laundering and Counter-Terrorist Financing.

(d) “Handbook” means MFSC’s Handbook on Anti-Money Laundering and Counter-Terrorist Financing.

(e) "MFIU" means Mauritius Financial Intelligence Unit.

(f) "MFSC" means Mauritius Financial Services Commission.

(g) "MLRO" means money laundering reporting officer.

(h) "Money laundering" means the conduct which constitutes an offence of money laundering under section 11 of the Proceeds of Crime Act [CAP 284], i.e.

(i) the person engages, directly or indirectly, in a transaction that involves money, or other property, that the person knows, or ought reasonably to know, to be proceeds of crime; or

(ii) the person receives, possesses, conceals, disposes of or brings into Mauritius money, or other property, that the person knows, or ought reasonably to know, to be proceeds of crime.

(i) "Politically exposed person" or "PEP" means an individual who is or has been entrusted with prominent public functions such as the Head of State, the Prime Minister, Ministers, senior politicians, senior government officials, judicial or military officials, senior executive members of state-owned corporations or international organisations and officials of a political part.

(j) "Proceeds of crime" means property derived or realised directly or indirectly from a serious offence, including:

(i) property into which any property derived or realised directly from the offence is later successively converted or transformed; and

(ii) income, capital or other economic gains derived or realised from that property since the offence.

If the property that is proceeds of crime (the original proceeds) is intermingled with other property from which it cannot readily be separated, that proportion of the whole represented by the original proceeds is taken to be proceeds of crime.

(k) "Proliferation financing" means the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

(l) "Regulation" means Financial Intelligence and Anti-Money Laundering Regulation 2018.

(m) "Source of wealth" refers to the origin of an individual's entire body of wealth (i.e. total assets).

(n) "Source of funds" refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and us (e.g. the amounts being invested, deposited, or wired as part of the business relationship).

(o) "Terrorist financing" or "Terrorism financing" means:

(i) the provision or collection, by any means, directly or indirectly, of any property:
(aa) with the intention that the property be used; or
(ab) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is so used);

(ii) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether the person is a terrorist or terrorist associate; or

(iii) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether the person is a terrorist or terrorist associate.

3. MONEY LAUNDERING

3.1 The stages of money laundering are as follows:

(a) Placement - disposal of cash proceeds derived from illegal activities;

(b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and

(c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

3.2 Some of the possible signs of money laundering includes, but is not limited to the following:

(a) reluctance by clients to provide information;

(b) incomplete or inconsistent information by clients;

(c) irregular money transfers and transactions;

(d) unexplained third-party investment;

(e) transactions carried by unusually high volume;

(f) source of funds from poorly-regulated sources;

(g) transactions with no apparent legitimate or economic purpose;

(h) transactions which are unnecessarily complex;

(i) client's lifestyle appears in excess of known sources of income;

(j) business structure is unnecessarily complicated;

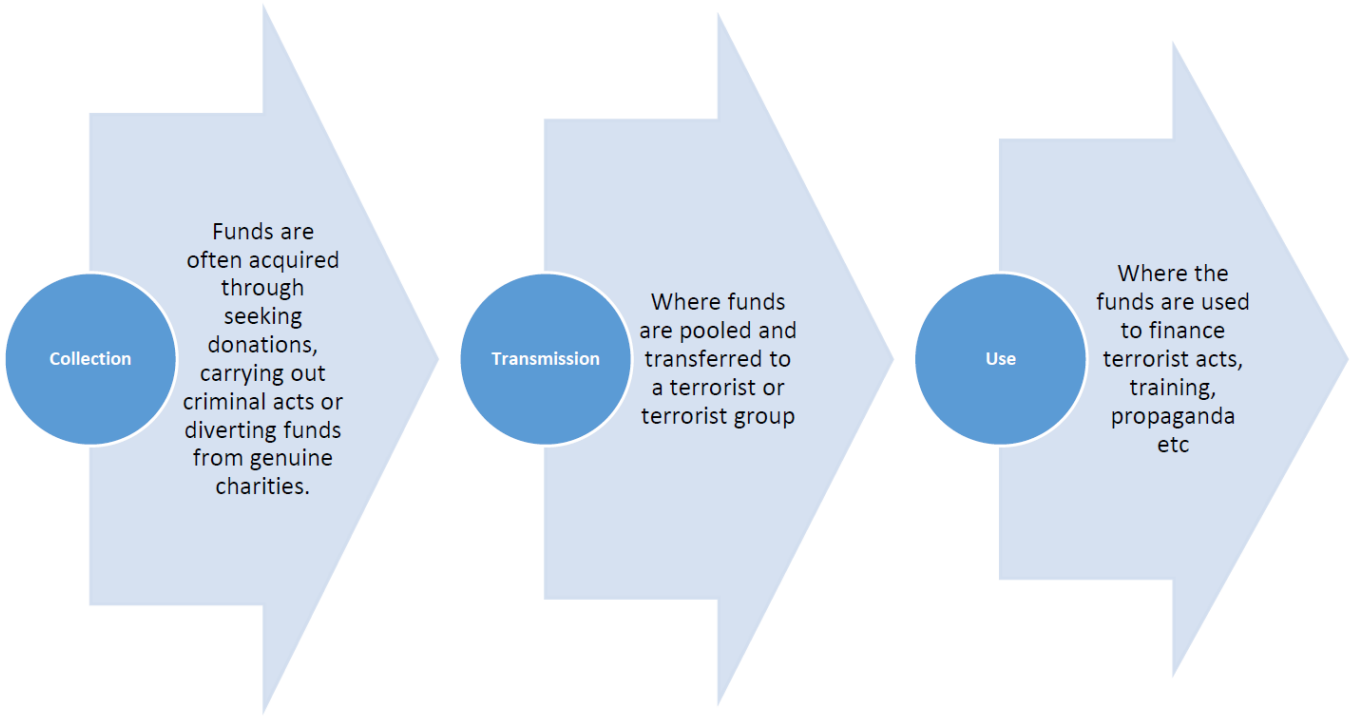
(k) use of bank accounts without valid reason;

(l) the client appears to be acting as an agent for another entity or individual but is evasive about the identity of another identity;

(m) the client has multiple accounts under a single name or multiple names, with a large number of inter-account transfers;

(n) the client deposits funds followed by a request to withdraw the funds.

3.3 Terrorism financing refers to the act of supporting and financing of terrorism activities. Unlike money laundering, the source of funds of terrorism financing can be legitimate. Terrorism financing generally involves a complex series of transactions. The Handbook has explained the flow of a generic terrorism financing model (illustrated below).



4. CLIENT DUE DILIGENCE ("CDD")

4.1. Doo Prime has established a "know your client" policy to verify the identities of all our clients and to conduct client due diligence ("CDD"). We perform ongoing due diligence process to monitor our client's account, service or relationship with each of our clients to identify, mitigate and manage the risk it may reasonably face with its client that might involve money laundering, financing of terrorism or other serious offences.

4.2 As provided under Section 3 of the Regulation, we shall:

(a) identify our client whether permanent or occasional and verify the identity of our client using reliable, independent source documents, data or information, including, where available, electronic identification means, or any other secure, remote or electronic identification process as may be specified by the relevant regulatory body or supervisory authority;

(b) verify that any person purporting to act on behalf of a client is so authorised, and shall identify and verify the identity of that person;

(c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source such that the Doo Prime is satisfied that he knows who the beneficial owner is;

(d) understand and obtain adequate and relevant information on the purpose and intended nature of a business relationship or occasional transaction;

(e) conduct ongoing monitoring of a business relationship, including:

(i) scrutiny of transactions undertaken throughout the course of the relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with his knowledge of the client and the business and risk profile of the client;

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

4.3 Section 17C of the Act imposed a statutory requirement to conduct CDD:

(a) when opening an account for, or otherwise establishing a business relationship with, a client;

(b) where a client who is neither an account holder nor in an established business relationship with Doo Prime wishes to carry out:

(i) a transaction in an amount equal to or above 500,000 rupees or an equivalent amount in foreign currency or such amount as may be prescribed, whether conducted as a single transaction or several transactions that appear to be linked; or

(ii) a domestic or cross-border wire transfer;

(c) whenever doubts exist about the veracity or adequacy of previously obtained client identification information;

(d) whenever there is a suspicion of money laundering or terrorism financing involving the client or the client's account.

4.4 If the client is an individual, we shall obtain and verify the following information as required by Section 4 of the Regulation:

(a) the full legal and any other names, including, marital name, former legal name or alias;

(b) the date and place of birth;

(c) the nationality;

(d) the current and permanent address; and

(e) such other information as may be specified by a relevant supervisory authority or regulatory body.

4.5 If the client is a business entity, we shall obtain and verify the following information as required by Section 5 of the Regulation:

(a) in relation to the client, understand and document:

(i) the nature of his business; and

(ii) his ownership and control structure;

(b) identify the client and verify his identity by obtaining the following information:

(i) name, legal form and proof of existence;

(ii) powers that regulate and bind the client;

(iii) names of the relevant persons having a senior management position in the body corporate or arrangement; and

(iv) the address of the registered office and, if different, a principal place of business.

4.6 Section 6 of the Regulation mentioned that identity verification of beneficial owners can be done by obtaining information on:

(a) the identity of all the natural persons who ultimately have an ownership interest of 20% or more in the body corporate;

(b) where there is doubt under subparagraph (a) as to whether the person with the ownership interest of 20% is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control of the body corporate through other means as may be specified by the relevant regulatory body or supervisory authority; and

(c) where no natural person is identified under subparagraph (a) and (b), the identity of the relevant person who holds the position of senior managing official.

4.7 Section 10 of the Regulation also provides that in determining when to take CDD measures in relation to existing clients, we shall take into account, among other things:

(a) any indication that the identity of the client or the beneficial owner, has changed;

(b) any transactions which are not reasonably consistent with his knowledge of the client;

(c) any change in the purpose or intended nature of his relationship with the client;

(d) any other matter which might affect his assessment of the money laundering, terrorist financing or proliferation financing risk in relation to the client.

4.8 **Required document and information list** (adopted from Section 5.3 of the Handbook).

A. FOR INDIVIDUAL CLIENTS

No.	Data to be collected	Permissible methods for verifying data:
1	Legal name (including any former names, aliases and any other names used)	(a) current valid passport (b) current valid national identity card (c) current valid driving licence (where Doo Prime is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence). In each case, the document must incorporate photographic evidence of identity. Where the body corporate with which the natural person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. However, where the body corporate is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary
2	Sex	
3	Date of birth	
4	Place of birth	
5	Nationality	
6	Current residential address. PO Box addresses are not acceptable	(a) any of the identity sources listed above; (b) a recent utility bill issued to the individual by name; (c) a recent bank or credit card statement; or (d) a recent reference or letter of introduction from (i) a financial institution that is regulated in Mauritius; (ii) a regulated financial services business which is operating in an equivalent jurisdiction or a jurisdiction that complies with
7	Permanent residential address (if different to current residential address)	

No.	Data to be collected	Permissible methods for verifying data:
		the FATF standards; or (iii) a branch or subsidiary of a group headquartered in a well-regulated overseas country or territory which applies group standards to subsidiaries and branches worldwide, and tests the application of, and compliance with, such standards. 'recent' means within the last three months.
8	Any public position held and, where appropriate, nature of employment (including self-employment) and name of employer	A letter or other written confirmation of the individual's status from the public body in question and or any enhanced CDD; a letter or other written confirmation of employment.
9	Government issued personal identification number or other government issued unique identifier	The relevant government document.

B. FOR BODY CORPORATE CLIENTS

No.	Persons to be identified	Data to be identified	Method of data verification
1	Underlying persons who are individuals.	As per the requirements for a natural person. Where the individual persons are such by virtue of their status as members of the board of directors of a relevant body corporate (or equivalent – for examples partners in a partnership, or council members in a foundation), financial institutions are required to identify and verify the identity of all such persons.	As per the requirements for individuals. Where the body corporate with which the underlying person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. However where the body corporate is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary
2	Private companies	1. Legal status of body 2. Legal name of body 3. Any trading names 4. Nature of business	a. Certificate of incorporation (or other appropriate certificate of registration or licensing); b. Memorandum and Articles of Association (or equivalent);
3	Partnerships		

No.	Persons to be identified	Data to be identified	Method of data verification
4	Sociétés	5. Date and country of incorporation/registration 6. Official identification number (for example, company number) 7. Registered office address 8. Mailing address (if different) 9. Principal place of business / operations (if different) 10. Any other data which the financial institution considers to be reasonably necessary for the purposes of establishing the true identity of the body corporate.	c. Company registry search, including confirmation that the person is not in the process of being dissolved, struck off, wound up or terminated; d. Latest audited financial statements or equivalent; e. Annual report or equivalent; f. Personal visit to principal place of business; g. Partnership deed or equivalent; h. Charter of Foundation; i. Acte de société; j. Certificate of good standing from a relevant national body; k. Reputable and satisfactory third party data, such as a business information service. l. Any other source of information that to verify that the document submitted is genuine.
5	Foundations		
6	Other body corporates		

4.9 We strictly prohibit establishing any business relationship with clients with false, fictitious or misleading names, and we shall make a record of if any of our clients is using a different name from which the client is commonly known.

4.10 We will consider on a case-by-case basis any clients that cannot reasonably be expected to produce the standard evidence of identity and will seek to agree on the use of other confirmations of identity so that clients are not unreasonably denied access to the products and services. In the event it is reasonably proved that there is doubt on the identification and verification of the beneficial owners, we may carry out CDD on the senior management officials of the client in accordance with this AML and CTF policy.

4A. VERIFICATION

4A.1 We shall verify the client's information above through our client service and risk management department, together with Refinitiv Limited's World-Check One systems. Our scope of CDD includes, but is not limited to our retail clients, business partners, the board members, shareholders and ultimate beneficial owners. We carry out the following CDD measures:

(a) identifying the client and verifying the client's identity using documents, data or information provided by a reliable and independent source;

(b) where there is a beneficial owner in relation to the client, identifying and taking reasonable measures to verify the beneficial owner's identity so that we are satisfied that we know who the beneficial owner is, including in the case where the client is a

body corporate or trust, measures to enable us to understand the ownership and control structure of the body corporate or trust;

(c) obtaining information on the purpose and intended nature of the business relationship (if any) established with us unless the purpose and intended nature are obvious; and

(d) if a person purports to act on behalf of the client:

(i) identifying the person and taking reasonable measures to verify the person's identity using documents, data or information provided by a reliable and independent source; and

(ii) verifying the person's authority to act on behalf of the client;

(e) if we deem the identity verification unsatisfactory or insufficient, we will not establish a business partnership or proceed with any further transaction. If the client either refuses to provide the required information, or provide false/misleading information, we will terminate the business partnership or reject the requested transactions.

4A.2 In the identity verification process, we will request a copy of the original and a coloured scanned copy of the identification documents; we may also request more than one identity documents for cross-verification if we deem necessary.

4A.3 When electronic verification is used or a client has not been physically present for identification purposes, we will carry out an additional verification check to manage the risk of impersonation fraud. This check may take the form of:

(a) requiring the first payment to be carried out through an account in the client's name with a regulated credit institution;

(b) telephone contact with the client on a home or business number that has been verified, before opening the account;

(c) communicating with the client at the address that has been verified;

(d) requiring copy documents to be certified by an appropriate person.

4A.4 If we are unable to carry out the prescribed identification process on a person, we:

(a) shall not open an account for the person;

(b) shall not enter into a business relationship with the person; and

(c) if a business relationship already exists with the person, we shall terminate the existing business relationship.

5. AML AND CTF SCREENING PROCESS

5.1 We strictly prohibit clients related to terrorism financing, proliferation financing, PEP and clients on the financial sanctions list decided by the UN Security Council. We shall not conduct any business relationship with them in any way.

5.2 We screen:

(a) clients and any beneficial owners of the clients against the current database at the establishment of the relationship;

(b) clients and any beneficial owners of the clients against all new and any updated designations to the database as soon as practicable; and

(c) all relevant parties in a cross-border wire transfer against the current database before executing the transfer;

(d) against the latest list of designated individuals and entities extracted from:

(i) UN Security Council https://www.un.org/securitycouncil/;

(ii) Mauritius FSC https://www.fscmauritius.org/en;

(iii) Refinitiv Limited, UK;

(iv) Office of Foreign Asset Control US Department of the Treasury ("OFAC") at https://sanctionssearch.ofac.treas.gov/;

(v) Office of Financial Sanctions Implementation HM Treasury UK, https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets.

5.3 We have engaged Refinitiv Limited to perform their World-Check One systems on our clients for sanction list filtering. Their screening systems also entails the following:

5.3.1 Clients and entities

- Foreign financial institutions, including banks and foreign money services providers (e.g., casas de cambio, currency exchanges, and money transmitters).
- Nonbank financial institutions (e.g., money services businesses; casinos and card clubs; brokers/dealers in securities; and dealers in precious metals, stones, or jewels).
- Senior foreign political figures and their immediate family members and close associates (collectively known as politically exposed persons (PEP)).
- Non-resident alien (NRA)
- Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies and Private Investment Companies (PIC) and international business corporations (IBC)) located in higher-risk geographic locations.
- Deposit brokers, particularly foreign deposit brokers.
- Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages).
- Nongovernmental organizations and charities (foreign and domestic).
- Professional service providers (e.g., attorneys, accountants, doctors, or real estate brokers).

5.3.2 Geographic locations

- Countries subject to Office of Foreign Assets Control (OFAC) sanctions, including state sponsors of terrorism.
- Countries identified as supporting international terrorism under Section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State.
- Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to Section 311 of the USA PATRIOT Act.
- Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorism financing identified as non-cooperative by international entities such as the FATF.
- Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries which are identified as jurisdictions of primary concern.
- Offshore financial centres (OFC).
- Other countries identified by the bank as higher-risk because of their prior experiences or other factors (e.g., legal considerations, or allegations of official corruption).
- Domestic higher-risk geographic locations may include, but are not limited to, banking offices doing business within, or having clients located within, a U.S. government–designated higher-risk geographic location. Domestic higher-risk geographic locations include:
  - High Intensity Drug Trafficking Areas (HIDTA).
  - High Intensity Financial Crime Areas (HIFCA).

5.4 In case of any suspicions of terrorism financing, proliferation financing and sanctions violations, we will submit a suspicious transaction report to the MFIU. We will report any asset frozen or actions taken in compliance with the financial sanctions requirements by way of filing a suspicious activity report or suspicious transaction report to the MFIU.

6. CLIENT RISK ASSESSMENT

6.1 Doo Prime will perform client risk assessment using the risk-based approach. We assess the risk for each client taking into account specific products, services, clients, entities, number of transactions, volume of transactions, nature of client relationships, geographic locations, the purpose of the account or relationship, the level of assets involved, the size of transactions to be undertaken and the regularity or duration of the business relationship.

6.2 As Section 17(1) of the Act provides, Doo Prime shall:

(a) take appropriate steps to identify, assess and understand the money laundering and terrorism financing risks for clients, countries or geographic areas and products, services and transactions or delivery channels;

(b) consider all relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied.

6.3 The initial risk assessment of a particular client will help determine:

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

6.4 A risk-based approach[1]:

(a) identifies that risks related to money laundering and financing of terrorism differ across clients, countries and territories, products and services and delivery channels;

(b) allows licensees to understand the nature of the client based on its vulnerabilities in a way that matches its risk;

(c) while having minimum standards, allows licensees to apply adequate internal controls and system, commensurate with the nature of its activities and arrangements; and

(d) assist licensees in the allocation of resources for the prudential conduct of business.

6.5 Section 4.2 of the Handbook explained that a risk-based approach prescribes the following procedural steps to manage the ML and TF risks faced by Doo Prime:

(a) identifying the specific threats posed to Doo Prime by ML and TF and those areas of the firm's business with the greatest vulnerability;

(b) assessing the likelihood of those threats occurring and the potential impact of them on Doo Prime;

(c) mitigating the likelihood of occurrence of identified threats and the potential for damage to be caused, primarily through the application of appropriate and effective policies, procedures and controls;

(d) managing the residual risks arising from the threats and vulnerabilities that the financial institution has been unable to mitigate; and

(e) reviewing and monitoring those risks to identify whether there have been any changes in the threats posed to the financial institution which necessitate changes to its policies, procedures and controls.

6.6 Our steps to conduct the institutional money laundering/terrorism financing risk assessment include:

(a) documenting the risk assessment process which includes the identification and assessment of relevant risks supported by qualitative and quantitative analysis and information obtained from relevant internal and external sources;

(b) considering all the relevant risk factors before determining the level of overall risk, and the appropriate level and type of mitigation to be applied;

[1] Wolfsberg Statement, Guidance On A Risk-Based Approach For Managing Money Laundering Risks 2006

(c) obtaining the approval of senior management on the risk assessment results;

(d) having a process by which the risk assessment is kept up-to-date; and

(e) having appropriate mechanisms to provide the risk assessment to the MFSC when required to do so.

6.7 Section 4.4 Handbook's flowchart below shall be adopted by Doo Prime while performing our core client risk assessment duties:

Flowchart from page 39 of the Handbook.

6.8 Section 17(2) of the Act mentioned that the scope of the relevant risk factors includes:

(a) the nature, scale and complexity of the Doo Prime's activities;

(b) the products and services provided by the Doo Prime;

(c) the persons to whom and the manner in which the products and services are provided;

(d) the nature, scale, complexity and location of the client's activities;

(e) reliance on third parties for elements of the client due diligence process; and

(f) technological developments.

6.9 Section 4.3.3 and Section 4.3.4 of the Handbook further provides a guideline on risk assessment in relation to the following:

(a) the person to whom and the manner in which the products and services are provided

(i) Consider the threats posed by the types of clients. Some examples include high net worth individuals, those from or operating in a higher risk jurisdiction; and non-face-to-face business.

(ii) The type of product should be considered, the higher risk products or services are more likely to be those with high values and volumes; where unlimited third party funds can be freely received and those where funds can regularly be paid to third parties without CDD on the third parties being obtained.

(iii) The speed with which products and services can be delivered or transactions undertaken.

(b) The nature, scale, complexity and location of the client's activities

(i) Whether the client base has any involvement in those businesses which are likely to be most vulnerable to corruption, such as oil, construction or arms sales.

(ii) Consider jurisdictional factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect ML/TF in countries where it may have clients.

(iii) The countries, territories and geographic areas with which clients (and the beneficial owners of clients) have a relevant connection.

(c) Risk factors of which Doo Prime can consider when identifying the level of TF risk associated with a country or territory include:

(i) Is there information (for example, from law enforcement or credible and reliable open media sources) suggesting that a country or territory provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory?

(ii) Is the country or territory subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the UN or the EU?

6.10 Further to the above, we perform risk-profiling on the client considering the following factors:

(a) The nature and type of client;

(b) The commercial rationale for the relationship;

(c) The geographical location of the client's residence;

(d) The geographical location of the client's business interests and/or assets;

(e) The nature and value of the assets concerned in the relationship;

(f) The client's source of funds and where necessary the source of wealth;

(g) The role of any introducer and the introducer's regulated or professional status. We will routinely consider the risks that all relationships pose to us and the manner in which those risks can be limited through the effective use of documented CDD information.

	Nature, Scale, Complexity	*Products and Services*	*Clients*	*Geography*	*Delivery Channels*	*Total Risk Rating*
Client 1/ Bucket 1 e.g Fintech	Low	Medium	Medium	Low	Low	Low
Client 2/ Bucket 2	Medium	High	High	Medium	High	High
Client 3/ Bucket 3	Medium	Medium	High	Low	Low	Medium

Client to be risk-rated using the risk matrix above. Table from page 39 of the Handbook.

6.11 We shall review our client risk assessment at least once annually, taking into account:

(a) jurisdictions placed under increased monitoring by the FATF;

(b) emerging risks of trading instruments;

(c) emerging transactional risks;

(d) national risk assessment report by the MFSC.

7. SIMPLIFIED DUE DILIGENCE ("SDD")

7.1 If Doo Prime has determined that ML and TF risks are low, Doo Prime may adopt a simplified due diligence ("SDD") approach.

7.2 As provided by Section 11 of the Regulation and Chapter 7 of the Handbook, SDD may be performed when:

(a) lower risks have been identified and the simplified CDD measures shall be commensurate with the lower risk factors;

(b) there is a low level of risk, Doo Prime shall ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment carried out, whichever is most recently issued;

(c) provided that Doo Prime retains:

(i) the document that decision in a manner which explains the factors which it took into account (including retaining any relevant supporting documentation) and its reasons for adopting the measures in question; and

(ii) keep the relationship with the applicant (including the continued appropriateness of using the simplified measures) under review, and operate appropriate policies, procedures and controls for doing so.

7.3 Simplified CDD shall not apply where Doo Prime knows, suspects, or has reasonable grounds for knowing or suspecting that a client or an applicant for business is engaged in money laundering or terrorism financing or that the transaction is conducted by the client or applicant for business is being carried out on behalf of another person engaged in money laundering or terrorist financing.

7.4 In cases of SDD, we will

(a) identify the client and verify the client's identity;

(b) if a business relationship is to be established and its purpose and intended nature are not obvious, obtain information on the purpose and intended nature of the business relationship with us; and

(c) if a person purports to act on behalf of the client,

(i) identify the person and take reasonable measures to verify the person's identity; and

(ii) verify the person's authority to act on behalf of the client.

8. ENHANCED DUE DILIGENCE ("EDD")

8.1 If Doo Prime has determined that ML and TF risks are high, Doo Prime shall adopt an enhanced due diligence ("EDD") approach and enhanced ongoing monitoring. Approval from Doo Prime's senior management will be required before engaging or continuing a business relationship and/or transaction with high risks clients.

8.2 Section 12(1) of the Regulation mentioned that EDD shall be performed:

(a) where a higher risk of money laundering or terrorist financing has been identified;

(b) where through supervisory guidance a high risk of money laundering or terrorist financing has been identified;

(c) where a client or an applicant for business is from a high-risk third country;

(d) in relation to correspondent banking relationships, pursuant to Section 16 of the Regulation;

(e) subject to Section 15 of the Regulation, where the client or potential client is a PEP;

(f) where Doo Prime discovers that a client has provided false or stolen identification documentation or information and Doo Prime proposes to continue to deal with that client;

(g) in the event of any unusual or suspicious activity;

(h) where the client originates from FATF's non-cooperative jurisdictions (as updated from time to time).

8.3 High-risk situations for which EDD apply includes:

(a) client risk factor:

(i) business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic difference between us and the client);

(ii) body corporates or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose;

(iii) companies that have nominee shareholders or shares in bearer form;

(iv) cash-intensive business;

(v) the ownership structure of the body corporate or legal arrangement appears unusual or excessively complex given the nature of the body corporate's or legal arrangement's business; or

(vi) the client or the beneficial owner of the client is a PEP or foreign PEP.

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

(i) anonymous transactions (which may involve cash); or

(ii) frequent payments received from unknown or unassociated third parties.

(c) country risk factors. We strictly prohibit all dealings, bank transfers and transactions with clients from high risk countries, including but not limited to:

(i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML and CTF systems;

(ii) countries identified by the Financial Action Task Force;

(iii) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;

(iv) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or

(v) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operation.

8.4 Section 12(2) of the Regulation provides that EDD could be performed through:

(a) obtaining additional information on the client (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of the client and the beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship;

(c) obtaining information on the source of funds or source of wealth of the client;

(d) obtaining information on the reasons for intended or performed transactions;

(e) obtaining the approval of senior management to commence or continue the business relationship;

(f) conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;

(g) requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards.

8.5 Section 24 of the Regulation have guided on the following factors in determining whether a country is a high-risk country:

(a) strategic deficiencies in the anti-money laundering and combating the financing of terrorism legal and institutional framework, in particular in relation to:

(i) criminalisation of money laundering and terrorism financing

(ii) measures relating to CDD;

(iii) requirements relating to record-keeping;

(iv) requirements to report suspicious transactions;

(v) the availability of accurate and timely information of the beneficial ownership of body corporates and arrangements to competent authorities;

(b) the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing including appropriately effective, proportionate and dissuasive sanctions, as well as the third country's practice in cooperation and exchange of information with overseas competent authorities;

(c) the effectiveness of the third country's system for combating money laundering and terrorism financing in addressing money laundering or terrorist financing

8.6 We shall not accept any PEP clients or beneficial owners who are PEP.

8.7 We shall comply with Section 17H of the Act whereby EDD shall be conducted on jurisdictions placed under increased monitoring by the Financial Action Task Force.

8.8 Our EDD entails:

8.8.1 **Increasing the quantity of information obtained for client due diligence purposes**:

(a) About the client's or beneficial owner's identity, or ownership and control structure, to be satisfied that the risk associated with the relationship is well known. This may include obtaining and assessing information about the client's or beneficial owner's reputation and assessing any negative allegations against the client or beneficial owner. Examples include: information about family members and close business partners; information about the client's or beneficial owner's past and present business activities; and adverse media searches;

(b) About the intended nature of the business relationship, to ascertain whether the nature and purpose of the business relationship are legitimate and to help firms obtain a more complete client risk profile. It includes obtaining information on:

(i) the number, size and frequency of transactions that are likely to pass through the account to be able to spot deviations that may give rise to suspicions, requesting evidence where appropriate;

(ii) the reason the client is looking for a specific product or service, in particular where it is unclear why the client's needs cannot be met better in another way, or in a different jurisdiction;

(iii) the destination of funds;

(iv) the nature of the client's or beneficial owner's business to understand the likely nature of the business relationship better.

8.8.2 **Increasing the quality of information obtained for client due diligence purposes to confirm the client's or beneficial owner's identity including by:**

(a) Requiring the first payment to be carried out through an account verifiable in the client´s name with a bank;

(b) Establishing that the client's source of wealth and source of funds that are used in the business relationship are not the proceeds from criminal activity and that they are consistent with our knowledge of the client and the nature of the business relationship. The sources of funds or wealth may be verified, among others, by reference to income tax returns, copies of audited accounts, payslips, public deeds or independent and credible media reports;

(c) Increasing the frequency of reviews, to be satisfied that we continue to be able to manage the risk associated with the individual business relationship and to help identify any transactions that require further review, including by:

(i) Increasing the frequency of reviews of the business relationship, to ascertain whether the client's risk profile has changed and whether the risk remains manageable;

(ii) Obtaining the approval of the MLRO/nominated officer to commence or continue the business relationship to ensure senior management are aware of the risk we are exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;

(iii) Reviewing the business relationship on a more regular basis to ensure any changes to the client's risk profile are identified, assessed and, where necessary, acted upon;

(iv) Conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that may give rise to suspicion of money laundering or terrorism financing. This may include establishing the destination of funds or ascertaining the reason for certain transactions;

(d) The MLRO will need to provide approval, or refusal, to proceed with the client set up process before conducting any business with a client who has been through the enhanced due diligence process.

8.9 We will apply EDD measures on any situations, clients or transactions that are deemed to be high risk by us.

8.10 **Source of Funds and Source of Wealth**

8.10.1 Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets).

8.10.2 Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and us (e.g. the amounts being invested, deposited, or wired as part of the business relationship).

8.11 **How Source of Funds and Source of Wealth measures are incorporated into our EDD Process**

8.11.1 Source of wealth will usually indicate the size of wealth the client would be expected to have, and a picture of how the individual acquired such wealth. Although we may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources.

8.11.2 Source of funds information should not simply be limited to knowing from which the funds may have been transferred, but also the activity that generates the funds. The

information obtained should be substantive and establish a provenance or reason for the funds having been acquired.

8.11.3 Please refer to Schedule 3 on our source of wealth and origin of funds information and evidential guide.

8.12 It is Doo Prime's policy not to accept any funding from any third party, but in the event such exceptional circumstances occur, we shall conduct EDD to identify and verify its ultimate beneficial owner including body corporate, partnership, trust and other legal arrangements.

8.13 Where Doo Prime is unable to perform the EDD as required by the Regulation, we shall:

(a) not open the account, commence the business relationship or perform a transaction; or

(b) terminate the business relationship; and

(c) in relation to the client, file a suspicious transaction report under Section 14 of the Act;

9. ONGOING CDD AND TRANSACTION MONITORING

9.1 We shall conduct ongoing monitoring through ongoing CDD and transaction monitoring to ensure compliance with the AML and CTF Systems. We shall review the existing CDD records upon any trigger events and maintain adequate systems to monitor transactions in accordance with the risk-based approach adopted. The extent of monitoring shall be proportional to the ML and TF risk profile of a client.

9.2 Section 9.1 of the Handbook mentioned that there are two strands of effective ongoing monitoring:

(a) The first relates to the transactions and activity which occur on a day-to-day basis within a business relationship and which need to be monitored to ensure they remain consistent with Doo Prime's understanding of the client and the product or service it is providing to the client.

(b) The second relates to the client themselves and the requirement for Doo Prime to ensure that it continues to have a good understanding of its clients and their beneficial owners. This is achieved through maintaining relevant and appropriate CDD and applying appropriate ongoing screening.

9.3 We referred to Section 3(1)(e) of the Regulation while implementing our ongoing CDD and transaction monitoring, whereby it shall include:

(a) scrutiny of transactions undertaken throughout the course of the relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with his knowledge of the client and the business and risk profile of the client;

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

9.4 As for ongoing CDD and ongoing monitoring for high-risk clients, Section 9.3 of the Handbook has provided the following guideline:

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

(b) collecting information on a more regular basis;

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

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

(e) reviews being conducted by persons not directly involved in managing the relationship,

(f) ensuring that Doo Prime has adequate AML systems to provide the board, the MLRO and CO with the timely information needed to identify, analyse and effectively monitor high-risk relationships and accounts;

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

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

Ongoing Monitoring

9.5 We continuously monitor the activity of our clients by:

(a) reviewing from time-to-time documents, data and information relating to the client that have been obtained to comply with CDD requirements to ensure that they are up-to-date and relevant;

(b) conducting appropriate scrutiny of transactions carried out for the client to ensure that they are consistent with our knowledge of the client and the clients' business, risk profile and source of funds; and

(c) identifying transactions that are complex, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose and which may indicate ML and TF.

9.6 We shall ensure that there is consistency between the information we had on the clients and the nature of their transactions.

9.7 We shall perform CDD again on the clients in the event:

(a) we are aware that there is a change in the client's material information;

(b) there are inconsistencies between the information we had on the clients and the nature of their transactions

Transaction monitoring

9.8 We maintain adequate systems to monitor and review all transactions performed based on a risk-based approach, and we shall check and review whether the transactions are normal based on the following factors:

(a) the size and complexity of its business;

(b) the ML and TF risks arising from its business;

(c) the nature of its systems and controls;

(d) the monitoring procedures that already exist to satisfy other business needs; and

(e) the nature of the products and services provided (which includes the means of delivery or communication)

9.9 We regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including parameters and thresholds adopted. The parameters and thresholds adopted include the following factors:

(a) the nature and type of transactions (e.g. abnormal size or frequency);

(b) the nature of a series of transactions (e.g. structuring a single transaction into several cash deposits);

(c) the counterparties of transactions;

(d) the geographical origin/destination of payment or receipt;

(e) the client's normal account activity or turnover;

(f) the client's behaviour - sudden and/or significant changes in transaction activity by value, volume or nature, such as a change in beneficiary or destination;

(g) client's linked relationships – identifying common beneficiaries and remitters amongst apparently unconnected accounts or clients.

9.10 In the event any of the red-flag scenarios as described in Clause 3.2 occurs, we shall examine the background and purpose of those transactions by:

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

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

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

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

9.11 We will carry out retrospective reviews on the client to ensure the business being transacted is consistent with what was anticipated when the client was taken in. The frequency will depend on the risk classification of the client:

- high risk will be reviewed no less than weekly;
- medium risk will be reviewed no less than monthly;
- low risk will be reviewed on a real-time risk basis and may not need to undergo a retrospective check.

9.12 On an annual basis, all clients, who have been classed as high risk, will undergo a complete review. This will entail establishing the following:

- Re-confirmation of address
- Re-confirmation of corporate structure (if applicable)
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse news
- Complete review of transaction profile, including new products requested

10. REPORT

10.1 As Section 28(1) of the Regulation provides, where Doo Prime identifies any suspicious activity or has reasonable ground to suspect that a transaction is suspicious in the course of a business relationship or occasional transaction, we shall:

(a) consider obtaining EDD in accordance with Section 12 of the Regulation; and

(b) make an internal disclosure in accordance with the procedures established under Section 27 of the Regulation (sample of which attached in Schedule 1)

10.2 An internal disclosure shall be made in the event there is any:

(a) suspicious transaction;

(b) suspicious activity;

(c) transaction conducted by money laundering entities;

(d) transaction involving terrorist property;

(e) transaction with no legitimate purpose;

(f) our supervisory body or auditor has reasonable grounds to suspect that a transaction or an attempted transaction or information that it has in its possession involves proceeds of crime or is related to the financing of terrorism; or

(g) any transaction described in Clause 3.2.

10.3 If suspicious signals of money laundering are identified, the transaction should be suspended and should not proceed without the authorization of the MLRO.

10.4 As provided by Section 29 of the Regulation, where an internal disclosure has been made, the MLRO shall assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorism financing or proliferation financing.

10.5 After making appropriate investigations, the MLRO will report the matter to MFIU via a suspicious transaction report (as attached in Schedule 2) if we believe there are any potential serious ML and TF risks. We shall consider the following factors before submitting our report:

(a) the manner and form in which the transactions were conducted;

(b) the amount of the currency involved in each transaction;

(c) the aggregate amount of the currency involved in the transactions;

(d) whether a person conducts 2 or more transactions with the intention to avoid the amount threshold as described in Clause 4.3,

(e) the period over which the transactions occurred;

(f) the interval of time between the transactions;

(g) the locations at which the transactions were initiated or conducted;

(h) any explanation made by the person concerned as to the manner or form in which the transactions were conducted.

10.6 The MLRO shall forthwith make a report in accordance with Section 14 of the Act to the MFIU where he knows or has reason to believe that an internal disclosure may be suspicious.

10.7 The Guidance Note 4 for Suspicious Transaction Reports provided that suspicious transaction report for cash transaction reports, electronic transfer of money to or from Mauritius provided under Section 14A and Section 14B of the Act (threshold of 500,000 rupees) shall not be applicable to exempt transaction.

10.8 The suspicious transaction report shall include:

(a) the identification of the party or parties to the transaction;

(b) the amount of the transaction, the description of the nature of the transaction and all the circumstances giving rise to the suspicion;

(c) the business relationship of the suspect with Doo Prime or auditor;

(d) where the suspect is an insider, any information as to whether the suspect is still affiliated with Doo Prime or auditor;

(e) any voluntary statement as to the origin, source or destination of the proceeds;

(f) the impact of the suspicious activity on the financial soundness of Doo Prime or person; and

(g) the names of all the officers, employees or agents dealing with the transaction.

10.9 Doo Prime shall retain a register internal disclosures and external disclosures with:

(a) the date on which the report is made;

(b) the person who makes the report;

(c) information sufficient to identify the relevant papers.

10.10 All notifications made will be handled with strict confidentiality. However, please note that there may be circumstances in which we are required to reveal an individual's identity, for example where we are compelled to do so by law and therefore anonymity cannot be guaranteed.

10.11 We are aware that it is an offence for a person, knowing or suspecting that a disclosure has been made to the MFIU, if he/she discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following the disclosure (commonly referred to as "tipping-off"). The client's awareness of a possible suspicious activity report or suspicious transaction report or investigation could prejudice future efforts to investigate the suspected ML and TF operation. Therefore, if we form a suspicion that transactions related to ML and TF, we will take into account the risk of tipping-off when performing the CDD process. We shall ensure that our employees are aware of and sensitive to these issues when conducting CDD.

10.12 We shall not disclose any information to any other person:

(a) that we, or our supervisory body or auditor or a person has formed a suspicion in relation to a transaction or an attempted transaction, or activity or attempted activity; or

(b) that a report under Act is made to MFIU; or

(c) that information under the Act is given to MFIU; or

(d) any other information from which a person to whom the information is disclosed may reasonably be expected to infer any circumstances in paragraph (a)-(c).

10.13 Clause 10.12 does not apply to a disclosure made to:

(a) an officer, employee or agent of a Doo Prime who has made or is required to make a report or provide information under this Act for any purpose connected with the performance of that our duties; or

(b) a lawyer for the purpose of obtaining legal advice or representation in relation to the disclosure; or

(c) the supervisor of Doo Prime; or

(d) a law enforcement agency or any other person assisting the MFIU under this Act.

11. RECORD KEEPING

11.1 Section 17F of the Act imposed a statutory requirement on Doo Prime to maintain all books and records concerning our clients and transactions, which shall include:

(a) all records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of clients and beneficial owners, and records and the results of any analysis/assessment undertaken in accordance with the Act, all of which shall be maintained for a period of not less than 7 years after the business relationship has ended;

(b) records on transactions, both domestic and international, that are sufficient to permit reconstruction of each transaction for both account holders and non-account holders, which shall be maintained for a period of 7 years after the completion of the transaction; and

(c) copies of all suspicious transaction reports made pursuant to section 14 or other reports made to FIU in accordance with the Act, including any accompanying documentation, which shall be maintained for a period of at least 7 years from the date the report was made.

11.2 The record keeping requirements in respect of each transaction are as follows:

(a) We will keep the original or a copy of the documents, and a record of the data and information obtained in connection with the transaction, including but not limited to the following:

(i) nature of the transaction;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted;

(iv) the name, address and occupation, business or principal activity, as the case requires, of each person:
(aa) conducting the transaction; and
(ab) for whom, or for whose ultimate benefit, the transaction is being conducted, if we have reasonable grounds to believe that the person is undertaking the transaction on behalf of any other person;

(v) the type and identifying number of any accounts/services with us that were involved in the transaction;

(vi) if the transaction involves a negotiable instrument other than currency:
(aa) the drawer of the instrument;
(ab) the name of the institution on which it is drawn;
(ac) the name of the payee (if any);
(ad) the amount and date of the instrument; and
(ae) the number (if any) of the instrument and details of any endorsements appearing on the instrument;

(vii) the name and address of Doo Prime, and of each officer, employee or agent of Doo Prime who prepared the relevant record or a part of the record;

(viii) any other information relating to that transaction.

(b) Records required to be kept under subparagraph (a) must be kept for at least six years beginning on the date on which the transaction is completed, regardless of whether the business relationship ends during the period.

12. AML AND CTF AUDIT FUNCTION

12.1 The MLRO and our compliance department conduct an internal audit on our AML and CTF policy annually to ensure our AML and CTF policy is updated. We are aware of our statutory liability to comply with the Act and we shall update and review our AML and CTF policy at least once annually.

12.2 We will regularly identify and assess ML and TF risks that may arise in relation to:

(a) the nature and level of money laundering and terrorism financing risk that we may reasonably expect to face in the course of its business;

(b) the nature, size and complexity of our business;

(c) development of new products and new business practices, including new delivery mechanisms; and

(d) use of new or developing technologies for both new and pre-existing products.

12.3 We shall also consider the emerging ML and TF risks that may arise in relation to the technological advancements and new business practices, including but not limited to:

(a) digital information storage including cloud computing;

(b) digital or electronic documentation storage;

(c) electronic verification of documentation;

(d) data and transaction screening systems; or

(e) the use of virtual or digital currencies.

13. MONEY LAUNDERING REPORTING OFFICER AND COMPLIANCE OFFICER

13.1 Our MLRO and CO shall be responsible for the implementation and ongoing compliance of internal programmes, controls and procedures with the requirements of the Act and the Regulation.

13.2 Section 4.3.1 of the Handbook also provides that the CO appointed must be:

(a) be a natural person;

(b) be of at least senior management level as defined under the Regulation;

(c) be an approved officer under Section 24 of the Financial Services Act; and

(d) have the appropriate qualification knowledge, skill and experience to fulfil a compliance role within Doo Prime.

13.3 Section 22(3) of the Regulation provides that the functions of the CO shall include:

(a) ensuring continued compliance with the requirements of the Act and regulations subject to the ongoing oversight of the board of Doo Prime and senior management;

(b) undertaking day-to-day oversight of the program for combating money laundering and terrorism financing;

(c) regular reporting, including reporting of non-compliance, to the board and senior management;

(d) contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combating money laundering and terrorism financing.

13.4 Doo Prime shall ensure that the CO:

(a) has timely and unrestricted access to the records of the financial institution;

(b) has sufficient resources to perform his or her duties;

(c) has the full co-operation of the financial institution staff;

(d) is fully aware of his or her obligations and those of the financial institution; and

(e) reports directly to, and has regular contact with, the board of directors so as to enable the board of directors to satisfy itself that all statutory obligations and provisions in Act, Regulation, the Code, and this Handbook are being met and that the financial institution is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF.

13.5 Section 26(4) of the Regulation states that MLRO shall:

(a) be sufficiently senior in the organisation of Doo Prime or have sufficient experience and authority; and

(b) have a right of direct access to the board of directors of Doo Prime and have sufficient time and resources to effectively discharge his functions.

13.6 As provided by Section 3.4.2 of the Handbook:

(a) the MLRO appointed by Doo Prime shall be:

(i) a natural person;

(ii) a senior management level executive;

(iii) approved under Section 24 of the Financial Services Act.

(b) The role of the MLRO shall be as follows:

(i) undertaking a review of all internal disclosures in the light of all available relevant information and determining whether or not such internal disclosures have substance and require an external disclosure to be made to the FIU;

(ii) maintaining all related records;

(iii) giving guidance on how to avoid tipping off the client if any disclosure is made;

(iv) liaising with the FIU and if required the FSC and participating in any other third party enquiries in relation to money laundering or terrorist financing prevention, detection, investigation or compliance;

(v) providing reports and other information to senior management;

(vi) is the main point of contact with the FIU in the handling of disclosures;

(vii) has unrestricted access to the CDD information of the Doo Prime's clients, including the beneficial owners thereof;

(viii) has sufficient resources to perform his or her duties;

(ix) is available on a day-to-day basis;

(x) reports directly to, and has regular contact with, the Board or equivalent of the Doo Prime; and

(xi) implementing and monitoring the day-to-day operation of the AML/CFT policy and procedures.

(xii) reporting to the board of directors or a committee of the board of directors on any material breaches of the internal AML/CFT policy and procedures and of the AML/CFT laws, codes and standards of good practice.

(xiii) preparing reports annually and such other periodic reports as he/she deems necessary to the board of directors or a committee of the board of directors dealing with:
(aa) the adequacy/shortcomings of internal controls and other AML/CFT procedures implemented,
(bb) recommendations to remedy the deficiencies identified above,
(cc) the number of internal reports made by staff the number of reports made to the MFIU

(xiv) is fully aware of both his or her personal obligations and those of the Doo Prime under Act and Regulation, the Code, and the Handbook.

13.7 Doo Prime shall ensure that the MLRO:

(a) is the main point of contact with the FIU in the handling of disclosures;

(b) has unrestricted access to the CDD information of the financial institution's clients, including the beneficial owners thereof;

(c) has sufficient resources to perform his or her duties;

(d) is available on a day-to-day basis;

(e) reports directly to, and has regular contact with, the Board or equivalent of the financial institution; and

(f) is fully aware of both his or her personal obligations and those of the financial institution under the Act, the Regulation, the Code, and this Handbook.

13.8 Any internal report on reasonable suspicion of ML and TF risks shall be directed to the appointed MLRO. A deputy MLRO shall be appointed as well to manage the duties of the MLRO in his absence.

14. TRAINING PROGRAMME

14.1 All relevant staff in Doo Prime will be provided with relevant policy and knowledge training provided in this AML and CTF Policy. In addition, all relevant staff in Doo Prime will be briefed about their job descriptions and will be trained on their responsibilities concerning money laundering and financing of terrorism transactions. They will be guided on how to identify and deal with transactions that possibly involve money laundering and financing of terrorism.

14.2 As Section 22(1)(c) of Regulation provides, the ongoing training provided by us shall cover:

(a) the Act, the Regulation, any AML/CFT Code issued by the MFSC and this Handbook;

(b) the implications of non-compliance by employees to requirements of the Act, the Regulation, any AML/CFT Code issued by the MFSC and this Handbook; and

(c) our policies, procedures and controls for the purposes of foreseeing, preventing and detecting ML and TF.

14.3 In accordance with Section 12.7 of the Handbook, we shall ensure that the ongoing training provided to directors, officers and employees also covers, to a minimum:

(a) the requirements for the internal and external disclosing of suspicion;

(b) the criminal and regulatory sanctions in place, both in respect of the liability of Doo Prime and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of Doo Prime;

(c) the identity and responsibilities of the MLRO, CO and Deputy MLRO;

(d) dealing with business relationships or occasional transactions subject to an internal disclosure, including managing the risk of tipping off and handling questions from clients;

(e) those aspects of our business deemed to pose the greatest ML and TF risks, together with the principal vulnerabilities of the products and services offered by the financial institution, including any new products, services or delivery channels and any technological developments;

(f) new developments in ML and TF, including information on current techniques, methods, trends and typologies;

(g) our policies, procedures and controls surrounding risk and risk awareness, particularly in relation to the application of CDD measures and the management of high risk and existing business relationships;

(h) the identification and examination of unusual transactions or activity outside of that expected for a client;

(i) the nature of terrorism funding and terrorist activity so that employees are alert to transactions or activity that might be terrorist-related;

(j) the vulnerabilities of Doo Prime to financial misuse by PEPs, including the effective identification of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs; and

(k) UN, US and other sanctions and our controls to identify and handle natural persons, body corporates and other entities subject to sanction.

14.4 Focused training for appropriate staff or groups of staff will enable Doo Prime and senior management to implement their AML and CTF systems effectively. The following areas of training may be appropriate for certain groups of staff:

(a) All new staff (irrespective of seniority)
(i) an introduction to the background of ML and TF and the importance of AML and CTF to us; and

(ii) the need and obligation to identify and report suspicious transactions to the MLRO, and the offence of "tipping-off".

(b) Front-line staff (i.e. staff dealing with clients directly)
(i) the importance of their roles in the estate agency company's AML and CTF strategy being the first point of contact with potential money launderers and persons involved in TF;
(ii) the estate agency company's policies and procedures in relation to CDD and record-keeping requirements relevant to their job responsibilities;
(iii) guidance or tips for identifying unusual activities in different circumstances that may give rise to suspicion; and
(iv) the relevant policies and procedures for reporting unusual activities, including the line of reporting and the circumstances where extra vigilance might be required.

(c) Back-office staff
(i) appropriate training on client verification and the relevant processing procedures; and
(ii) ways to recognise unusual activities including abnormal settlements, payments or delivery instructions.

(d) Managerial staff (including internal audit staff)
(i) higher-level training covering all aspects of Mauritius' AML and CTF regime;
(ii) specific training in the AML and CTF requirements applicable to us; and
(iii) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as the reporting of suspicious transactions to the MFSC.

(e) CO and MLRO
(i) specific training in relation to the CO's and MLRO's responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the MFSC; and
(ii) training to keep abreast of AML and CTF requirements/developments generally;
(iii) receive reports of suspicious activity from firm personnel;
(iv) coordinate required AML reviews/meetings with appropriate staff.

14.5 We will monitor the effectiveness of the training. This may be achieved by:

(a) testing staff's understanding of our policies and procedures to combat ML and TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions;

(b) monitoring the compliance of staff with our AML and CTF systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken; and

(c) monitoring attendance and following up with staff who miss such training without reasonable cause.

14.6 We conduct AML training, workshops and assessments on all related staff members at least once annually.

14.7 We shall observe and record our employees who have been adequately trained, when they are trained or last trained, and thereafter provide additional, necessary and adequate training to them.

14.8 We will record all AML and CFT training provided to the employees. These records will include:

(a) the dates on which the training was provided;

(b) the nature of the training, including its content and mode of delivery; and

(c) the names of the employees who received the training.

14.9 Doo Prime shall also conduct appropriate screening on all employees. As adopted by Section 12.4 of the Handbook, this shall include:

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

(b) obtaining and confirming appropriate references;

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

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

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

15. FOREIGN BRANCHES AND SUBSIDIARIES

15.1 Doo Prime shall ensure that its foreign branches and subsidiaries:

(a) apply measures to combat money laundering and terrorism financing consistent with the home country requirements, where the minimum requirements of the host country are less strict than those of the home country, to the extent that host country laws and regulations permit; and

(b) where the host country does not permit the proper implementation of anti-money laundering and combating the financing of terrorism measures, apply appropriate additional measures to manage the money laundering and terrorism financing risks, and inform their home supervisors.

16. MISCELLANEOUS

16.1 This AML and CTF Policy and anything related to it shall be governed by the laws of the Republic of Mauritius.

16.2 The official language of this AML and CTF policy shall be English. Doo Prime may provide this AML and CTF policy in other languages for information purposes only and in the event of any inconsistency or discrepancy between the English version of this AML and CTF policy and any other language version, the English version shall prevail.

16.3 The Client acknowledges that Doo Prime reserves the right to amend or update this AML and CTF policy at any time without prior notice to the Client. The amendments to the AML and CTF policy shall become effective immediately and shall be legally binding on the Client upon publishing of the AML and CTF policy on Doo Prime's website. The Client undertakes to regularly review this AML and CTF policy on the Doo Prime's website.

(the rest of this page is intentionally left blank)

Schedule 1
(Sample Internal Suspicious Transaction Report)

Appendix I

Sample Internal Disclosure Form to MLRO

1. Reporting Employee

Name :_____

Telephone No :_____

2. Client

Client Name :_____

Address :_____

Contact Name :_____

Contact Telephone No :_____

Date Client Relationship

Commenced _____

Client reference :_____

3. Information/Suspicion

Suspected Information/

Transaction : _____

Reasons for Suspicion : _____

_____

_____

_____

Please attach copies of any relevant documentation to this report.

Reporter's Signature : _____ Date: _____

It is an offence to advise the customer/client or anyone else of your suspicion and report.

This report will be treated in the strictest confidence.

MLRO Use:

Date received:……Time received: …….. Ref:…….

FIU advised: Yes/No…..Date: …….. Ref:……

Schedule 2
(Sample Suspicious Transaction Report)

FINANCIAL
INTELLIGENCE UNIT
REPUBLIC OF MAURITIUS

SUSPICIOUS TRANSACTION REPORT

SECTION 14 & 15
FINANCIAL INTELLIGENCE AND ANTI-MONEY LAUNDERING ACT, 2002 (FIAMLA)

SEND COMPLETED FORM BY REGISTERED POST OR HAND DELIVERY TO:

FINANCIAL INTELLIGENCE UNIT
7TH FLOOR, EBÈNE HEIGHTS
34, EBÈNE CYBERCITY EBÈNE
MAURITIUS

OR SEND COMPLETED FORM BY FAX: (230) 466 2431

*KINDLY FILL IN **CAPITAL**. PLEASE TYPE OR PRINT. ALWAYS COMPLETE ENTIRE REPORT. PLEASE SEE GUIDANCE NOTE 3 FOR MORE DETAILS ABOUT STR BEFORE COMPLETING THE FORM.*

PART I REPORT DETAILS

1.1	**REPORT TYPE:***			
1.2	**ENTITY REFERENCE NO.:**			
1.3	**FIU REFERENCE NO.:**			
1.4	**SUBMISSION DATE:***		**SIGNATURE OF MLRO/RP:***	

PART II INFORMATION ON REPORTING ENTITY/PERSON

2.1.A REPORTING ENTITY DETAILS

BUSINESS TYPE:*

PLEASE PROVIDE DETAILS FOR 'OTHERS':

NAME OF REPORTING ENTITY:*

ACRONYM:*

SECTOR:

2.1.B PARTICULARS OF THE MONEY LAUNDERING REPORTING OFFICER/CONTACT PERSON

FIRST NAME:*

LAST NAME:*

DATE OF BIRTH: NIC:

OCCUPATION:

2.2 ADDRESS*

STREET ADDRESS:

CITY:

COUNTRY:

2.3 PHONE*

TELEPHONE NO: FAX NO:

2.4 SUPERVISION

SUPERVISED BY:

2.5 TOTAL NUMBER OF PAGES ATTACHED TO THIS STR

PART III INFORMATION ON SUSPICION

3.1 INDICATORS

IN/TYP/OFF 1:

IN/TYP/OFF 2:

IN/TYP/OFF 3:

IN/TYP/OFF 4:

IN/TYP/OFF 5:

IN/TYP/OFF 6:

PLEASE PROVIDE DETAILS FOR 'OTHERS':

3.2 DESCRIPTION OF SUSPICIOUS ACTIVITY *

THIS SECTION OF THIS REPORT IS CRITICAL.
DESCRIBE CLEARLY AND COMPLETELY THE FACTS OR UNUSUAL CIRCUMSTANCES THAT LED TO THE SUSPICION OF MONEY LAUNDERING OR TERRORIST FINANCING. THE CARE WITH WHICH THIS SECTION IS WRITTEN MAY MAKE THE DIFFERENCE IN WHETHER OR NOT THE DESCRIBED CONDUCT AND ITS POSSIBLE CRIMINAL NATURE ARE CLEARLY UNDERSTOOD.

IF THIS FIELD DOES NOT PROVIDE SUFFICIENT SPACE, PLEASE REPORT ONLY A SHORT SUMMARY, THEN INCLUDE THE ENTIRE TEXT (NOT A CONTINUATION OF WHAT APPEARS IN THE "REASON" FIELD) IN A DOCUMENT ATTACHED TO THE REPORT.

3.3 MATERIAL IMPACT *

HAS THERE BEEN A MATERIAL IMPACT ON THE FINANCIAL SOUNDNESS OF THE REPORTING ENTITY?
IF YES, EXPLAIN HOW.

PART IV DESCRIPTION OF ACTION TAKEN*

WHAT ACTION WAS OR WILL BE TAKEN BY YOU AS A RESULT OF THE SUSPICIOUS TRANSACTION(S).
STATE ALSO WHETHER THE SUSPECT MADE ANY VOLUNTARY STATEMENT AS TO THE ORIGIN OR SOURCE OF THE PROCEEDS. KINDLY ENCLOSE COPY OF THE STATEMENT, IF ANY.

IF THIS FIELD DOES NOT PROVIDE SUFFICIENT SPACE, PLEASE REPORT ONLY A SHORT SUMMARY , THEN INCLUDE THE ENTIRE TEXT (NOT A CONTINUATION OF WHAT APPEARS IN THE "ACTION TAKEN" FIELD) IN A DOCUMENT ATTACHED TO THE REPORT.

PART V TRANSACTION DETAILS

5.1 **TRANSACTION NO:***

5.2 **TRANSACTION DATE:***

5.3 **DATE OF POSTING IF DIFFERENT FROM DATE OF TRANSACTION:**

5.4 **TRANSACTION MODE: ***

5.5 **DATE TRANSACTION DETECTED:***

5.6 **CURRENCY TYPE:**

5.7 **FOREIGN AMOUNT:**

5.8 **EXCHANGE RATE:**

5.9 **LOCAL AMOUNT:***

5.10 **DESCRIPTION:***

NOTE:

PLEASE COMPLETE SECTION 5.11, IF THE TRANSACTION INVOLVES ITEMS OF ANY KIND E.G GOODS AND SERVICES.

IF THE FIELD FOR DESCRIPTION DOES NOT PROVIDE SUFFICIENT SPACE, PLEASE REPORT ONLY A SHORT SUMMARY, THEN INCLUDE THE ENTIRE TEXT (NOT A CONTINUATION OF WHAT APPEARS IN THE "DESCRIPTION" FIELD) IN A DOCUMENT ATTACHED TO THE REPORT.

5.11 **GOODS AND SERVICES**

IF TRANSACTION INCLUDES ANY GOODS OR SERVICE PLEASE PROVIDE THE FOLLOWING DETAILS:

ITEM TYPE:*

COMMENTS:

PREVIOUSLY REGISTERED TO:

PRESENTLY REGISTERED TO:

(PLEASE PROVIDE DETAILS ON EACH PARTY INVOLVED IN PART VII OR PART VIII)

ESTIMATE VALUE:

STATUS CODE:

DISPOSED VALUE:

5.12 **LOCATION OF OFFICE CONDUCTING THE TRANSACTION**

STREET ADDRESS:

CITY:

5.13 **NAME OF OFFICERS DEALING WITH THE SUSPICIOUS TRANSACTION***

NAME OF PERSONS	REPORTING ENTITY	CAPACITY IN WHICH DEALING WITH TRANSACTION

5.14 **TRANSACTION TYPE***

IF TRANSACTION TYPE IS BI-PARTY, THEN SELECT APPROPRIATE PARTY TYPE:

FROM TYPE: ☐ **MY CLIENT** ☐ **NOT MY CLIENT**

PARTY TYPE: ☐ **ACCOUNT** ☐ **ENTITY** ☐ **PERSON**

TO TYPE: ☐ **MY CLIENT** ☐ **NOT MY CLIENT**

PARTY TYPE: ☐ **ACCOUNT** ☐ **ENTITY** ☐ **PERSON**

IF TRANSACTION TYPE IS MULTI-PARTY, THEN SELECT APPROPRIATE NUMBER OF INVOLVED PARTIES:

		PARTY TYPE		
		ACCOUNT	ENTITY	PERSON
PARTY IS	MY CLIENT			
	NOT MY CLIENT			

NOTE:

IN SECTION 5.10, CLEARLY INDICATE THE PARTIES THAT ARE LINKED TO THE TRANSACTION BEING REPORTED. FULL DESCRIPTION OF PARTIES MUST BE PROVIDED IN PARTS VI, VII AND VIII WHERE RELEVANT.

IN CASE YOU ARE REPORTING SEVERAL TRANSACTIONS, PLEASE REPEAT INFORMATION IN PART V FOR EACH TRANSACTION.

PART VI ACCOUNT DETAILS

6.1 TRANSACTION NO: PARTY IS:

6.2 ROLE:

6.3 FUNDS TYPE: 6.4 COUNTRY:

6.5 ACCOUNT NUMBER:

6.6 NAME OF ACCOUNT HOLDER:

6.7 INSTITUTION NAME:

6.8 A/C TYPE: 6.9 A/C CURRENCY:

IF YOU SELECTED 'OTHER', PLEASE PROVIDE DETAILS IN THE 'COMMENTS' BOX BELOW

6.10 A/C STATUS:

6.11 OPENED ON: 6.12 CLOSED ON:

6.13 BALANCE IN ACCOUNT AT DATE OF REPORTING: DATE OF BALANCE:

COMMENTS:

PLEASE PROVIDE DETAILS FOR 'OTHER' AND ANY COMMENTS DEEMED NECESSARY

NOTE:

IN CASE THERE ARE SEVERAL ACCOUNTS INVOLVED IN THE TRANSACTION, PLEASE REPEAT INFORMATION IN PART VI FOR EACH ACCOUNT BEING REPORTED.
DETAILS ON ENTITY/INDIVIDUAL HOLDING THE ACCOUNT MUST BE PROVIDED IN PART VII/PART VIII.
DETAILS ON SIGNATORIES TO THE ACCOUNT MUST BE PROVIDED IN PART VIII IF THE ABOVE ACCOUNT IS 'MY CLIENT'
IF PARTY INVOLVED IS 'MY CLIENT' IN PART VI, THEN THE FOLLOWING FIELDS ARE MANDATORY: 6.1, 6.2, 6.3, 6.4,6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 6.11, 6.13
IF PARTY INVOLVED IS 'NOT MY CLIENT' IN PART VI, THEN THE FOLLOWING FIELDS ARE MANDATORY: 6.1, 6.2, 6.3, 6.4, 6.5, 6.6

PART VII ENTITY DETAILS

7.1 TRANSACTION NO: PARTY IS:

7.2 ROLE:

7.3 FUNDS TYPE: 7.4 COUNTRY:

7.5 NAME:

7.6 INCORPORATION LEGAL FORM:

IF YOU SELECTED 'OTHER', PLEASE PROVIDE DETAILS IN THE 'COMMENTS' BOX BELOW

7.7 BUSINESS SECTOR: 7.8 DATE OF INCORP.:

7.9 INCORP. NUMBER: 7.10 COUNTRY OF INCORP.:

7.11 STREET ADDRESS:

7.12 CITY: 7.13 COUNTRY: 7.14 TELEPHONE NO:

COMMENTS:

PLEASE PROVIDE DETAILS FOR 'OTHER' OR ANY OTHER COMMENTS DEEMED NECESSARY

NOTE:

IN CASE THERE ARE SEVERAL ENTITIES INVOLVED IN THE TRANSACTION, PLEASE REPEAT INFORMATION IN PART VII FOR EACH ENTITY BEING REPORTED.
DETAILS ON PERSONS LINKED TO THE ENTITY MUST BE PROVIDED IN PART VIII IF ABOVE ENTITY IS 'MY CLIENT'.
IF PARTY INVOLVED IS 'MY CLIENT' IN PART VII, THEN THE FOLLOWING FIELDS ARE MANDATORY: 7.1, 7.2,7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 7.11, 7.12, 7.13
IF PARTY INVOLVED IS 'NOT MY CLIENT' IN PART VII, THEN THE FOLLOWING FIELDS ARE MANDATORY: 7.1, 7.2, 7.3, 7.4, 7.5

PART VIII PERSON DETAILS

8.1 TRANSACTION NO: PARTY IS:

8.2 ROLE:

8.3 FUNDS TYPE: 8.4 COUNTRY:

8.5 GENDER:

8.6 FIRST NAME:

8.7 LAST NAME:

8.8 STREET ADDRESS:

8.9 CITY: 8.10 COUNTRY:

8.11 TELEPHONE NO: 8.12 DATE OF BIRTH:

8.13 NATIONALITY: 8.14 RESIDENCE:

8.15 IDENTIFIER: NUMBER:

8.16 IF INSIDER RELATIONSHIP, PLEASE SPECIFY IF

DATE OF SUSPENSION/TERMINATION/RESIGNATION:

8.17 IF PERSON IS SIGNATORY TO ACCOUNT IN PART VI, PLEASE COMPLETE THE FOLLOWING SECTION:

☐ IS A PRIMARY SIGNATORY ROLE:

8.18 IF PERSON IS LINKED TO ENTITY IN PART VII, PLEASE COMPLETE THE FOLLOWING SECTION:

ROLE:

IF YOU SELECTED 'OTHER', PLEASE PROVIDE DETAILS IN THE 'COMMENTS' BOX BELOW

COMMENTS:

PLEASE PROVIDE DETAILS FOR 'OTHER' OR ANY OTHER COMMENTS DEEMED NECESSARY

NOTE:

IN CASE THERE ARE SEVERAL PERSONS INVOLVED IN THE TRANSACTION AND/OR SEVERAL SIGNATORIES TO THE ACCOUNT MENTIONED IN PART VI AND/OR SEVERAL PERSONS LINKED TO THE ENTITY MENTIONED IN PART VII, REPEAT INFORMATION IN PART VIII FOR EACH PERSON BEING REPORTED.
IF PARTY INVOLVED IS 'MY CLIENT' IN PART VIII, THEN THE FOLLOWING FIELDS ARE MANDATORY: 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.12, 8.13, 8.14, 8.15
IF PARTY INVOLVED IS 'NOT MY CLIENT' IN PART VIII, THEN THE FOLLOWING FIELDS ARE MANDATORY: 8.1, 8.2, 8.3, 8.4, 8.6, 8.7

Schedule 3
(Source of wealth and origin of funds information and evidential guide)

Description of source of Wealth	Details required	Documentary Evidence required (original or fully certified copy)
1. **Income-savings from salary (basic and/or bonus)-** if self- employed or company share owner refer to 4 below	All of the following: • Salary per annum • Employer's name and address • Nature of Business	One of the following: • Payslip (or bonus payment) from the last three months • Letter from employer confirming salary on letter-headed paper • Bank statement showing clearly showing receipt of most recent regular salary payments from named employer
2. Sale of investment /liquidation of investment portfolio	All of the following: • Description of shares/units/deposits • Name of seller • How long held • Sale amount • Date funds received	One of the following: • Investment/savings certificates, contract notes, or surrender statements • Bank statements clearly showing receipt of funds and investment company name • Signed letter detailing funds from a regulated accountant on letter –headed paper.
3. Sale of Property	All of the following: • Sold property address • Date of Sale • Total sale amount	One of the following: • Letter form a licenced solicitor or regulated accountant stating property address, date of sale, proceeds received, and name of purchaser • Copy of Sale contract
4. Company Sale	All of the following: • Name and nature of the company • Date of Sale • Total sale amount • Client's share	• Letter detailing company sale signed by a licensed solicitor or regulated accountant on letter headed paper. • Copy of contract of sale, plus bank statement showing proceeds • Copies of media coverage (if applicable) supporting evidence
5. Inheritance	All of the following: • Name of deceased • Date of death • Relationship to client • Date received • Total amount • Solicitors details	One of the following: • Grant of probate (with a copy of the will) which must include the value of the estate • Copy of will • Letter from lawyer or trustee
6. Divorce settlement	Date and total amount received Name of divorced partner	One of the following: • Copy of the court order • Letter detailing divorce settlement signed by a licensed solicitor on letter headed paper
7. Company profits	All of the following: • Name and address of the company • Nature of company • Amount of annual profit	One of the following: • Copy of the latest audited company accounts • Confirmation of the nature of the business activity and turnover detailed in a letter from a regulated accountant
8. Retirement income	All of the following: • Retirement date • Details of previous occupation/profession	One of the following: • Pension statement • Letter from a regulated accountant

Description of source of Wealth	Details required	Documentary Evidence required (original or fully certified copy)
	• Name and address of the employer • Details of pension income source	• Bank statement showing receipt of the latest pension income and name of provider • Savings account statement
9. Fixed Deposits/Savings	All of the following: • Name and institution where savings account are held • Date the account was established • Details of how the savings were acquired	All of the following: • Savings statement • Evidence of account start (letter from the account provider) • Additional evidential information can be requested in relation to the origin of the savings held.
10. Dividend payments	All of the following: • Date of receipt of dividend • Total amount received • Name of company paying dividend • Length of time the shares have been held in the company	One of the following: • Dividend contract note • Bank statement clearly showing receipt of funds and name of the company paying the dividend If dividend is payable from the client's own company, one of the following; • Letter detailing dividend details signed by a regulated accountant on letter headed paper • Set of company accounts showing the dividend details
11. Gift	• Details of date and amount of gift • Details of person making gift – ID and occupation details for PEP/Sanctions screening • Reason for gift and the nature of the relationship to the individual making the gift	• Letter from donor confirming details of gift • If PEP Documented evidence of donor's source of wealth as laid out in this table
12. Loan	• Name of loan provider • Date and amount of loan	• Copy of the Loan Agreement and details of any security or, • Copy of loan statements
13. Lottery/Gambling Win	• Name of source • Details of Windfall	• Evidence from the lottery company • Cheque • Winnings' receipt
14. Compensation Pay-out	• Details of events leading to claim	• Letter/court order from compensating body or • Solicitor's letter
15. Life Insurance/general insurance pay-out	• Amount Received • Policy Provider • Policy Number/reference • Date of pay-out	• Pay-out statement • Letter from insurance provider confirming pay-out