JAINAM
Prosperity with Security

JAINAM IFSC MAVENS PRIVATE LIMITED

POLICIES AND PROCEDURE FOR PREVENTION OF MONEY LAUNDERING

Version Details

Version	Version-8
Author of the Policy:	Mr. Omprakash Singh
Approved by:	Vidhi Parikh, Director
Approved by the Board on:	09/07/2024

Policy made as per the IFSCA (Anti Money Laundering, Counter Terrorist-Financing and Know Your Customer) Guidelines, 2022 (IFSCA/2022-23/GN/GL001) (hereinafter referred to as 'KYC AML Guideline' or 'Guideline')

JAINAM IFSC MAVENS PRIVATE LIMITED
CIN : U65990GJ2017PTC097096

Unit - 235, 2nd Floor, Signature Tower, Block - 1, Road 1C, Zone - 1,
GIFT SEZ, GIFT City, Gandhinagar - 382355, Gujarat, India.
Corporate E-mail ID : corp@jainam.in Website : www.jainam.in

1. OBJECTIVE

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

Jainam IFSC Mavens Private Limited (herein after referred to as 'company') aims to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

The objectives of the policy is to-

1. To undertake Customer Due Diligence (CDD).
2. To undertake Risk Assessment of the Cutomers
3. To identify money laundering or terrorist financing activities
4. To monitor and report suspicious transactions
5. To take adequate measures to follow the 'KYC AML Guideline' in spirit.

2. IMPORTANT DEFINITONS:

2.1 "Act" and "Rules" means the Prevention of Money-laundering Act, 2002 and the Prevention of Money laundering (Maintenance of Records) Rules, 2005, respectively.

2.2 "Authority" or "IFSCA" means the International Financial Services Centres Authority established under sub-section (1) of section 4 of International Financial Services Centres Authority Act, 2019.

2.3 "Business Facilitator" means a person authorised by the Company, to verify the information/officially valid documents provided by the customer for opening account with it.

2.4 "Central KYC Records Registry" means an entity defined under rule 2 (1) (ac) of the Rules, which is authorised to receive, store, safeguard and retrieve the KYC records of a customer in digital form.

2.5 "Certified Copy" means comparing the original officially valid document provided by the customer with the copy thereof and recording the same as 'true copy' by the authorised officer of the Company.

Provided that in case of non-resident individuals including Non-Resident Indians (NRIs), the certification may be carried out by:

(i) Authorised official of a bank located in a Financial Action Task Force (FATF) compliant jurisdiction with whom the individual has banking relationship;

(ii) Notary Public (outside India);

JAINAM IFSC MAVENS PVT. LTD.

(iii) Court Magistrate (outside India);

(iv) Judge (outside India);

(v) Certified public or professional accountant (outside India);

(vi) Lawyer (outside India);

(vii) The Embassy/Consulate General of the country of which the non-resident individual is a citizen; or

(viii) Any other authority as may be specified by the Authority

2.6 "Customer" or "Client" for the purpose of these Guidelines shall mean a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person engaged in the transaction or activity, is acting.

2.7 Designated Director" means a person designated by the Company to ensure overall compliance with the obligations imposed under Chapter IV of the Act, the Rules and these Guidelines.

2.8 "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Company as per the provisions contained in the Act

2.9 "Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid Digital Signature, including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016 or its equivalent in other jurisdictions, as may be recognised by the Authority.

2.10 "FATCA" means Foreign Account Tax Compliance Act, 2010 of the United States of America (USA) which, inter-alia, requires reporting financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

2.11 "Financial Group" means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.

2.12 "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961.

2.13 "Governing Body" means:

a) In relation to a company- the board of directors;

JAINAM IFSC MAVENS PVT. LTD.

b) In relation to a partnership firm- the partner(s);

c) In relation to a limited liability partnership- the partners including any designated partner (s);

d) In relation to a trust- the managing trustee (s); and

e) In relation to an unincorporated association or a body of individuals - committees of management or anybody who controls and manages the affairs of such unincorporated association or a body of individuals (consisting of more than one person);

2.14 "Non-profit organization" means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);

2.15 "Principal Officer" means an officer designated by the Company as such, who shall be responsible for furnishing information as required under rule 8 of the Rules.

2.16 "Officially Valid Document" means the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card issued by the Election Commission of India or letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government in consultation with the Regulator;

Provided that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document.

Provided further that, where simplified measures are applied for verifying the identity of the customers, the following documents shall also be deemed to be 'officially valid document': -

(a) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;

(b) letter issued by a gazetted officer, with a duly attested photograph of the person.

Provided also that,

where the simplified measures are applied for verifying the limited purpose of proof of address of the customer, where a prospective customer is unable to

produce any proof of address, the following document shall also be deemed to be Officially Valid Document:

(i) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

(ii) property, Municipal tax receipt, city council tax receipt, or such other equivalent document;

(iii) Post Office savings bank account statement or statement of a bank account including of a foreign bank;

(iv) pension or family Pension Payment Orders (PPOs) issued to retired employees by Government, Departments or Public Sector Undertakings, if they contain the address;

(v) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation; and

Provided also that in case the Officially Valid Document presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address;

(vi) Provided also that where the client submits his proof of possession of Aadhaar number as an Officially Valid Document, he may submit it in such form as are issued by the Unique Identification Authority of India.

Document shall also be deemed to be an Officially Valid Document even if there is a change in the name subsequent to its issuance, provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name

2.17 "Politically Exposed Person" means the individuals who are or have been entrusted with prominent public functions by any country, which shall include Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials or International Organisation Politically Exposed Person.

not intended to cover middle ranking or more junior individuals in the definition

2.18 "Shell financial institution" means a bank or financial institution incorporated, formed or established in a country or jurisdiction where the bank or financial institution has no physical presence, and which is unaffiliated with a financial group that is subject to effective supervision.

JAINAM IFSC MAVENS PVT. LTD.

"Physical presence means meaningful mind in the form of senior management located within an IFSC. The existence simply of a local agent or low-level staff does not constitute physical presence."

2.19 "Suspicious Transaction" means a "Transaction" as defined below, including an attempted transaction, which to a person acting in good faith-

(a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

(b) appears to be made in circumstances of unusual or unjustified complexity; or

(c) appears to have no economic rationale or bona-fide purpose; or

(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

2.20 "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

(a) opening of an account;

(b) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether by payment order or other instruments or by electronic or other non-physical means;

(c) the use of a safety deposit box or any other form of safe deposit;

(d) entering into any fiduciary relationship;

(e) any payment made or received, in whole or in part, for any contractual or other legal obligation; and

(f) establishing or creating a legal person or legal arrangement.

2.21 "Video based Customer Identification Process" or "V-CIP" means an alternate method of customer identification with facial recognition and customer due diligence, by an authorised official of the company, by undertaking seamless, secure, live, informed &consent based audio-visual interaction with the customer to obtain identification information required for Customer Due Diligence purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process.

3. PRINCIPAL OFFICER / DESIGNATED DIRECTOR DESIGNATION AND DUTIES

The company has designated Mr. Dishant Parikh as a Principal Officer for its Anti-Money Laundering Program, with full responsibility for the company AML program. He is qualified by experience, knowledge and training.

The duties of the Principal Officer shall include:

JAINAM IFSC MAVENS PVT. LTD.

i. carrying out, or overseeing the carrying out of, ongoing monitoring of business relations for compliance with the KYC AML Guidelines;
ii. promoting compliance of these Guidelines and taking overall charge of all AML/CFT matters within the organisation;
iii. informing employees, officers and representatives promptly of regulatory changes;
iv. ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;
v. reporting or overseeing the reporting of suspicious transactions;
vi. advising and training employees, officers and representatives on developing and implementing internal policies, procedures and controls on AML/CFT;
vii. reporting to Senior Management on the outcome of reviews of the Company's compliance with these Guidelines & risk assessment procedures; and
viii. reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection & compliance reviews to the Company's Board of Directors.

(i) The Principal Officer will also ensure that proper AML records are kept.

(ii) When warranted, the Principal Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU – IND)

The company shall provide the FIU with contact information of the Principal Officer, including name, title, mailing address, e-mail address and telephone number. The company will promptly notify FIU of any change to this information

The business interests of the Company shall not interfere with the effective discharge of the responsibilities of the Principal Officer.

In addition to the existing requirement of designation of a Principal Officer, we have Mrs. Vidhi Parikh as a Designated Director. The Designated Director is entrusted with the obligation as stated in The Prevention of Money-Laundering Act, 2002 and Prevention of Money laundering (Maintenance of Records) Rules, 2005

4. RISK BASED APPROACH:

Company shall adopt Risk-Based Approach (RBA) to identify and assess the Money Laundering (ML) and Terrorist Financing (TF) risk, depending upon exposure to or involvement with certain types of clients, countries or geographic areas, products, services, transactions, or delivery channels, etc..

The Company shall carry out Risk Assessment of its Clients and shall use the result to classify the ML/TF risks as low, medium, and high.

JAINAM IFSC MAVENS PVT. LTD.

The Company shall review its risk assessment at least once every two years or when a material trigger event occurs, whichever is earlier. The Outcome shall also be placed before the board of the Company.

5. BUSINESS RISK ASSESSMENT:

The Company Shall take suitable steps to identify the exposure to ML/TF risks. The Company shall take into account type of Customers, geographical areas from where the client belongs, complexity and volume of transaction, products and services offered, technology used, and such other factors to assess the risk and shall take mitigation measures accordingly.

6. CUSTOMER RISK ASSESSMENT:

The customer risk assessment shall be performed shall be completed prior to undertaking Customer Due Diligence. The Company shall undertake risk-based assessment of every Customer. The outcome of the Customer risk assessment shall be used to assign the risk rating of the customer as high, medium or low, proportionate to the ML/TF risks.

While Undertaking Customer Risk Assessment, the Company shall Consider the

(i) identify the customer and Beneficial Owner, if any;
(ii) obtain information on the purpose and intended nature of the business relationship;
(iii) obtain information on, and take into consideration, the nature of the customer's business;
(iv) take into consideration the customer's country of origin, residence, nationality, place of incorporation or place of business;

6.1 Factors that may indicate high ML/TF risk

When assessing if there is a high risk of ML/TF in a particular situation, the Company shall take into account, among other things:

(a) Customer risk

(i) Whether the customers are from high-risk businesses / activities / sectors

(ii)Whether the ownership structure of the legal person or arrangement appears unusual or excessively complex;

(iii)Whether the business relations are conducted under unusual circumstances (e.g., significant unexplained geographic distance between the Company and the customer);

(iv)Whether the companies have nominee shareholders or shares in bearer form;

(v)Whether the legal persons or legal arrangements are personal asset holding vehicles; and,

(vi) Whether the corporate structure of the customer is unusual or excessively complex given the nature of the business.

(b) Country or Geographic risk

(i) Whether the countries or jurisdictions the Company is exposed to, either through its own activities or the activities of its customers (including the Company's network of correspondent account relationships) have relatively high levels of corruption, organized crime or inadequate AML/CFT measures, as identified by the FATF;

(ii) Whether the countries or jurisdictions are identified by any credible body as having significant levels of corruption, terrorism financing or other criminal activities;

(iii) Whether the countries or jurisdictions are identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems;

(iv) Whether the countries or jurisdictions do not have effective systems to counter ML/TF; or not implementing the AML/CFT measures that are consistent with FATF Recommendations;

(v) Whether the countries or jurisdictions are subject to sanctions, embargos or similar measures issued by International Organisations or India;

(vi) Whether the countries or jurisdictions are funding or supporting the terrorism; and,

(vii) Whether countries or jurisdictions have organizations operating within their territory that have been designated by India, other countries or International Organizations as terrorist organizations.

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

(i) Whether the service involves private banking;

(ii)Whether the product, service or transaction is one that might favour anonymity;

(iii)Whether the situation involves non-face-to-face business relationships or transactions, without adequate safeguards;

(iv) Whether the payments received are from unknown or unassociated third parties;

(v) Whether the services offered are in relation to nominee directors, nominee shareholders or the formation of companies in another country; and

(vi) Whether there are anonymous transactions or any transaction which involves frequent payments, received from unknown or unassociated third parties.

When assessing the risk factors, the Company shall examine the overall risk while keeping in mind that the presence of one or more risk factors alone may not always indicate a high risk of ML/TF in a particular situation.

6.2 Factors that may indicate low ML/TF risks

When assessing if there is a low risk of ML/TF in a particular situation, a Company shall take into account, among other things:

(a) customer risk factors, including whether the customer is:

(i) a Government entity;

(ii) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.

(iii) regulated financial institution incorporated or established outside India that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

(iv) a subsidiary of a regulated financial institution referred to in point (iii) above, if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML standards as that of its Parent entity;

(v) a public body or a publicly owned enterprise;

(vi) a resident established or registered in a geographical area of low risk;

(b) product, service, transaction or delivery channel risk factors, including whether the product or service is:

(i) a product where the ML/TF risks are adequately managed by other factors such as transaction limits or transparency of ownership; and

(ii) financial products or services that provide appropriately defined and limited services to certain types of customers.

When assessing the risk factors, the Company shall examine the overall risk while keeping in mind that the presence of one or more risk factors alone may not always indicate a low risk of ML/TF in a particular situation.

6.3 Business relationship shall not be established in the following cases:

The Company shall not establish the business relationship with the customer, which is a legal person or legal arrangement, and : -

(a) The ownership or control arrangements of the customer prevent the Company from identifying one or more of the customer's Beneficial Owners;

(b) There are anonymous accounts, accounts in fictitious names, or a nominee account which is held in the name of one person, but is controlled by or held for the benefit of another person whose identity has not been disclosed to the company; or

(c) a Shell Financial Institution

JAINAM IFSC MAVENS PVT. LTD.

7. CUSTOMER DUE DILIGENCE:

7.1 Undertaking Customer DueDiligence

Company after assigning risk rating for each Customer proportionate to their AML/CFT risks, shall undertake the Customer Due Diligence. Company shall undertake the Customer Due Diligence of a customer: -

(i) at the time of establishing business relationship, and,

(ii) after establishing a business relationship, as an ongoing Customer Due Diligence

7.1.1 Company shall also undertake Customer Due Diligence if, at any time:

(i) in relation to an existing customer, it doubts the veracity or adequacy of documents, data or information obtained for the purposes of Customer Due Diligence;

(ii) it suspects ML/TF; or,

(iii) there is a change in risk-rating of the customer, or it is otherwise warranted by a material change in circumstances of the customer.

7.1.2 The Company may establish a business relationship with a customer before undertaking Customer Due Diligence, subject to fulfilling the following conditions:

(i) the deferral of completion of the verification of the customer or Beneficial Owner is obtained; and

(ii) there is low risk of occurrence of ML/TF activity and any such risks identified can be effectively managed by the Company;

This may include case of Non-face-to-face business and transactions required to perform without delay depending upon market conditions, and in such circumstances, the execution of the transaction may be required before verification of identity is completed

The relevant verification shall be completed as soon as reasonably practicable and, in any event, it shall not exceed 30 business days after the establishment of business relationship.

7.1.3 Where the Company is not able to comply with the 30-day requirement, the Company shall, prior to the end of the 30-day period:

(i) document the reason for its non-compliance;

(ii) complete the verification as soon as possible; and

(iii) record the non-compliance event for reporting to the Board of Directors.

7.1.4 The Company shall suspend business relationship with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the

extent that is possible) if such verification remains uncompleted for 30 days after the establishment of business relationship.

7.1.5 The Company shall terminate business relations with the customer if such verification remains uncompleted for 120 days after the establishment of business relationship.

7.2 Customer Due Diligence Requirements

In undertaking Customer Due Diligence, the following measures shall be undertaken by the Company: -

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, in such a manner that the Company is satisfied that it knows who the beneficial owner is. Similarly, for legal persons and arrangements, the CDD shall include taking reasonable steps to understand the nature of the customer's business, its ownership and control structure.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of business relationship to ensure that the transactions that are being conducted, are consistent with the Company's knowledge of the customer, customer's business and risk profile, including, where necessary, the source of funds.

7.2.1 Identification of Customer

(a) If a customer is a natural person, Company shall obtain at least the following information:

(i) Full name, including any aliases;

(ii) Unique Identification Number (such as an Identity card number, passport number, etc.);

(iii) Date of birth;

(iv) Nationality;

(v) Legal domicile;

(vi) Current residential address; (other than a post office box address);

(vii) Contact details such as personal, office or work telephone numbers.

(b) If a customer is a legal person or legal arrangement, Company shall obtain at least the following information:

(i) The full name and any trading name;

(ii) Unique identification Number (i.e., Tax identification number or equivalent where this exists, incorporation number or business registration number);

(iii) Registered or business address, and if different, its principal place of business;

(iv) Date of establishment, incorporation or registration;

(v) Place of incorporation or registration.

(c) Further, in cases where the customer is a legal person or legal arrangement, the Company shall, also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement.

In addition to this, the Company shall also identify and screen the related parties or connected parties of such customer and shall take necessary steps to remain apprised of any changes to connected parties. For identification of the connected parties, the Company shall obtain at least the following information of each related or connected party:

(i) full name, including any aliases; and

(ii) Unique Identification Number (such as an Identity card number, passport number, etc.).

Identification of connected parties or related parties may be undertaken using publicly available sources or databases such as company registries, annual reports. Additionally, it could be based on substantiated information provided by the customers.

7.2.2 Verification of Identity of Customer

(a) The Company shall verify the identity of the customer using reliable, independent source data, documents or information. Where the customer is a legal person or legal arrangement, the Company shall verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent source data, documents or information.

(b) When relying on documents, the Company may include government-issued identity cards or current valid passport, reports from independent company registries, published or audited annual reports and other reliable sources of information. The rigor of the verification process shall be commensurate with the customer's risk profile.

(c) In verifying the identity of a customer, the Company may obtain the following documents:

In case of Natural Persons –

(i) any of the OVD defined above in para 2.15 that contains photograph of the customer, name, unique identification number, date of birth and nationality; and

(ii) residential address based on OVD or recent utility bill, bank statement or such other documents specified under the definition of OVD.

In cases where a customer is a foreign national, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national would also be considered as OVD.

In case where the customer is an Indian national, OVD shall include the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card, etc. as prescribed. For the purpose of customer verification, equivalent e-documents of OVDs shall also be treated as original document by the Company.

In cases where other than simplified measures are applied, the customer shall submit updated OVD or their equivalent e-documents thereof with current address within a period of three months of submitting the documents mentioned under para 2.15 above.

For those customers to whom simplified measures are not applied, the bank account or Post Office savings bank account statement or statement of foreign bank shall not be accepted as deemed OVD for the limited purpose of proof of address

In case of Legal persons or Legal Arrangements-

(i) Name, legal form, proof of existence and constitution: - the verification for the same can be obtained from certificate of incorporation, certificate of good standing, partnership deed/agreement, trust deed, constitutional document, certificate of registration or any other document from a reliable independent source; and

(ii) Powers that regulate and bind the legal person or legal arrangement: - This can be ascertained from the constitutional documents, as well as the names of the relevant persons having a Senior Management position in the legal person or legal arrangement and board resolution or similar document authorising the opening of an account and appointment of its authorised signatories.

List of information and documents required to be obtained for onboarding customers are specified in Annexure-I. Further, for onboarding Indian Nationals, a Company may follow the procedure as specified under Annexure-II.

The Company shall examine the original identification documents and retain a copy of the same.

However, if a customer is unable to produce, or it might not be possible for customer to submit original documents for verification (e.g., in situations where Company has no physical contact with the customer or the on boarding of customer is done through non-face to face mode) i.e. in case of non- resident individuals including Non-residents, the Company shall obtain a copy of the document that is certified to be a 'true copy' as specified in para 2.5.

Documents obtained for performing CDD, shall be clear and legible.

JAINAM IFSC MAVENS PVT. LTD.

Except for high-risk customers, the following mode of verifications are also considered as sufficient to satisfy the requirements of Verification of the identity of the Client

(i) downloading publicly available information from an official source (such as a regulator's or other official government website);

(ii) CDD information and research obtained from a reputable company or information obtained from reliable and independent public information found on the internet and commercial databases, provided that the commercial database is recognized for such purpose by the home regulator, if any, of the database.

Where the customer is rated as high-risk, the identification information shall be independently verified, using both public and non-public sources.

7.2.3 Identification and Verification of Identity of Natural Person appointed to act on behalf of Customer

Where a customer is a natural person or legal person, and appoints one or more natural persons to act on its behalf for establishing business relations with the Company, the Company shall identify each natural person who acts or is appointed to act on behalf of such natural or legal person by obtaining Information as specified in para 7.2.1.

Further, the Company shall verify the identity of each such natural persons using reliable, independent source data, documents or information. Furthermore, the Company shall verify the authorisation of each natural person appointed to act on behalf of the customer by obtaining at least the following:

(i) The appropriate documentary evidence authorising the appointment of such natural person by the customer to act on his or its behalf which may include power of attorney, resolution passed by Governing Body or authorisation granted to transact on its behalf.

(ii) Where there is a long list of natural persons appointed to act on behalf of the customer (e.g., a list comprising more than 10 authorized signatories), the Company shall verify those natural persons who will deal directly with the Company.

Where the client purports to act on behalf of juridicial person or individual or trust, the Company shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

In case of a trust, the Company shall ensure to obtain from the trustees disclosure in their status at the time of commencement of an account based relationship or when carrying out transactions.

7.2.4 Identification and Verification of Identity of Beneficial Owners

Where there is one or more Beneficial Owners in relation to a customer, the Company shall identify the Beneficial Owners and take reasonable measures to verify their identities using the relevant information or data obtained from reliable, independent sources.

For the identification and verification of Identity of Beneficial Owner, the Company shall consider the following in relation to:

(a) Customers that are legal persons

(i) The identity of the natural person(s) (whether acting alone or together) exercising control over the legal person through ownership or who ultimately owns the legal person;

(ii) To the extent that there is doubt as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural person(s) (if any) who ultimately control the legal person or have ultimate effective control over the legal person.

(b) Customers that are legal arrangements

(i) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

(ii) In all other types of legal arrangements, the Company shall identify persons in equivalent or similar positions.

At the time of opening an account or executing any transaction with it, the company will verify and maintain the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status.

7.2.4.1 Parameters to Identify and Verify the Identity of Beneficial Owners/ Meaning of Beneficial Owner: -

(a) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

For the purpose of the above -

(i) "Controlling ownership interest" means ownership of or entitlement to more than ten per cent of the shares or capital or profits of the company;

(ii) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

(b) Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than ten per cent. of capital or profits of the partnership or who exercises control through other means;

For this purpose "Control" shall include the right to control the management or policy decision

(c) Where the customer is an unincorporated association or body of individuals ('body of individuals' includes societies), the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of the unincorporated association or body of individuals.

(d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

Where no natural person is identified above, the beneficial owner is the relevant natural person who holds the position of senior managing official. However, in such cases, the Company shall keep a record of all the actions it has taken to identify the Beneficial Owners of such legal persons or legal arrangement. If the ownership or control arrangements of a customer are of such a nature that the Company is prevented from identifying the Beneficial Owners, the Company shall not establish a business relationship

Where the client or the owner of the controlling interest is an entity listed on the stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities and such other entities who have been excluded from the requirements regarding identifying and verifying beneficial owners of a customer under the Act and Rules, then unless the Company has doubts about the veracity of the CDD information, or suspects that customer may be connected with ML/TF, the company shall not be required to identify and verify the identity of any shareholder or beneficial owner of a customer.

Currently the notified jurisdictions by Central Government are as follows: -

(i) United States of America

(ii) Japan

(iii) South Korea

(iv) United Kingdom excluding British Overseas Territories

(v) France

(vi) Germany

(vii) Canada

JANAM IFSC MAVENS PVT. LTD.

In cases where a customer is subscribing or dealing with depository receipts or equity shares issued or listed in jurisdictions notified by the Central Government, of a company incorporated in India, and it is acting on behalf of a beneficial owner who is resident of such jurisdiction, the determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction.

7.2.5 Information on the Purpose and Intended Nature of Business Relations

The Company shall, while establishing business relationship, understand and as appropriate, obtain information from the customer as to the purpose and intended nature of business relations.

7.2.6 Accounts of Politically Exposed Persons (PEP)

The Company shall, in addition to undertaking CDD measures, undertake at least the following additional measures where a customer or any beneficial owner of the customer or Beneficial Owner of a beneficiary is determined to be a PEP:

(i) Collect by appropriate and reasonable means, adequate information including information about the source of wealth and income of family members, any beneficial owner and close relatives;

(ii) Verify the identity before accepting the PEP as a customer;

(iii) Obtain approval from its Senior Management before opening an account of a PEP;

(iv) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, obtain the Senior Management's approval to continue the business relationship;

(v) Increase the degree and nature of ongoing monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.

The Company may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for:-

(i) PEP, their family members and close associates;

(ii) International Organisation PEP, their family members, and close associates; or

(iii) PEP who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down, their family members and close associates, except in cases where their business relations or transactions with the Company present a high risk for ML/TF.

JANAM IFSC MAVENS PVT. LTD.

Company shall also ascertain the source of wealth of the customers by appropriate and reasonable means.

Source of wealth generally refers to the origin of the customer's and beneficial owner's entire body of wealth(i.e., total assets). This relates to how the customer and beneficial owner have acquired the wealth which is distinct from identifying the assets that they own. Source of wealth information shall give an indication about the size of wealth the customer and beneficial owner would be expected to have. Company may obtain general information from the customer, commercial databases or other open sources.

Verification of source of wealth shall be carried out by various measures including obtaining independent corroborating evidence such as share certificates, publicly available registers of ownership, information and documents such as evidence of title, copies of trust deeds, bank or brokerage account statements, probate documents, audited accounts and financial statements, salary details, tax returns, news items from a reputable source and other similar evidence. For instance:

(i) for a legal person, the company shall obtain its financial or annual reports published on its website or news articles and press releases that reflect its financial situation or the profitability of its business; and

(ii) for a natural person, the company shall obtain documentary evidence such as , if a natural person attributes the source of his wealth to inheritance, he may be asked to provide a copy of the relevant will or grant of probate. In other cases, bank statements, salary statements or tax returns shall be obtained.

Company shall not automatically treat all individuals who are PEPs, as a high-risk customer. Each PEP shall be assessed on risk sensitive basis and the Company thereafter shall determine what risk category is appropriate for such PEPs.

7.3 Enhanced Due Diligence

(a) Where the risks of ML/TF are high, Company shall conduct enhanced CDD measures, consistent with the risks identified. The enhanced CDD measures are as follows: -

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

(ii) Obtaining information and taking additional steps to examine the ownership and financial position, including source of wealth and source of funds of the customer or, if applicable, of the Beneficial Owner.

(iii) Obtaining information and taking additional steps to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.

JAINAM IFSC MAVENS PVT. LTD.

(iv) Obtaining the approval of Senior Management to commence or continue the business relationship.

(v) 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; and,

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

Where applicable, first payment made by a customer in order to open an account with the company shall be carried out through a bank account in the customer's name with:

(i) a Bank;

(ii) a regulated financial institution whose entire operations are subject to regulation and supervision, including AML/CFT regulation and supervision, in a jurisdiction where its regulations on AML/CFT are equivalent to the standards set out in the FATF recommendations; or

(iii) a subsidiary of a regulated financial institution referred to in (ii), if the law that applies to the Parent entity ensures that the subsidiary also observes the same AML/CFT standards as its Parent entity.

Company shall specifically apply enhanced due diligence measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries called for by the FATF

Circumstances where a customer presents or may present a high probability of ML/TF risk may include,but are not limited to the following:

(i) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures; and

(ii) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the Company for itself or notified to Company generally by the Authority or other relevant domestic authorities in India or other foreign regulatory authorities.

For establishing an account-based relationship with high-risk customers, the approval shall be given by Senior Management or committee of senior managers or an individual member who has been authorised by the Senior Management in this behalf time to time.

In cases where a customer uses complex legal structures and/or trusts, private investment vehicle, the Company shall satisfy itself that it is used for a legitimate and genuine purpose.

The Company shall take reasonable measures to examine the source of wealth and source of funds. That is, where the funds for a particular service or transaction will

come from (e.g., a specific bank account held with a specific financial institution) and whether that funding is consistent with the source of wealth of the customer or, if applicable, of the Beneficial Owner.

Examples of appropriate and reasonable means of establishing source of funds are such as proof of dividend payments connected to a shareholding, bank statements, salary payments or bonus certificates, sale proceeds, loan documentation and proof of a transaction which gave rise to the payment into the account.

(8) A customer should be able to demonstrate and document how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a transaction.

7.4 Simplified Customer Due Diligence

(a) Where the risks of ML/TF are low, The Company may conduct simplified CDD measures, corresponding with the low risk factors. Examples of possible measures are:

(i) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship.

(ii) Reducing the frequency of customer identification updates.

(iii) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

(b) Simplified CDD (SCDD) measures shall not be conducted where there is a suspicion of ML/TF.

(c) The Company shall perform ongoing monitoring as specified under para 7.5 below.

(d) Identification or verification of Beneficial Owners for retail investment funds which are widely held and for investment funds where the investor invests via pension contributions is not required.

7.5 Ongoing customer due diligence:

Company shall undertake the ongoing customer due diligence, for which, the following shall be considered: -

(i) Monitoring its business relations with the customer on an ongoing basis.

(ii) The Company during the course of business relations with a customer, shall observe the conduct of the customer's account and scrutinize transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with Company's knowledge of the customer, its business and risk profile and where appropriate, may seek the source of wealth and source of funds.

(iii) The Company shall pay particular attention to any complex, unusually large or unusual patterns of transactions undertaken throughout the course of business relations, that have no apparent or visible economic or legitimate purpose.

(iv) The Company shall make further enquiries into the background and purpose of the transaction specified in point (iii) above and document its findings so that this information is made available to the relevant authorities, should the need arise.

(v) A Company shall periodically review each customer to ensure that the risk rating assigned, is commensurate with the ML/TF risks posed by the customer.

(vi) Where there are indications that the risks associated with an existing business relation with the customer may have increased, the Company shall request additional information and conduct a review of the customer's risk profile in order to determine if additional measures are necessary.

(vii) The Company shall ensure that the Customer Due Diligence data, documents and information obtained in respect of customers, natural persons appointed to act on behalf of the customers, related parties of the customers and beneficial owners of the customers, are relevant and kept up-to-date by undertaking the review of adequacy of the existing Customer Due Diligence data, documents and information, particularly for customers with high-risk rating.

The rigor and extent of monitoring of a customer shall be determined based on the customer's ML/TF risk profile

Further, the following shall be followed by the Company: -

(i) for customers who are rated as high risk, the Company shall obtain updated CDD information (including updated copies of the customer's Officially Valid Documents if these have expired), as part of its periodic CDD review, or upon the occurrence of a trigger event as deemed necessary by the Company, whichever is earlier; and

(ii) for all other risk categories of customers, a Company shall obtain updated CDD information upon the occurrence of a trigger event.

A Company shall undertake a review under points (v) and (vii) both periodically and at other appropriate times, including when:
(i) the Company changes its CDD documentation requirements;
(ii) an unusual transaction with the customer is expected to take place;
(iii) there is a material change in the business relationship with the customer; or
(iv) there is a material change in the nature or ownership of the customer.

7.6 Ongoing sanctions screening

A Company shall review its customers, their business and transactions against United Nations Security Council sanctions lists and also against any other relevant sanctions list.

7.7 Accounts of Non-profit organization:

The Company shall register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and a reporting entity has ended or the account has been closed, whichever is later

7.8 Failure of Company to conduct or complete customer due diligence:

In cases where a Company is unable to conduct or complete the requisite Customer Due Diligence for a customer, the Company shall: -

(i) not open an account or otherwise provide a service;
(ii) not carry out a transaction with or for the customer;
(iii) not otherwise establish a business relationship;
(iv) terminate or suspend any existing business relationship with the customer;
(v) return any monies or assets received from the customer; and,
(vi) consider whether the failure to conduct or complete Customer Due Diligence necessitates the filing of a Suspicious Transaction Report (STR).

A Company is not bound to comply with the points (i) to (v) above, if it amounts to "tipping off" of the customer, or FIU-IND directs the Company to act otherwise.

7.9 Periodic Updation:

The periodicity of updation from the date of opening of the account / last CDD updation for different categories of customers is as follows: -

(i) Annually- for high-risk customers;
(ii) once in three years- for medium risk customer; and,
(iii) once in every five years- for low-risk customers.

(a) Individual Customers:

(i) No change in CDD information:

In case of no change in the CDD information, a self-declaration from the customer in this regard may be obtained through mobile number registered with the Company or through digital channels (such as online banking / internet banking, e-mail or mobile application of the Company).

(ii) Change in address:

(a) In case of a change only in the address details of the customer, a self-declaration of the new address may be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels (such as online banking internet banking, e-mail or mobile application

of the Company). The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.
(b) Further, a Company shall obtain a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address declared by the customer at the time of periodic updation.

(b) Customers other than Natural Persons:
(i) No change in CDD information:
In case of no change in the CDD information of a customer, which is a non-natural person, a self -declaration through email id registered with the company , digital channels (such as online banking / internet banking, mobile application of company), a letter duly signed by authorised official and requisite resolutions in this regard shall be obtained from the customer.
(ii) Change in CDD information:
In case of change in CDD information, Company shall undertake fresh CDD process as is applicable for on boarding a new customer which is a non-natural person.

Where the client has submitted any documents for the purpose of change, it shall submit to the reporting entity any update of such documents, for the purpose of updating the records within 30 days of such updation.

(c) Additional measures:
In addition to the above, company shall ensure that:
(i) The KYC documents of the customer as per the current CDD standards are available with it. This is applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the company has expired at the time of periodic updation of CDD, company shall undertake fresh CDD process equivalent to that applicable for on boarding a new customer.
(ii) In case of Indian National, the customer's PAN details, shall be verified from the database of the issuing authority at the time of periodic updation of CDD.
(iii) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, the Company shall ensure that the information / documents obtained from the customers at the time of periodic updation of CDD are promptly updated in its records / database and an intimation, mentioning the date of updation of CDD details, is provided to the customer.
(iv)A Company shall adopt a risk-based approach with respect to periodic updation of CDD.

8. THIRD PARTY RELIANCE

"Third Party" shall mean-
(a) A financial institution which is subject to and supervised by a financial regulator; or
(b) In relation to a Company, its branches, subsidiaries, parent entity, the branches and subsidiaries of the parent entity, and other related corporations;
AND

JAINAM IFSC MAVENS PVT. LTD.

(c) Has an existing client relationship with a person whose data would be used for CDD and customer verification by a Company.

Company may rely on a Third Party to perform CDD measures, subject to the following conditions:

(a) The Company shall obtain records or information of the client due diligence carried out by the third party, immediately;

(b) The copies of identification data and other relevant documentation relating to the client due diligence will be made available by the third party upon request, without delay;

(c) The third party, is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements mentioned under recommendation 10 and 11 of the FATF recommendations and also are inline with the requirements and obligations under the Act;

Where the Company relies on a third party that is part of the same Financial Group, the above condition is not applicable. Company can rely on member of the Financial Group subject to the condition that such member meets the following requirements: -

(i) the Financial Group applies and implements a group-wide programmes on customer due diligence and record keeping, which meets the standards set out in the FATF Recommendations; and

(ii) the implementation of Customer Due Diligence and record keeping at the group level are supervised by a financial services regulator or other competent authority in a country.

Company shall consider following factors including, among other things for assessing the reliance on the third party:

(i)mutual evaluations, assessment reports or follow-up reports published by FATF and other International Organisations;

(ii) contextual factors such as political stability or the level of corruption in the jurisdiction;

(iii) evidence of recent criticism of the jurisdiction, including in:

(i) FATF advisory notices;

(ii) public assessments of the jurisdiction's AML regime by organisations referred to in (i); or

(iii) reports by other relevant non-government organisations or specialist commercial organisations.

(iv) The third party shall not based in a country or jurisdiction assessed as high risk;

(v) The Company shall not rely on a third party to conduct ongoing monitoring of business relations with customers;

(vi) The Company shall not rely on a third party specifically precluded by the Authority from relying upon;

(vii) The Company shall document the basis for its satisfaction that the requirements under point (c) above, have been met;

(viii) The reliance on Third Party shall also be subject to the conditions that are specified in rule 9 (2) of the PMLA Rules and shall be in accordance with the regulations and circulars/guidelines issued by Authority from time to time; and,

(ix) The Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

9. AUDIT:

The Company shall maintain an audit function that is adequately resourced and independent, that is able to regularly assess the effectiveness of the Company's internal policies, procedures and controls, in compliance with regulatory requirements and the Guidelines.

Company's AML/CFT framework is subjected to periodic audits. Such audits shall be performed not just on individual business functions but also on an Entity-wide basis or Financial group wide basis.

10.TRAINING AND AWARENESS

The Company shall: -
(a) provide AML/CFT training to all relevant employees, periodically;
(b) ensure that its AML/CFT training enables its employees to:
(i) comprehend the applicable laws relating to ML/TF, including the Act and Rules;
(ii) understand its policies, procedures, systems and controls related to AML/CFT and any amendments/modifications thereto;
(iii) recognise and deal with transactions and other activities which may be related to ML/TF;
(iv) comprehend the kind of activity that may constitute suspicious activity, which warrants prompt notification to the Principal Officer;
(v) have knowledge of the prevailing techniques, methods and trends in ML/TF, relevant to the business of the Company;
(vi) understand their roles and responsibilities in combating ML/TF, including the identity and duties of the Company's Principal Officer and deputy, where applicable; and,
(vii) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions
(c) ensure that its AML/CFT training:
(i) is relevant and tailored to the Company's activities, including its products, services, customers, distribution channels, business partners, level and nature of its transactions; and
(ii) identifies and indicates the different levels of ML/TF risk and vulnerabilities associated with the
Company.

11. RECORD KEEPING

JAINAM IFSC MAVENS PVT. LTD.

Company shall maintain the following records:
(a) a copy of all documents and information obtained in undertaking initial and ongoing Customer Due Diligence;
(b) records of customer business relationships (both original and certified copies), which include: -
(i) correspondence of business and other information relating to a customer's account;
(ii)adequate records of transactions to enable standalone transactions to be reconstructed; and
(iii) internal findings and analysis relating to a business transaction or other transactions, where the transaction or business may be unusual or suspicious, whether or not it results in a Suspicious Transactions Report;
(c) notifications made by the employee to intimate potential ML/TF transaction;
(d) Suspicious Transactions Reports and any relevant supporting documents and information, including internal findings and analysis;
(e) any relevant communications, if made with the FIU;
(f) Risk assessment Documents and
(g) any other Document may be expressly required to record and maintain, under the Guidelines.

The Company shall preserve all necessary records, for at least six years or for such period as prescribed under the applicable laws, from the date on which business relationship has ended or transaction is completed.

The Company shall provide to the Authority or any law enforcement agency immediately on request, a copy of a records maintained by it under these Guidelines

The Company shall comply with the requirements prescribed under rule 3, 4 and 5 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

The above records may be kept in electronic format.

Where the date on which the business relationship with a customer has ended remains unclear, it may be taken to have ended on the date of the completion of the last transaction.

12. PROCESS OF IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

12.1 The process of identification of suspicious transactions is divided into below four steps:

(a) Detect a suspicious indicator(s);
(b) Ask the customer questions;
(c) Review customer's records; and
(d) Evaluate the above information

(a) Detect a suspicious indicator(s):

The first step in identifying a suspicious transaction is to detect indicators that a transaction(s) may involve funds that are derived from an illegal activity or that the transaction(s) is an attempt to disguise funds derived from illegal activity or lacks a business or apparent lawful purpose. The suspicious indicators act as "red flags" and includes:

(a) complex, unusual or large transactions that have no apparent economic or lawful purpose;
(b) unusual pattern of transactions that have no apparent economic or lawful purpose;
(c) the transaction (or attempted transaction) does not match the known background, nature and type of customer, including source of funds;
(d) unusual customer behaviour;
(e) Customers whose identity verification seems difficult or clients that appear non-cooperative;
(f) Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
(g) Customers based in high-risk jurisdictions;
(h) Substantial increases in business without apparent cause; or
(i) Attempted transfer of investment proceeds to apparently unrelated third parties.

The presence of suspicious indicators does not immediately equate to the criminality or suspicion.

The Company on the detection of an indicator especially a combination of indicators, shall increase monitoring and shall further take actions to assess whether the transaction(s) should be reported to the FIU-IND as suspicious.

(b) Ask Customer Questions

(i) If one or more suspicious indicators are detected, the Company shall ask the customer relevant and appropriate questions to determine whether there is a reasonable explanation for that observed indicator. Questions shall be asked using a service approach.

(c) Review Customer's Records

The next step is to determine whether the suspicious indicators identified earlier is justifiable given what is known about the customer. The Company shall review its

customer's records and consider all information that is already known about the customer. This may include:
(i) the customer's usual occupation, business or principal activity;
(ii) the customer's transaction history;
(iii) the customer's risk profile;
(iv) the customer's income level;
(v) the customers source of income as stated during account opening or initial engagement;
(vi) reasons for the transactions as provided by the customer;
(vii) the "relationship" of the customer with the sender or beneficiary of funds;
(viii) the frequency of transactions;
(ix) the size and complexity of the transaction;
(x) the identity or location of any other person(s) involved in the transaction;
(xi) the usual or typical financial, business or operational practices or behaviour of customers in the similar occupation or business category; and
(xii) the availability of identification documents and other documentation.

After reviewing as aforesaid if the Company finds that the customer's profile has changed, it shall update the customer's profile.

(d)Evaluate Information Collected
(a) Company shall evaluate the:
(i) suspicious indicators,
(ii) information solicited from the customer through questions asked, and
(iii) known information about the customer to determine if there are reasonable grounds to suspect that the transaction(s) is related to the commission of a ML/ TF or any other serious offence.
(b) If the Company concludes that there are reasonable grounds to suspect that the transaction(s) or attempted transaction(s) is linked to a ML/ TF or any other serious offence, Company will report this suspicion to the FIU-IND by completing and submitting a STR.

If the Company is not able to obtain satisfactory evidence of a customer's identity, the Company shall not proceed further with the transaction unless directed in writing to do so by the FIU-IND.

If the Company finds, the reasons for the customer's failure or refusal to produce adequate identification documentations as unreasonable or suspicious, it shall report the attempted transaction to the FIU-IND as a suspicious transaction.

12.2 Reporting Requirements to Financial Intelligence Unit – India

The reporting shall be made in the as per the formats and comprehensive reporting format guide prescribed or released by FIU-IND from time to time and Report Generation Utility and Report Validation Utility developed. The editable electronic utilities to file Suspicious Transaction Reports (STR) which FIU-IND has placed on its website, shall be used.

The Company shall report to the information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:
Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Tower-2,
Jeevan Bharati Building,
Connaught Place,
New Delhi-110001,
Telephone: 91-11-23314429, 23314459
Website: http://fiuindia.gov.in

The Company shall follow all the reporting requirements and formats that are available on the website of FIU – IND.

(i) The Suspicious Transaction Report (STR) shall be submitted promptly on arriving at a conclusion that any transaction or a series of transactions that are integrally connected, are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.
(ii) The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
(iii) The Principal Officer shall be responsible for timely submission of STR and NTR to FIU-IND;
(iv) Utmost confidentiality shall be maintained in filing of STR and NTR to FIU-IND by the Company.

12.3Confidentiality of Suspicious Transaction Report (STR)
The Company and its employees or agents shall not disclose to any person (including the customer):
(i) that it has reported or will be reporting a suspicious transaction to the FIU-IND;
(ii) that it has formed a suspicion on a particular customer's transaction; or
(iii) any other information which may cause the person to conclude that a suspicion has been formed or that a report has been or may be made to the FIU-IND.

(b) Disclosure of information on suspicious transactions is only allowed under the following circumstances:
(i) disclosure to an officer, employee or agent of the Company for any purpose connected to the performance of that person's duties;
(ii) disclosure to a lawyer for the purpose of obtaining legal advice on the matter;
(iii) disclosure to a supervisory authority (to enable it to carry out its supervisory role);
(iv) disclosure in compliance with the court order; or
(i) disclosure or information sharing among entities in a Financial Group.

13 COMPLIANCE OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS AND DOMESTIC LAWS

13.1. Requirements/obligations under International Agreements Communications from International Agencies –

(a) In terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, no account shall be opened in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

(i) The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al- Qaida Sanctions List is available at: https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

(ii) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at: https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl

(b) Details of accounts resembling any of the individuals/entities mentioned in the above lists, shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, which is available https://www.mha.gov.in/sites/default/files/ProcedureImplementationSection51A_30032021.pdf

(c) In addition to the above, other UNSC Resolutions circulated by the IFSCA in respect of any other jurisdictions/ entities from time to time, shall also be taken note of for necessary compliances.

13.2 Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, shall be strictly followed.

(a) FATF Statements circulated from time to time, and publicly available information for identifying countries which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

(b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or emanating in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in the FATF statements.

(c) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations as aforesaid shall be examined, and written findings, together with all documents, shall be retained and be made available to the Authority and other relevant authorities, on request.

13.3. Secrecy Obligations and Sharing of Information:

(a) The Company shall maintain secrecy regarding the customer information that arises out of the contractual relationship between it and the customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged without the express consent of the customer.

(c) Company shall consider the requests for data/information from Government and other agencies, after satisfying itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy.

(d) The exceptions to the above obligations shall be as under:

(i) Where disclosure is under compulsion of law;
(ii) Where there is a duty to the public to disclose;
(iii) Where the interest of the Company requires disclosure; and
(iv) Where the disclosure is made with the express or implied consent of the customer.

13.4. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, Company shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether it is a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

(a) Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link: https://incometaxindiaefiling.gov.in/ post login > My Account --> Register as Reporting Financial Institution;

(b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

The Company shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at https://fedai.org.in/ for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

(c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

(d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

(e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

(f) Ensure compliance with updated instructions/ rules/ guidance notes/ Press Releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to

time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. A Company shall also take note of the following:
(i) updated Guidance Note on FATCA and CRS; and
(ii) a press release on 'Closure of Financial Accounts' under Rule 114H.

13.5. Sharing of KYC information pertaining to Indian Resident (Natural and Legal Entities) with Central KYC Records Registry (CKYCR):
(a) In terms of provision of rule 9(1A) of Rules, Company shall capture customer's KYC records and upload on CKYCR within 10 days of commencement of an account-based relationship with the customer in the form and manner as prescribed under Central KYC Registry Operating Guidelines 2016, released by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) and shall ensure that:
(i) the KYC records to be uploaded are as per KYC Template released by CERSAI.
(ii) Once KYC Identifier is generated by CKYCR, the same is communicated to the Customer.
(iii) It has performed the last KYC verification or has sent updated information in respect of a Customer to CKYCR.
(b) Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the Company with an explicit consent to download records from CKYCR, then in such cases, Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

(i) there is a change in the information of the customer as existing in the records of CKYCR;
(ii) the current address of the customer is required to be verified; and,
(iii) Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

14. GROUP PROGRAMME
The Company shall develop a Financial Group's policy on AML/CFT to meet the requirements of the Guidelines.

15. REVIEW OF PMLA POLICY:
This Policy has been reviewed, approved and adopted on 09/07/2024 in the Board Meeting. This policy has been reviewed and updated to incorporate all regulatory requirements until and including those in IFSCA guidelines IFSCA (Anti Money Laundering, Counter Terrorist-Financing and Know Your Customer) Guidelines, 2022, and circular no. F. No. 939/IFSCA/FATF-C/PMLA/2023-24/02, F. No. 822/IFSCA/FATF-C/Legal/2022-23/02 and notified by the Exchange. The policy shall be reviewed annually or pursuant to amendments or modification in the guidelines by the IFSCA or Exchange or on triggering of any event.

JAINAM IFSC MAVENS PVT. LTD.

Annexure-I
CDD Procedure
Part-I

For identification of the customers

The information to be obtained for onboarding customers is as stated below: -

(1) For Individual

(i) Full name, including any aliases;
(ii) Unique Identification Number (such as an Identity card number, passport number, etc.);
(iii) Date of birth;
(iv) Nationality;
(v) Legal domicile;
(vi) Current residential address; (other than a post office box address);
(vii) Contact details such as personal, office or work telephone numbers.
(viii) Occupation or profession, name of employer and location of activity; (wherever applicable)
(ix) Information regarding the nature of the business to be conducted; (wherever applicable)
(x) Information regarding the origin of the funds; and (wherever applicable)
(xi) Information regarding the source of wealth or income. (wherever applicable).

(2) For Legal Person or Legal Arrangement

In cases where the customer is a legal person or legal arrangement, Company shall also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement, identify and screen the related parties or connected parties of such customer and take steps to remain apprised of any changes to connected parties.
For identification of the connected parties,
Company shall obtain the following information of each related or connected party:
(i) full name, including any aliases; and
(ii) Unique Identification Number (such as an Identity card number, passport number, etc.).

Part-II

For verification of the identity of the customers

(1) Verification of identity through following documents:
(i) Passport;
(ii) Driving license;
(iii) Proof of possession of Aadhar number (for Indian Nationals) ;
(iv) Voter's Identity Card issued by Election Commission of India (for Indian Nationals);
(v) For foreign nationals, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorized by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as OVD.

(2) where simplified measures are applied for verifying the identity of the customers, the following documents shall also be deemed to be OVD:

(i) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
(ii) letter issued by a gazetted officer, with a duly attested photograph of the person.

(3) Any document used for the purpose of verification of the identity of the customer shall be an original document.

(4) In case a customer is unable to produce, or it might not be possible for customer to submit original documents for verification i.e where there's no physical contact with the customer, or the onboarding of customer is done through non-face to face mode); a copy of the OVD that is certified to be a 'true copy' and such certification may be carried out by any one of the following: -
(i) Authorised official of a bank located in a Financial Action Task Force (FATF) compliant
jurisdiction with whom the individual has banking relationship;
(ii) Notary Public (outside India);
(iii) Court Magistrate (outside India);
(iv) Judge (outside India);
(v) Certified public or professional accountant (outside India);
(vi) Lawyer (outside India);
(vii) The Embassy/Consulate General of the country of which the non-resident individual is a
citizen; or
(viii) any other authority as may be specified by the Authority.
Shall be obtained.

(5) The person certifying the OVD will be contactable and such certified copy shall be dated, signed and marked with 'original sighted/verified'.

(6) Where the simplified measures are applied for verifying the limited purpose of proof of address of the customer, where a prospective customer is unable to produce any proof of address, the following document shall also be deemed to be Officially Valid Document:
(i) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
(ii) property, Municipal tax receipt, city council tax receipt, or such other equivalent document;
(iii) bank account or Post Office savings bank account statement or statement of foreign bank; (applicable only for low-risk customers)
(iv) pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
(v) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation; and

In case the OVD presented by a foreign national does not contain the details of address, the documents issued by the Government departments of foreign jurisdictions or letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

(7) The list of documents, which may be obtained for verification of the identity of Legal Person or Legal Arrangement, are as follows:

(i) In case of Company

(a) Certificate of incorporation;
(b) Memorandum and Articles of association;
(c) PAN or equivalent document prevalent in the home jurisdiction of the company;
(d) A resolution passed by the Board of Directors and power of attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf;
(e) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the company.

(ii) In case of Partnership/limited liability partnership

(a) Registration certificate;
(b) Partnership deed/limited liability partnership deed;
(c) PAN or equivalent document prevalent in the home jurisdiction of the partnership firm;
(d) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the partnership firm;
(e) Such other documents as may be required to collectively establish the existence of such partnership firm.

(iii) In case of Trust

(a) Registration certificate;
(b) Trust deed;
(c) PAN or Form No. 60 or equivalent document prevalent in the home jurisdiction of the trust;
(d) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transact on behalf of the Trust.
(e) the names of the beneficiaries, trustees, settlor and authors of the trust and the address of the registered office of the trust; and
(f) list of trustees and documents as are required for individuals under part-I, for those discharging role as trustee and authorised to transact on behalf of the trust.";

(iv) In case of Unincorporated Associations/ Bodies

(a) Resolution of the managing body of such association/body;
(b) PAN or Form No. 60 or equivalent prevalent document in the home jurisdiction;
(c) Power of attorney granted to transact on its behalf;
(d) Such OVDs as are required for verification of the identity of the beneficial owners, managers, officers or employees, or power of attorney holders, as the case may, who are authorised to transaction on behalf of the Unincorporated Associations/ Bodies;
(e) Such other documents as may be required to collectively establish the existence of such association/body.

Part-III

Various modes of verification of the identity of the customers

(i) Use of Business Facilitators;

(ii) Except for high-risk customers, the following mode of verification may also be considered: -

(a) downloading publicly available information from an official source (such as a regulator's or other official government website).

(b) CDD information and research obtained from a reputable company or information obtained from reliable and independent public information found on the internet and commercial databases may also be acceptable as a reliable source, provided that the commercial database is recognized for such purpose by the home regulator.

Important notes for Business Facilitator: -

1) Company may identify the Business Facilitators in different geographies and shall sign agreements with them with specific terms and conditions ensuring customer secrecy and data protection.

2) Company shall maintain the details of the Business Facilitators assisting the customer, where such services are utilized.

3) Company will use Business Facilitators for verifying the information/OVD provided by the customer for opening account.

4) The Business Facilitators shall be domiciled and regulated or registered in jurisdiction not identified in the public statement of FATF as 'High Risk Jurisdictions' subject to a 'Call for Action'; or from any country specified by the Government of India by an order or by way of agreement or treaty with other sovereign governments.

Annexure-II

PART-A

V-CIP PROCESS FOR ONBOARDING INDIAN NATIONALS

1.1. Company may undertake V-CIP to carry out:

(a) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons.

(b) Updation/Periodic updation of KYC for eligible customers.

Company may use V-CIP after considering the below:

(i) complying with the minimum baseline cyber security and resilience framework as may be specified, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure shall be housed in own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall be compliant with the standards as may be specified.

(ii) Ensuring end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent shall be recorded in an auditable and alteration proof manner.
(iii) The V-CIP infrastructure / application shall be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

(iv) The video recordings shall contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

(vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as workflows shall be regularly upgraded.

Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

(vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration Testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests shall be conducted by suitably accredited agencies as may be specified. Such tests shall also be carried out periodically in conformance to internal / regulatory guidelines.

(viii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment.

Only after closure of any critical gap found during such tests, the application shall be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

1.2.2.V-CIP Procedure
(i) VCIP procedure shall be carried according to the workflow and standard operating procedure made by the Company. The V-CIP process shall be operated only by officials of the Company specially trained for this purpose. The official shall be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.
(ii) If there is a disruption in the V-CIP procedure, the same shall be aborted and a fresh session initiated.
(iii) The sequence and/or type of questions, including those indicating the liveness of the interaction during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

(iv) Any prompting, observed at the end of customer shall lead to rejection of the account opening process.
(v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list shall be factored in at appropriate stage of workflow.
(vi) The authorised official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
(a) Offline Verification of Aadhaar for identification;
(b) KYC records downloaded from CKYCR using the KYC identifier provided by the customer;
(c) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.
(vii) Aadhaar number shall be redacted or blackout
(viii) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three days from the date of carrying out V-CIP.
(ix) Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, the video process of the V-CIP shall be undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document; if in the rare cases, the entire process cannot be completed at one go or seamlessly.
(x) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.
(xi) Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.
(xii) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
(xiii) The authorised official of the Company shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.
(xiv) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of the process and its acceptability of the outcome.
(xv) All the provisions the Information Technology (IT) Act shall be appropriately complied.

1.2.3.V-CIP Records and Data Management

(a) The entire data and recordings of V-CIP shall be stored in a system / systems located in the territory of India. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical

data search. The extant instructions on record management, as stipulated in these Guidelines, shall also be applicable for VCIP.
(b) The activity log along with the credentials of the authorised person performing the V-CIP shall be preserved.

PART-B

DIGITAL KYC PROCESS FOR INDIAN NATIONALS

2.1. For undertaking CDD of Indian nationals, the Company shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:
(a) the Aadhaar number where: -

(i) the customer decides to submit his Aadhaar number voluntarily to a bank or any Company notified under first proviso to sub-section (1) of section 11A of the Act; or
(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
(bb) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of the customer's identity and address; and
(b) the Permanent Account Number or the equivalent e-document thereof, as defined in Income-tax Rules, 1962; and
(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof. Where the customer has submitted, (i) Aadhaar number under point (a) above, to a bank or a Company notified under first proviso to sub-section (1) of section 11A of the Act, such bank or Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he shall give a self-declaration to that effect to the Company.

(ii) proof of possession of Aadhaar under point (aa) above, where offline verification can be carried out, the Company shall carry out offline verification.

(iii) an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issued thereunder and take a live photo as specified under digital KYC Process as specified under Annexure I of Rules.

(iv) any OVD or proof of possession of Aadhaar number under (a)(i)(bb) above where offline verification cannot be carried out, the Company shall carry out verification through digital KYC Process as specified under Annexure I of Rules.

For a period not beyond such date as may be notified by the Government instead of carrying out digital KYC, the Company may obtain a certified copy of the proof of

possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means.

Biometric based e-KYC authentication can be done by authorised official of the Company/business facilitators.

The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

****