Falcon Trading Private Limited
210, Floor-2, Parekh Market, Jagannath Shankarsheth Marg,
Kennedy Bridge, Girgaon,
Mumbai, Maharashtra, India – 400004
CIN- U51909WB1991PTC051448
RBI NBFC License No: 05.01173

KNOW YOUR CUSTOMER AND ANTI- MONEY LAUNDERING MEASURES POLICY

CHAPTER – I

1. INTRODUCTION:

Reserve Bank of India has issued Master Direction- Know Your Customer (KYC) Direction, 2016 including comprehensive guidelines on Know Your Customer (KYC) norms and Anti- money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

In order to prevent Banks and other Financial Institutions from being used as a channel for Money Laundering (ML) / Terrorist financing (TF) and in order to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

In India the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT). In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Regulated Entities (REs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company.

This policy is applicable to all categories of products and services offered by the Company.

2. DEFINITIONS:

a. **"Aadhaar Number"** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016)

b. **"Act"** and **"Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

c. **Authentication**", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

d. **"Central KYC Records Registry" (CKYCR)** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

e. **"CKYC Identifier"**: Upon successful submission/registration of KYC Documents of the Borrower on CERSAI Portal, a 14- digit KYC Identifier Number (KIN) is issued. An SMS/email will be sent to the Borrower, once the KIN is generated. The Company need to ensure that the KIN is communicated to the Customer (either individual/Legal Entity) as the case maybe.

f. **"Certified Copy"(Original Seen & Verified/OSV)** -Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Company as per the provisions contained in the Act.

g. **Central KYC Records (CKYCR)** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

h. **Customer** For the purpose of KYC Guidelines, a "customer" is defined as:

- A person or entity that maintains an account and/or has a business relationship with the Company.

- One on whose behalf the account is maintained (i.e. the beneficial owner);
- Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Company Secretaries, Chartered Accountants, Solicitors etc. as permitted under the law, and

- Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company, say a wire transfer or issue of a high value demand draft as a single transaction.

i. **"Customer Due Diligence (CDD)**" means **identifying and verifying** the customer and the beneficial owner using reliable and independent sources of identification.

Explanation- The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

a. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;

c. Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

j. **"Customer identification"** means undertaking the process of CDD.

k. **"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.

l. **"Digital Signature"** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

m. **"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.

n. **"FATCA"** means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S Tax payers or foreign entities in which U.S Taxpayer should substantial ownership interest.

o. **"GROUP"** The term "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 (43 of 1961).

p. **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.

q. **"Non-profit organisations" (NPO)** 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 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

r. **"Non-face-to-face customers"** means customers who open accounts without visiting the branch/ offices of the company or meeting the officials/ authorized representatives of the Company.

s. **"Non- Profit Organisation"** means any entity or organisation, constituted for religious or charitable purposes referred as per section 2 (15) of the Income Tax Act, 1961, which is 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);"

t. **"Officially Valid Document" (OVD)** means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

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 or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. 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;

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

d. where the OVD 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.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD 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.

u. **"Offline verification" shall have the meaning specified in clause (pa) of Section 2 of Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016.**

v. **"On-going Due Diligence**" means regular monitoring of transactions in accounts to ensure that they are consistent with the Company's knowledge about the customers, customer's business and risk profile, the source of funds / wealth.

w. **"Payable-through accounts":** The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

x. **"Periodic Updation"** means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

y. **"Politically Exposed Persons" (PEPs)** are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

z. **"Principal Officer"** means an officer at the management level nominated by the Company, responsible for furnishing information *as per rule 8 of the Rules.*

aa. **Video based Customer Identification Process (V-CIP)":** an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

bb. "Wire Transfer" related definitions:

i) **Batch transfer:** Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.

ii) **Beneficiary:** Beneficiary refers to a natural or legal person or legal arrangement who / which is identified by the originator as the receiver of the requested wire transfer.

iii) **Beneficiary RE:** It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary RE and makes the funds available to the beneficiary.

iv) **Cover Payment:** Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

v) **Cross-border wire transfer:** Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

vi) **Domestic wire transfer:** Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.

vii) **Financial Institution:** In the context of wire-transfer instructions, the term 'Financial Institution' shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.

viii) **Intermediary RE:** Intermediary RE refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

ix) **Ordering RE:** Ordering RE refers to the financial institution, regulated by the RBI, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

x) **Originator:** Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

xi) **Serial Payment:** Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or

through one or more intermediary financial institutions (e.g., correspondent banks).

xii) **Straight-through Processing:** Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.

xiii) **Unique transaction reference number:** Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.

xiv) **Wire transfer:** Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

3. OBJECTIVE:

Objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandates making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

It is also mandated to implement a group wise policy for the purpose of discharging obligations under the provisions of Chapter VI of the Prevention of Money-Laundering Act, 2002 (15 of 2003).

In terms of PML Rules, the Company/group is required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act, 2002. (15 of 2003). Accordingly, Company, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

The Company's policy framework should seek to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing,

Proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, FTPL may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

4. Money Laundering and Terrorist Financing Risk Assessment by Company:

a) Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with Company from time to time.

b) The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the Company to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

4A. Company shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. Company shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, Company shall monitor the implementation of the controls and enhance them if necessary.

FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Company shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

CHAPTER –II

5. CUSTOMER ACCEPTANCE POLICY:

The Company shall follow the following norms while accepting and dealing with its customers:

a. No account is opened in anonymous or fictitious / benami name.

b. The Company shall carry out full scale customer due diligence (CDD) before opening an account. When the true identity of the applicant is not known or the Company is unable to apply appropriate CDD measures, no transaction or account-based relationship will be undertaken with such person / entity.

c. The account shall remain operational initially for a period of twelve months, within which CDD as per paragraph 16 or paragraph 18 of Master Direction (briefed in this policy) shall be carried out.

d. 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

e. The Company shall apply CDD measures at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of a RE desires to open another account or avail any other product or service with the same RE, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned. The Company shall, at their option, not issue UCIC to all walk-in/occasional customers provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

f. CDD Procedure is followed for all the joint account holders, while opening a joint account.

g. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

h. Additional information, where such information requirement has not been specified in the internal KYC Policy of the Company, is obtained with the explicit consent of the customer.

i. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk. The illustrative list of such risk categorization is provided in **Annexure –I.**

The customer profile contains mandatory information to be sought for KYC purpose relating to customer's identity, address, social/financial status, nature of business activity, information about the clients' business and their location etc. geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken –cash, cheque/monetary instruments, wire transfers, forex transactions, The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross selling or any other purpose. The Company shall maintain secrecy regarding customer information except where the disclosure is under compulsion of law, there is a duty to the public to disclose, the disclosure is made with express or implied consent of the customer.

The Company shall have suitable system in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in MD.

j. The intent of the Policy is not to result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers.

k. When the true identity of the account holder is not known, the Company shall file Suspicious Transaction Reporting (STR) as provided below in clause 8.

l. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

m. Where the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

6. CUSTOMER IDENTIFICATION PROCEDURE:

a. The Company shall undertake identification of customers before commencement of an account based relationship. Customer identification means identifying the customer and verifying his / her identity by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious/ anonymous/ benami person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship.

b. An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP is integrated into the AML (Anti Money Laundering) program for the company in terms of the Prevention of Money Laundering Act, 2002 and the relevant rules notified there under(PMLA), which contains provisions requiring the business processes to:

- **Verify the identity of any Person** transacting with the Company to the extent reasonable and practicable.

- **Maintain records of the information** used to verify a customer's identity, including name, address and other identifying information and;

- Consult sanctions lists/ FATF statements of known or suspected terrorists:

- The Company shall ensure that, in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, the Company does not have any account 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",** established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes

names of individuals and entities associated with the Al- Qaida is available at https://scsanctions.un.org/ohz5jen-al-qaida.html

ii) The **"Taliban Sanctions List"**, established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/3ppp1en-taliban.htm

Company shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.

- **Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):**

a) FTPL shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).

b) In accordance with paragraph 3 of the aforementioned Order, FTPL shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

c) Further, FTPL shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

d) In case of match in the above cases, FTPL shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. Company shall file an STR

with FIUIND covering all transactions in the accounts, covered above, carried through or attempted.

It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

e) FTPL may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, Company shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

g) In case an order to freeze assets under Section 12A is received by the Company from the CNO, Company shall, without delay, take necessary action to comply with the Order.

h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual / entity regarding unfreezing shall be forwarded by FTPL along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

- In In addition to the above, FTPL will take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

- The Company may ensure the aforesaid, verifying the name of person or entity through the website of the concerned entity or through the service provider, who provide the said service of third-party verification, in compliance applicable provisions/guideline of Reserve Bank of India/National Housing Bank, the Prevention of Money Laundering Act and rules made thereunder in this regard.

- Details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list, shall be treated as suspicious and reported to the FIU-IND, apart from advising Ministry of Home Affairs as required under UAPA notification.

  The Credit Head / Zonal Head, will be responsible to ensure that, the name of Borrower is not reflecting in the afore said list.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

c. The Company shall undertake identification of customers in the following cases:

- Commencement of an account-based relationship with the customer.
- When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- Selling third party products as agent.

d. The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company. Each business process shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks. Such standards and procedures shall include, at a minimum, the following elements.

e. **IDENTIFICATION:**

All the customers shall be identified by a unique identification code to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers.

The customer identification requirement detailed in **Annexure- II** to this policy. Each business process shall implement procedures to obtain from each Customer, prior to trans acting, the following information as may be relevant, to that business:

- **Name**: procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems as the customer will be exactly the same as (and not merely similar to, or a variation of) the name that appears on any identifying documentation reviewed in connection with the loan;

- **For individuals - age / date of birth;** For a person other than individual (such as corporation, partnership or trust) - date of incorporation;

- Address including the documentary proof there of:
  i. For an individual, a residential or business street address;
  ii. For a Person other than an individual (such as a corporation, partnership, or trust), the principal place of business, local office, or other physical location;

- Telephone/Fax number/E-mail ID;
- Identification number:

  i. A taxpayer identification number; passport number and country of issuance; proof of possession of Aadhaar number; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard or the unique number or code assigned by the Central KYC Records Registry. When opening an account for a person (other than an individual) that does not have an identification number, the business process must request alternative government- issued documentation certifying the existence of the business or enterprise;

  Where a customer submits proof of possession of Aadhaar number, the Company shall ensure that such customer redacts or blackout his Aadhaar number before submitting the same to the Company

  The submission of Aadhaar is mandatory only when the customer is desirous of receiving any benefit or subsidy under any scheme notified under Section7 of the Aadhaar Act or as per the Notification, Circular, Guidelines, as may be issued by RBI read with Directions/Guidelines, issued UIDAI from time to time, otherwise Aadhaar is not mandatory and the Company not to insist for the same. However, the individual, if so desires, may provide the same out of volition. The customer, at their option, shall submit one of the OVDs.

  ii. For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but each business process shall implement procedures to confirm that the application was filed before the loan is sanctioned to customer and to obtain the identification number within a reasonable period of time before disbursal of loan.

- **One** recent **photograph of the individual customer**. Fresh photographs will be obtained from minor customer on becoming major.

  For undertaking CDD, the list of documents that can be accepted as proof of identity and address from various customers across various products offered by the Company is given as **Annexure- III** to this policy. These are appropriately covered in the credit policies of the respective businesses and communicated to the credit approving authorities.

7. CUSTOMER DUE DILIGENCE (CDD)/VERIFICATION:

Each business process as a part of the credit policy will document and implement appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures foreach business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non-documentary verification methods that are appropriate given the nature of the business process, the products and services provided and the associated risks.

a. **Verification through Officially Valid Documents:**

Comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or Officially Valid Document so produced by the customer with the original and recording the same on the copy by the authorized officer of the Company.

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company as provided in **Annexure - III** to this policy. These are appropriately covered in the credit policies of the respective businesses. The customer verification processes will be covered in detail in the credit policies of every business.

b. **Verification through Non-Documentary Methods:**

These methods may include, but are not limited to:

i. Contacting or visiting a customer;

ii. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a

consumer reporting agency, public database, or other source;

iii. Checking references with other financial institutions; or

iv. Obtaining a financial statement.

c. **Offline Verification:**

The Company may carry out offline verification of a customer under the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016, Directions/Guidelines issued by the Unique Identification Authority of India (hereinafter referred as Aadhaar Regulations) if the customer is desirous of undergoing Aadhaar offline verification for identification purpose.

Offline Verification can be done by following two ways:

- **Option 1: Using the Quick Response (QR) codes:**
  Seek the Aadhaar QR code from the customers. The same has to be download and printed by the customer and submitted to the company who shall read it using a QR code reader. Scanning of QR code, from the QR code reader will provide the name, address and photograph of the customer, without providing the Aadhaar number.
- **Option 2: Using paperless local e-KYC:**
  The paperless local e-KYC involves generation of a digitally signed XML which can be stored in a laptop or phone and be communicated by the customer to the company, as and when required. Companies can receive the Aadhaar Paperless Offline e-KYC XML from the customers. The XML file provides the name, address and photograph of the customer, without providing the Aadhaar number.

  No such offline verification will be performed without obtaining the written consent of the customer in the manner prescribed in the Notification, Circular and Guideline issued by RBI read with Aadhaar Regulations.

  Except in accordance with the Notification, Circular, Guidelines issued by RBI read with Aadhaar Regulations, the Company shall not collect, use or store an Aadhaar number of its customer for any purpose.

d. **Verification of equivalent e-document:**

Where the customer submits an equivalent e-document of any Officially Valid Document (OVD), issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and take live photo of the customer as specified under digital KYC in RBI regulations.

e. Verification based on Digital KYC:

FTPL can undertake the Digital KYC process for CDD in which live photo of the customer will be captured and officially valid document or the proof of possession of Aadhaar to be taken, 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 authorized officer of the FTPL, as per the provisions contained in the Prevention of Money Laundering Act, 2002 and the rules made thereunder read with RBI Directions. The KYC Identifier with an explicit consent to download records from CKYCR. FTPL can shall retrieve the KYC records online from the CKYCR in accordance with paragraph 56 of Master Direction (briefed in this policy).

Once KYC Identifier is generated by CKYCR, Company shall ensure that the same is communicated to the individual/LE as the case may be.

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per clauses (e) and (f), respectively, at the time of periodic updating as specified in paragraph 38 of the Master Direction (briefed in this policy), or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the Company obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of the PML Rules, the Company shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updating of KYC record of the said customer. Once CKYCR informs an RE regarding an update in the KYC record of an existing customer, the Company shall retrieve the updated KYC records from CKYCR and update the

KYC record maintained by the Company.

The detailed procedure for Digital KYC is annexed as Annexure-IV.

f. Video based customer identification process (V-CIP):

A method of customer identification by an official of FTPL by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process.

The Company may undertake live V-CIP for establishment of an account-based relationship with an individual customer after obtaining his informed consent and adhering to the procedures prescribed in RBI regulations. This process shall be treated as face-to-face process for the purpose of customer identification.

Provided that in case of CDD of a proprietorship firm, FTPL shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Annexure III-Sole Proprietorship, apart from undertaking CDD of the proprietor.

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 3 days from the date of carrying out V-CIP.

The Company to comply the applicable provisions of RBI Master Direction-Know Your Customer (KYC) Directions, 2016 w.r.t. V-CIP.

The entire data and recordings of V-CIP shall be stored in a system(s) located in India. FTPL 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 the RBI Master Direction on KYC, shall also be applicable for V-CIP. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the FTPL only and all the data including video recording is transferred to the FTPL shall be exclusively owned / leased server(s) including

cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the FTPL.

The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses

The video recordings should 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.

The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

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 should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In).

Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

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

should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

The activity log along with the credentials of the official performing the V-CIP shall be preserved. The Procedure of V-CIP is given in **Annexure-V**.

g. **Accounts Opening through Aadhaar OTP based e-KYC:** FTPL may provide an option for One Time Pin (OTP) based e-KYC process for on- boarding of customers. Accounts opened in terms of this proviso i.e., using OTP based e-KYC, are subject to the following conditions:

- There must be a specific consent from the customer for authentication through OTP
- As a risk-mitigating measure for such accounts, Company shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. Company shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
- Only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year
- Account, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per paragraph 16 or as per paragraph 18 of Master Direction (briefed in this policy) (V-CIP) is carried out. If Aadhaar details are used under paragraph 18 of Master Direction (briefed in this policy), the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
- If the CDD procedure as mentioned above is not completed within a year, in respect of borrowed accounts no further debits shall be allowed.
- A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to- face mode with any other Regulated Entity (RE). Further, while uploading KYC information to CKYCR, Company shall clearly indicate that such accounts are opened using OTP based e-KYC and other Company shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to- face mode. Further, for updation/periodic updation, Aadhaar OTP based e-KYC in non-face to face mode may be used. To clarify, conditions stipulated in paragraph 17 of Master Direction (briefed

in this policy) are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

- FTPL shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.
- FTPL may apply for getting licence of KYC User Agency (KUA) or Sub KUA to e-KYC Authentication as per the applicable Notification, Circular and Guidelines issued by RBI, UIDAI and other Regulatory or Statutory Authority for the doing the CDD by way authentication of Aadhaar, as may be permitted by RBI.

h. Additional Measures:

- The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the FTPL are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the RE has expired at the time of periodic updation of KYC, RE shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

- Customer's PAN details, if available with the FTPL, is verified from the database of the issuing authority at the time of periodic updation of KYC.

- 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 updation/periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of updation/periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

- In order to ensure customer convenience, FTPL may consider making available the facility of updation/periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of FTPL or any

committee of the Board to which power has been delegated.

- FTPL shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Company such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the RE where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of Company or any committee of the Board to which power has been delegated.

- Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Company's end.

CHAPTER – III

8. RESOLUTION OF DISCREPANCIES:

Each business process shall document and implement procedures to resolve information discrepancies and to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

9. REPORTING:

The Company shall have a system of internal reporting of suspicious transactions, counterfeit transactions and cash transactions greater than Rs.10 lakhs, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

"**Suspicious transaction**" means a transaction whether or not made in cash which, to a person acting in good faith:

- Gives rise to reasonable grounds for suspicion that it may involve the proceeds of crime; or
- Appears to be carried out under circumstances of unusual or unjustified complexity; or
- Appears to lack any economic rationale or bona fide purpose; or
- Gives rise to reasonable grounds for suspicion that it may involve financing of activities related to terrorism; or
- Is abandoned by customers when asked to provide details or supporting documents.

Branch Sales Manager/Branch Manager/ Branch In-charge (if applicable) to give the required details of Cash Transactions [Rs.10 lakhs and above or its equivalent in foreign currency in one transaction or series of related transaction in any account(s)] and Suspicious Transaction(s), to the Company Secretary & Compliance Officer of the Company, promptly upon detecting the same and the Company Secretary & Compliance Officer, to report the said Transaction(s) to FIU-India, as per the PMLA Act and the rules made there under.

The report of the Cash transaction / Suspicious Transactions is to be filed on the website http://www.fiuindia.gov.in

Every Company, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. In terms of PML Rules, Company/group is required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act, 2002. (15 of 2003). Accordingly, Company/group shall implement group-wide programmes against money laundering and terror financing, including groupwide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off. However, such confidentiality requirement shall not inhibit sharing of information here for any analysis of transactions and activities which appear unusual, if any such analysis has been done.

The Company to place the details of Cash Transactions and Suspicious, as above before the Audit Committee/Board of Director, on periodically basis, as per the applicable provisions of Act and the Rules and the Board of Directors to ensure the compliance of the same.

Illustrative list of activities which would be construed as suspicious transactions are given in Annexure-VI to this policy.

Further, the Principal Officer shall furnish information of the above-mentioned transactions to the Director, Financial Intelligence Unit – India (FIU-IND) at the prescribed address in the formats prescribed in this regard including the electronic filing of reports.

Provided that where the Principal Officer, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued greater than Rs.10 lakhs so as to defeat the provisions of the PMLA regulations, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

The Company shall not put any restriction on operations in the accounts where a suspicious transaction report (STR) has been filed. The Company shall keep the fact of furnishing of STR strictly confidential and shall ensure that there is no tipping off to the customer at any level.

The Company shall upload the KYC information pertaining to individuals / legal entities, as applicable from time to time, with Central KYC Records Registry (CKYCR) within 10 days of commencement of account-based relationship with the customer, in terms of provisions of the RBI Directions read with Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

10. RECORDS RETENTION:

Each business process shall document and implement appropriate procedures to retain records of KYC due diligence and anti-money laundering measures. The business process shall implement, at a minimum, the following procedures for retaining records:

a. **Transactions for which records need to be maintained:**

- All cash transactions of the value of more than Rs.10 lakhs or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakhs or its equivalent in foreign currency.
- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place.
- All suspicious transactions whether or not made in cash.

b. **Information to be preserved:**

The information required to be preserved with respect to the above transactions are the nature of transactions, amount and the currency in which it was denominated, date of transaction and the parties to the transaction.

c. **Periodicity of retention:**

The following records shall be retained for a minimum period of five years after the business relationship is ended:

i. The customer identification information and residence identification information including the documentary evidence thereof.

ii. All other necessary records pertaining to the transactions that could be produced as evidence for prosecution of persons involved in criminal activity.

Further, a description of the methods used to verify customer identity as well as a description of the resolution of any discrepancies in verification shall be maintained for a period of at least Ten (10) years after such record was created. The above records shall be maintained either in hard or soft format and shall be made available to the competent authorities upon request.

11. EXISTING CUSTOMERS:

The requirements of the earlier sections are not applicable to accounts opened by existing customers, provided that the business process has previously verified the identity of the customer and the business process continues to have a reasonable belief that it knows the true identity of the customer. Further, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger are view of the due diligence measures.

12. Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of paragraph 17 of Master Direction (briefed in this policy)):

Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this paragraph includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by Company for non face-to-face customer onboarding (other than customer onboarding in terms of paragraph 17 of Master Direction (briefed in this policy)):

a) In case RE has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with

prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. RE shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

c) Apart from obtaining the current address proof, Company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

d) RE shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

For ongoing due diligence, FTPL may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

The following are the indicative list where the risk perception of a customer may be considered higher:

(i) Customers requesting for frequent change of address/contact details
(ii) Sudden change in the loan account activity of the customers
(iii) Frequent closure and opening of loan accounts by the customers

Enhanced due diligence may be in the nature of keeping the account monitored closely for a re-categorization of risk, updation of fresh KYC documents, field investigation or visit of the customer, etc., which shall form part of the credit policies of the businesses.

13. RELIANCE ON THIRD PARTY DUE DILIGENCE:

For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on a third party; subject to the conditions that- the Company obtains records or information of such customer due diligence carried out by the third party within two days from the third party or from Central KYC Records Registry;

a) The Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;

b) The Company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;

c) The third party is not based in a country or jurisdiction assessed as high risk; and

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

e) When any relation between the Company and a Non – Profit organisation Client is established, the Company is required to registered it on the DARPAN Portal of the NITI Aayog (if not already registered) and maintain such registration records for a period of 5 years after the business relationship between a client and a reporting entity has been ended or account has been closed, whichever is later.

CHAPTER –IV

14. RISK CATEGORISATION:

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers will be carried out from time to time.

The Company shall have an internal policy in place for periodical updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where the risk is high of customer identification data after the account is opened. Full KYC exercise will be done at a periodicity not less than once in ten years in case of low-risk category customers, not less than once in eight years in case of medium risk category customers and not less than once in two years in case of high-risk category customers.

Low risk category customers need not submit fresh proofs of identity and address at the time of periodic updation, in case of no change in status with respect to their identities and addresses and a self-certification by the customer to that effect shall suffice in such cases. In case of change of address of such 'low risk' customers, they can forward a certified copy of proof of address by mail/post, etc.

In case any existing customer fails to submit PAN or equivalent e-document or Form No.60, the Company may temporarily cease operations in the account till the time the same is submitted by the customer. For the purpose of ceasing the operation in the account, only credits shall be allowed.

However, the customer who are unable to provide PAN or equivalent e-document or Form No. 60 owing to injury, illness or infirmity on account of old age or such like causes, the Company will continue operation of accounts for such customers subject to enhanced monitoring of the accounts.

All the customers under different product categories are categorized into low, medium and high risk based on their profile. The Credit Manager while appraising the transaction and rendering his approval will prepare the profile of the customer based on risk categorization. An indicative categorization for the guidance of

businesses is provided in Annexure - I. Each business process adopts the risk categorization in their respective credit policies subject to confirmation by compliance based on the customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer. Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), and other agencies, etc., may also be used in risk assessment.

15. MONITORING OF TRANSACTIONS

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The different business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible legitimate purpose. High-risk accounts have to be subjected to intensified monitoring. The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high-risk scenarios, the identity of the customer shall be established as per paragraph 16 or paragraph 18 of the Master Direction (briefed in this policy) and foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per paragraph 16 or paragraph 18 the Master Direction (briefed in this policy).

16. RISK MANAGEMENT:

The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

For Risk Management, Company shall have a risk-based approach which includes the following.

a) Customers shall be categorised as low, medium and high-risk category, based on the assessment and risk perception of the Company.
b) Broad principles may be laid down by the Company for risk-categorisation of customers.
c) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
d) The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Bank Association (IBA), and other agencies, etc., may also be used in risk assessment.

Company's internal audit function play a role in evaluating and ensuring adherence to the KYC policies and procedures. Internal Auditors specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

The compliance in this regard is put up before the Audit Committee / Board from time to time.

The Company ensures that the decision-making functions of determining compliance with KYC norms are not outsourced.

17. HIRING OF EMPLOYEES AND EMPLOYEE TRAINING:

Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.

FTPL shall end eavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the RE, regulation and related issues shall be ensured.

18. APPOINTMENT OF DESIGNATED DIRECTOR / PRINCIPAL OFFICER:

A) Designated Director

- A “Designated Director” means a person designated by the Board of Directors to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules.
- The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
- Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.
- In no case, the Principal Officer shall be nominated as the 'Designated Director'.

B) PRINCIPAL OFFICER

- The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
- The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.
- Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

19. SECRECY OBLIGATIONS AND SHARING OF INFORMATION:

(a) Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the RE and 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 for the purpose of cross selling, or for any other purpose without the express permission of the customer.

(c) While considering the requests for data/information from Government and other agencies, Company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

(d) The exceptions to the said rule 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 RE requires disclosure and

iv. Where the disclosure is made with the express or implied consent of the customer.

20. INTRODUCTION OF NEW TECHNOLOGIES

FTPL shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and preexisting products.

Further, FTPL shall ensure:

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc

Falcon Trading Private Limited
210, Floor-2, Parekh Market, Jagannath Shankarsheth Marg,
Kennedy Bridge, Girgaon,
Mumbai, Maharashtra, India – 400004
CIN- U51909WB1991PTC051448
RBI NBFC License No: 05.01173

Annexure – I

Indicative list for Risk Categorization

Low Risk Category

Individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorized as low risk. Low risk customers can be:

a. Salaried employees
b. Individuals / entities with business income including Self Employed Professionals / Self Employed Non Professionals
c. Manufacturers, Traders, Distributors, Service Providers, Business Owners
d. People working in Government departments and Government-owned companies
e. People working in Statutory bodies & Regulators

Medium & High-Risk Category

Customers that are likely to pose a higher-than-average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

i. Medium Risk Customers can be considered as customers who are engaged in the following activity:

a. Real Estate,
b. Infrastructure/ Construction Activity
c. Jewellery Retail and Wholesaler
d. Bullion and Gold Traders
e. Diamond Traders and Manufacturers
f. Transporters
g. Travel Agents
h. Hotel Industry
i. Restaurants
j. Salon/ Spa
k. Gym Services

ii. High Risk Customers can be considered as customers who are engaged in the following activity:

a. Collection Agency (Agents for Banks / MFI)
b. Gambling and Gaming Business
c. Places of Worship
d. Amusement Oarks,
e. Liquor Parlours, Bars,
f. Unlawful Entertainment and recreation centres
g. Seasonal Business such as crackers,
h. Media
i. Lawyers and law enforcement agencies (close relatives also)
j. Policemen (Close relatives also)
k. STD & PCO owners (Sole Activity)
l. Local News paper
m. Local Finance Company
n. Production or activities involving harmful or explosive forms of forced labour/ harmful child labour
o. Production or trade in any product or activity deemed illegal
p. Production or trade in weapons and munitions
q. Production or trade in alcohol beverages
r. Production or trade in tobacco (if it is the only product)
s. Production or trade in radioactive materials
t. Production or trade in or use of unbonded asbestos fibres
u. Production or trade in pesticides/ herbicides subject to international phase out or bans.
v. Production or trade in ozone depleting substances subject to international phase out or bans
w. Drift net fishing and Marine Activity
x. Production or activities that impinge on the lands owned or claimed under adjudication, by indigenous peoples, without full documented consent of such peoples;
y. Non- Resident Indian customers with no residential/ permanent base in India
z. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
aa. Non-face-to-face customers
bb. Those with dubious reputation, Defaulters, Wilful Defaulters, as per public information available

Updation/Periodic updation of KYC Requirements:

Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where

there is high risk. Periodic updation shall be carried out at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account / last KYC updation, or in line with RBI guidelines issued from time to time in this matter.

Annexure - II

CUSTOMER IDENTIFICATION REQUIREMENTS

TRUST/NOMINEE OR FIDUCIARY ACCOUNTS

In the case of any application from trust/nominee or fiduciary accounts, the Company determines whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary.

If in doubt of the persons behind the customer, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. Company takes reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

ACCOUNTS OF COMPANIES AND FIRMS

Company needs to be vigilant against business entities being used by individuals as a 'front' for transactions. Company should examine the control structure of the entity and identify the natural persons who have a controlling interest and who comprise the management.

These requirements may be moderated according to the risk perception e.g. in the case of a public company.

Client accounts opened by professional intermediaries

Where the transaction is with a professional intermediary who in turn is operating on behalf of a single client, that client must be identified. The Company shall not open accounts with such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.

Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior

executives of state- owned corporations, important political party officials, etc.
The Company offers products primarily to Indian residents only. The Company if extending any finance to non-residents should check if he is PEP and check all the information available about the person in the public domain. The decision to transact with the PEP should be taken only by the Head of credit of the respective businesses supported by appropriate verification. The Company is also required to subject such accounts to enhanced monitoring on an ongoing basis. The above norms shall also be applied to the contracts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the approval of the Head of respective businesses shall be obtained to continue the business relationship and subject the account to the KYC due diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

A. The Company shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

a. Company shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;

b. Reasonable measures are taken by the Company for establishing the source of funds / wealth;

c. The approval to open an account for a PEP shall be obtained from the senior management;

d. all such accounts are subjected to enhanced monitoring on an on-going basis;

e. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

B. These instructions shall also be applicable to family members or close associates of PEPs.

Accounts of non-face-to-face customers

The Accounts of non-face to face customers will be categorised as a high risk Customer base. The process for enhanced due diligence is specified above for onboarding of such non face to face customers.

Identity of Beneficial Owner

The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a customer and/or the person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership

(i) 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 person, has a controlling ownership interest or who exercises control through other means.

Explanation:

a. "Controlling ownership interest" means ownership of or entitlement to more than Ten (10%) percent of shares or capital or profits of the company;

b. "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;

(ii) 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 ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercise control through other means;

Explanation- For this Purpose of this sub clause, control shall include the right to control the management or policy decision.

(iii) where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than 15 percent of the property or capital or profits of such association or body of individuals;

c. where no natural person is identified under (a) or (b) or (c) above, the beneficial

owner is the relevant natural person who holds the position of senior managing official;

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 percent 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. In case the customer is acting on behalf of another person as trustee/ nominee, the Company shall obtain satisfactory evidence of the identity of the persons on whose behalf they are acting; and

Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

Falcon Trading Private Limited
210, Floor-2, Parekh Market, Jagannath Shankarsheth Marg,
Kennedy Bridge, Girgaon,
Mumbai, Maharashtra, India – 400004
CIN- U51909WB1991PTC051448
RBI NBFC License No: 05.01173

Annexure-III

CUSTOMER IDENTIFICATION PROCEDURE – KYC DOCUMENTS THAT MAY BE OBTAINED FROM CUSTOMERS (OFFICIALLY VALID DOCUMENTS)

Nature of customer	List of applicable documents
Individual	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, authorized signatory or the power of attorney holder related to any legal entity; a. Proof of possession of Aadhaar number where offline verification can be carried out; or b. A certified copy of any OVD containing details of his identity and address; and; c. The Permanent Account Number (PAN) or Form no.60; and d. Such other documents as specified by the Company from time to time. **List of OVDs**: a. Passport (Valid) b. Driving license c. Proof of possession of Aadhaar number/ Aadhaar (Optional) d. Voter's identity card issued by the Election Commission of India e. Job card issued by NREGA duly signed by an officer of the State Govt. f. Letter issued by the National Population Register containing details of name and a ddress. **Provided that**: a. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the UIDAI. b. Where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address: -

	• Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); • Property or Municipal tax receipt; • Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; • Letter of allotment of accommodation from employer issued by State Govt. or Central Govt. Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation; c. Where the OVD 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. **Explanation**: A document shall be deemed to be an OVD 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.
Sole Proprietary firms	**a.** Customer due diligence of the individual proprietor shall be carried out as applicable / specified for Individual. **b.** In addition to the above, any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained: • Registration certificate including Udyam Registration Certificate (URC) issued by the Government. • Certificate/licence issued by the municipal authorities under Shop and Establishment Act. • Sales and income tax returns. • CST/VAT/ GST certificate ~~(provisional/final)~~. • Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

	• IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. • Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. • Utility bills such as electricity, water, landline telephone bills, etc. **Explanation**: In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at its discretion, accept only one of those documents as proof of business / activity after recording the appropriate reason for accepting one document. The Company shall undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
Company	Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: a. Certificate of incorporation b. Memorandum and Articles of Association c. Permanent Account Number of the company d. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf e. Documents, as specified for Individual, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf f. the names of the relevant persons holding senior management position; and g. the registered office and the principal place of its business, if it is different.
Partnership Firm	Certified copies of each of the following documents or the equivalent e-documents shall be obtained:

	a. Registration certificate b. Partnership deed c. Permanent Account Number of the partnership firm d. Documents, as specified for Individual, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf e. Names of all the partners f. the registered office and the principal place of its business, if it is different.
Trust	Certified copies of each of the following documents or the equivalent e-documents shall be obtained: a. Registration certificate b. Trust deed c. Permanent Account Number or Form No.60 of the trust d. Documents, as specified for Individual, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. e. the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust f. the address of the registered office of the trust; and g. list of trustees and documents, as specified in paragraph 16 of Master Direction (briefed in this policy), for those discharging the role as trustee and authorized to transact on behalf of the trust. Provided that in case of a trust, the RE shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified below : - Carrying out any international money transfer operations for a person who is not an account holder of the RE. -. Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

	f- When Company has reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
Unincorporated Association or a Body of Individuals	Certified copies of each of the following documents or the equivalent e-documents shall be obtained: a. Resolution of the managing body of such association or body of individuals b. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals c. Power of attorney granted to transact on its behalf d. Documents, as specified for Individual, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and; e. Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals. **Explanation:** **a.** Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'. **b.** Term 'body of individuals' includes societies.
Juridical persons not specifically covered above, such as societies, universities and local bodies like village panchayats who purports to act on behalf of such juridical person or individual or trust	Certified copies of the following documents or the equivalent e-documents shall be obtained: a. Document showing name of the person authorized to act on behalf of the entity; b. Documents, as specified for Individual, of the person holding an attorney to transact on its behalf and; c. Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Note: Notwithstanding the list of documents as stated above, in case of change, if any, in the regulations as notified by RBI from time to time, the list of documents as prescribed by RBI shall prevail over the above.

Annexure - IV

DIGITAL KYC PROCESS

A. FTPL **to develop** an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of the customers and the KYC process shall be undertaken only through this authenticated application of FTPL.

B. The access of the Application shall be controlled by the FTPL and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by FTPL to its authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official of FTPL or vice-versa. The original OVD shall be in possession of the customer.

D. The FTPL must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Company) and Date (DD/MM/YYYY) and time stamp (HH/MM/SS) on the captured live photograph of the customer.

E. The Application of the FTPL shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officers registered with FTPL shall not be used for customer signature. The FTPL must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the FTPL. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the FTPL, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of the FTPL shall check and verify that: -

- Information available in the picture of document is matching with the information entered by authorized officer in CAF.
- Live photograph of the customer matches with the photo available in the document.; and

- All of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the FTPL who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

N. FTPL may use the services of Business Correspondent (BC)/Authorised person for this process.

Annexure – V
PROCEDURE OF V-CIP

A. FTPL to formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of FTPL specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

B. If there is a disruption in the V-CIP due to pausing of video, reconnecting calls, etc., which does not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the FTPL. V-CIP procedure, the same should be aborted and a fresh session initiated.

C. 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.

D. Any prompting, observed at end of customer shall lead to rejection of the account opening process.

E. 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 should be factored in at appropriate stage of work flow.

F. The authorized official of FTPL 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:
   - OTP based Aadhaar e-KYC authentication
   - Offline Verification of Aadhaar for identification
   - KYC records downloaded from CKYCR, in accordance with paragraph 56 of Master Direction (briefed in this policy), using the KYC identifier provided by the customer;
   - Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker.
   - FTPL shall ensure to redact or blackout the Aadhaar number in terms of paragraph 16 of Master Direction (briefed in this policy).

- 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 working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, FTPL shall ensure that the video process of the V-CIP is undertaken within three working 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. However, FTPL shall ensure that no incremental risk is added due to this.

G. 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.

H. FTPL 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.

I. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

J. The authorized official of the FTPL 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.

K. Assisted V-CIP shall be permissible when FTPL take help of Business Correspondent (BC)/Authorised person facilitating the process only at the customer end. FTPL shall maintain the details of the BC/ Authorised person assisting the customer, where services of BC/ Authorised person are utilized. The ultimate responsibility for customer due diligence will be with the FTPL.

L. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

Falcon Trading Private Limited
210, Floor-2, Parekh Market, Jagannath Shankarsheth Marg,
Kennedy Bridge, Girgaon,
Mumbai, Maharashtra, India – 400004
CIN- U51909WB1991PTC051448
RBI NBFC License No: 05.01173

M. All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the FTPL.

Falcon Trading Private Limited
210, Floor-2, Parekh Market, Jagannath Shankarsheth Marg,
Kennedy Bridge, Girgaon,
Mumbai, Maharashtra, India – 400004
CIN- U51909WB1991PTC051448
RBI NBFC License No: 05.01173

Annexure - VI

ILLUSTRATIVE LIST OF ACTIVITIES WHICH WOULD BE CONSTRUED AS SUSPICIOUS TRANSACTIONS

Activities which are not consistent with the customer's business, i.e., accounts with large volume of credits whereas the nature of business does not justify such credits shall be construed as suspicious transactions.

Any attempt to avoid reporting / record-keeping requirements / provides insufficient/ suspicious information:

a. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

b. Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.

c. An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

d. Certain Employees of the Company arousing suspicion:

e. An employee whose lavish lifestyle cannot be supported by his or her salary.

f. Negligence of employees / wilful blindness is reported repeatedly.

g. Some examples of suspicious activities/transactions to be monitored by the operating staff:

h. Multiple accounts under the same name.

i. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds are doubtful etc.;

j. There are reasonable doubts over the real beneficiary of the loan.

k. Frequent requests for change of address.