KNOW YOUR CUSTOMER (KYC) AND ANTI-MONEY LAUNDERING (AML) POLICY OF ESPOUSE CAPITAL PRIVATE LIMITED

ESOPPDHAN

SUMMARY OF THE POLICY

Policy Name	**Know Your Customer and Anti Money Laundering Policy**
Issue and Effective date	
Date of next review	12 months from the Issue and Effective Date
Periodicity of review	Annually
Owner / Contact	Compliance Department
Approver	Board of Directors
Annexure	• Indicative list for risk categorization of customers as- **Annexure-A** • List of KYC documents for different type of customers as **Annexure-B** • Procedure for obtaining Identification Information as **Annexure- C** • Digital KYC Process as-**Annexure D**

TABLE OF CONTENTS

1. PREAMBLE

The Board of Directors (the Board) of **Espouse Capital Private Limited** (hereinafter referred to as "the Company"), has adopted the following policy regarding salient features of Know Your Customer (KYC)/Anti-Money Laundering (AML) norms for as prescribed by the Reserve Bank of India (RBI).

2. PURPOSE

The policy has been framed in accordance with the Reserve Bank of India (Know Your Customer (KYC) Directions, 2016 issued vide circular no. RBI/DBR/2015-16/18 dated February 25, 2016 and revised vide Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated May 10, 2021.

Further, the policy has been framed in compliance with the PML Rules vide Gazette Notification GSR 538 (E) dated June 1, 2017.

As per the above referred Master Circular, the Company shall adopt the guidelines contained therein with suitable modifications in accordance with the Company's business activity and ensure that a proper policy framework on KYC and AML measures are formulated and enforced with the approval of the Board.

In terms of the provisions of Prevention of Money-Laundering Act, 2002, Amendment to Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and Prevention of Money-Laundering (Maintenance of Records) Amendment Rules, 2019, the Company shall follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions.

This Policy envisages the establishment and adoption of measures and procedures relating to KYC, AML and CFT for the Company in accordance with the requirements prescribed by RBI and modified from time to time.

3. KEY DEFINITIONS

a) "**Aadhaar Number**", as defined under sub-section (a) of Section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth 'The Aadhaar Act', means an identification number issued to an individual by

Unique Identification Authority of India (UIDAI) on receipt of the demographic information and biometric information after verifying the information in such manner as may be specified in the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

Explanation 1: In terms of the Aadhaar Act, every resident shall be eligible to obtain an Aadhaar number.

Explanation 2: Aadhaar will be the document for identity and address.

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**", as defined under sub-section (c) of section 2 of the Aadhaar Act, means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository (CIDR) for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;

d) "**Central Identities Data Repository**" (CIDR), as defined in Section 2(h) of the Aadhaar Act, means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;

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

f) "**Certified Copy**" means comparative 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.

g) "**Company**" means Espouse Capital Private Limited.

h) "**Demographic Information**", as defined in Section 2(k) of the Aadhaar Act, includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar

number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history;

i) "**Designated Director**" means Managing Director or a whole-time Director, duly authorised by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money Laundering Act and the Rules;

Explanation:

1) For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.
2) "Directors" mean individual Director or Directors on the Board of the Company.

j) "**Digital KYC**" means 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.

k) "**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.

l) "**Enrolment Number**" means "Enrolment ID" as defined in Section 2(1)(j) of the Aadhaar (Enrolment and Update) Regulation, 2016 which means a 28-digit Enrolment Identification Number allocated to residents at the time of enrolment of Aadhaar.

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

o) "**Officially Valid Document**" (OVD) means Passport, Driving License, Proof of possession of Aadhaar Number, 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, Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

"Provided also that where the client submits their proof of possession of Aadhaar number as an officially valid document, they may submit it in such form as are issued by the Unique Identification Authority of India".

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.

p) "**Principal Officer**" means an officer nominated by the Company, responsible for furnishing information as per Rule 8 of the Rules;

q) "**Suspicious Transaction**" means a "transaction", including an attempted transaction, whether or not made in cash, which, to a person acting in good faith: gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Prevention of Money laundering Act, 2002, regardless of the value involved; or appears to be made in circumstances of unusual or unjustified complexity; or appears to not have economic rationale or bona-fide purpose; or gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

r) "**Transaction**" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes: opening of an account; deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means; the use of a safety deposit box or any other form of safe deposit; entering into any fiduciary relationship; any payment made or received, in whole or in part, for any contractual or other legal obligation.

s) "**Yes/No Authentication Facility**", as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the identity information and Aadhaar number securely submitted with the consent of the Aadhaar number holder

through a requesting entity, is then matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing "Yes" or "No", along with other technical details related to the authentication transaction, but no identity information.

Terms bearing meaning assigned in this Policy, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. "**Common Reporting Standards**" (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

ii. "**Customer**" means a person who is engaged in a financial transaction or activity with a company.

iii. "**KYC Templates**" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR for individuals.

iv. "**Non-face-to-face Customers**" mean customers who open accounts without visiting the branch/offices of the Company or meeting the officials of the Company.

v. "**On-going Due Diligence**" means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

vi. "**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.

vii. "**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.

viii. "**Simplified Procedure**" means the procedure for undertaking customer due diligence in respect of customers, who are rated as low risk by the Company and who do not possess any of the six officially valid documents, with the alternate documents prescribed under the two provisos of Section 3(a)(vi) of this Directions.

ix. "**Shell Bank**" means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. KEY ELEMENTS

The objective of this KYC Policy is to prevent Espouse Capital Private Limited from being used, intentionally or unintentionally, by criminal elements for money laundering activities. Our KYC procedures will also enable the Company to know/understand its customers and their financial dealings better, which in turn will help the Company to manage its risks prudently. The Company has framed its KYC policy incorporating the following four key elements:

a) Customer Acceptance Policy;
b) Customer Identification Procedures;
c) Monitoring of Transactions; and
d) Risk Management

For the purpose of the KYC policy, a 'Customer' is defined as per Clause 3 i.e., Key Definitions.

a) Customer Acceptance Policy (CAP)

The Company shall lay down a clear Customer Acceptance Policy elucidating explicit criteria for customer acceptance. The Customer Acceptance Policy will ensure that clear guidelines are in place on the following aspects of customer relationship in the Company:

i. No account is opened in anonymous or fictitious/benami name(s);
ii. Parameters of risk perception are clearly defined in terms of the borrower's character, location, credit report, etc., to enable categorisation of customers into low, medium and high risk;
iii. CDD procedure is applied at the UCIC level. This way, if an existing KYC compliant customer wishes to avail another loan from the Company, there will be no need for a fresh CDD exercise.
iv. The Company will take care of the documentation requirements and other information to be collected from the customers depending on perceived risk and

keeping in mind the requirements of PML Act, 2002 and guidelines issued by the Reserve Bank from time to time;

v. The Company will not open an account or close an existing account where it is unable to apply appropriate customer due diligence measures i.e. it is unable to verify the identity and/or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company. It may, however, be necessary to have suitable built-in safeguards to avoid harassment of the customer. For example, decision to close an account will be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

vi. Necessary checks will be performed before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, UN Security Council List of Prohibited clients. Further, the Company will ensure that the name of the proposed clients does not appear in the consolidated list of individual and entities circulated by the RBI for such purposes.

vii. Where the Permanent Account Number (PAN) is obtained from the customer, the same will be verified from the verification facility of Income Tax Act.

viii. Where an equivalent e-document is obtained from the customer, the company will verify the digital signature as per the provisions of the Information Technology Act, 2000.

Risk Categorisation

The risk categorisation process of the Company shall be two-fold, in order to assess the risks associated with the borrowers as well as the risks associated with their employing companies.

The Company shall first assess unlisted companies incorporated in India on the basis of the factors such as the company's valuation, background of its investors, rounds of funding, business model of the company, industry, etc. On the basis of such assessment, the Company shall categorise such companies into low, medium and high-risks entities.

The second stage of risk categorisation shall include assessment of the employees of such companies based on their character, position held in their employing company, cash flow, credit rating, etc. On the basis of such parameters, the Company shall then classify the individuals into low, medium and high-risk clients.

The Company will apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence may include:

- Non-face to face customers, and
- Those with dubious reputation as per public information available.

Espouse Capital Private Limited has formulated an indicative list of customers and their respective risk categories. The same is attached as **Annexure-A** to this Policy.

b) Customer Identification Procedures

The Company's adopted Customer Identification Procedure shall be carried out at different stages, i.e. while establishing a customer relationship; carrying out a financial transaction or when the Company has doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Customer Identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. Espouse Capital Private Limited will obtain the necessary information to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship.

Being satisfied means that the Company must be able to satisfy the competent authorities like the RBI that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Besides risk perception, the nature of information/documents required will also depend on the type of customer.

Customer identification requirements in respect of a few typical cases requiring an extra element of caution are given in **Annexure-A**.

The Company will ensure that the identity of the customer is done based on disclosures by the customers themselves.

The Company will also comply with Section 11 of PML Act, 2002 to verify the identity of its customers.

An indicative list of the nature and type of documents/information that will be relied upon for customer identification are provided as **Annexure-B**.

c) Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it can identify transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Since the Company may not have any deposit accounts, this situation will not arise, but the Company shall pay special attention to depleting financial ratios, adequacy of collateral, etc. The Company will put in place a system of half-yearly review of risk categorisation of all outstanding accounts and the need for applying enhanced due diligence measures.

The Company will ensure that record of transactions in the accounts is preserved and maintained as required under Section 12 of the PML Act, 2002 and Rule 3, 4, and 5 of the PMLA Rules 2005 in a separate register at the registered office of the Company in physical or electronic form and make it available to the regulatory and investigating authorities. It will also ensure that transactions of suspicious nature and/or any other type of transaction notified under Section 12 of the PML Act, 2002, and Rules 3, 4, and 5 of the PMLA Rules, 2005 is reported to the appropriate law enforcement authority.

d) Risk Management

The Board of Directors of Espouse Capital Private Limited has ensured that an effective KYC programme is in place and established appropriate procedures, while constantly overseeing its effective implementation. The programme covers proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility has been explicitly allocated within the Company to ensure that its policies and procedures are implemented effectively. The Board of the Company has devised procedures for creating Risk Profiles of new customers and will apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or customer relationship.

The Company's internal control and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function will provide an independent evaluation of the Company's policies and procedures, including legal and regulatory requirements. Espouse Capital Private Limited will ensure that its internal control systems and machinery is staffed adequately with individuals who are well-versed in such policies and procedures or hire the services of a reputed Company engaged in providing quality services in the said field. The Company will specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard. The compliance in this regard will be presented before the Audit Committee of the Board at quarterly intervals.

The Company will have an ongoing (at regular intervals) employee training programme so that members of the staff are adequately trained in KYC procedures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers.

For Risk Management, Espouse Capital Private Limited will have a risk-based approach which includes the following:

1) Customers shall be categorised as low, medium and high-risk category, based on the assessment and risk perception of the Company.
2) Each customer will be allotted a Unique Customer Identification Code (UCIC) at the time of sanction of loan by the Company.
3) Risk categorisation shall be undertaken based on parameters such as customer's character, cash flow, credit rating, and valuation and information of the clients' employing

company, etc. Provided that 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.

5. DESIGNATED DIRECTOR

The Board of Directors in its meeting held on 17th November 2021 has appointed the following person as the "Designated Director" and the same has been duly communicated to FIU:

Name	Mr Nitin Agarwal
Designation	Director
Address	B 34, 4th Floor, Royal I Estate, Naigaon, Cross Road, Wadala, Mumbai - 400031
Contact Details	Mobile No: +91 9820041747 Email ID: nitin@esopdhan.com

6. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

a) The 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 will 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, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.

b) The risk assessment exercise 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 of the Company, in alignment with the outcome of the risk assessment exercise. However, the same shall 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 will be available to the competent authorities and self-regulating bodies.

d) The Company shall apply a Risk-Based Approach (RBA) for mitigation and management of the identified risk and have Board approved policies, controls and procedures in this regard. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

7. PRINCIPAL OFFICER

The Board in its meeting held on 17th November 2021 has duly appointed the following "Principal Officer", who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations:

Name	Shyam Shroff
Designation	Director
Address	1st Floor, Nanik Niwas, Sarojini Road, Santacruz West, Mumbai - 400054
Contact Details	Mobile No.: +91 9820020257 Email: shyam@shringar.co.in

8. CUSTOMER DUE DILIGENCE PROCEDURES ("CDD")

Procedure for Obtaining Identification Information

For undertaking CDD, the Company will obtain the information from an individual while establishing an account-based relationship.

For undertaking CDD, the company shall obtain the following from an individual while establishing an account-based relationship:

a) The Aadhaar number where,

   i. he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016;

ii. he decides to submit his Aadhaar number voluntarily to the company, notified under first proviso to sub-section (1) of section 11A of the PML Act; or

b) The proof of possession of Aadhaar number where offline verification can be carried out; or

c) The proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

d) The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income Tax Rules, 1962.

A detailed procedure to be followed by the Company is attached as **Annexure-C**.

7. RECORDS RETENTION

Records pertaining to identification of the customer and their address obtained while opening their account and during course of business relationship will be preserved accordance with the Section 12 of the PLM Act, 2002. The provision specifies for retention of records for a period of at least five years after the business relationship has ended in case of all transaction related to the individuals, or for at least five years from the date of transaction between a client and the reporting entity in case of evidencing identity of its clients.

8. REPORTING TO CENTRAL KYC REGISTRY (CKYCR)

The customer KYC information will be shared with the CKYCR in the manner mentioned in the RBI Directions in the RBI's KYC templates prepared for individuals with Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI).

Further, during periodic updation, customers' KYC details will be migrated to current Customer Due Diligence (CDD) standards.

KYC Identifier generated by CKYCR will be communicated to the Individual.

If a customer submits KYC Identifier, with explicit consent to download records from CKYCR, KYC records shall be retrieved online from CKYCR Identifier and customer will not be required to submit any KYC records unless in the following events:

a) There is a change in information of customer as existing in the records of CKYCR;
b) The current address of customer needs to be verified;
c) It is considered necessary to verify identity or address of customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

9. REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT - INDIA

Espouse Capital Private Limited shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub-Rules 3 and 4 of Rule 7, Director, FIU-IND shall have powers to issue guidelines for detecting transactions referred to in various clauses of sub-Rule (1) of Rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

The reporting formats and comprehensive reporting format guide prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by the Company if it has not installed/adopted suitable technological tools for extracting CTR/STR from its live transaction data.

The Company's Principal Officers, whose all branches are not fully computerised, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Company shall not put any restriction on operations in the accounts where an STR has been filed. The Company shall

keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

However, robust software sending out alerts when the transactions are inconsistent with risk categorisation and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

ANNEXURE-A

Indicative List for Risk Categorisation

Low-Risk Entities	Medium-Risk Entities	High-Risk Entities
Unlisted Companies: • With business valuation of more than $500 million as on date. • With high probability of getting listed on a recognised Stock Exchange in India within the next 2 years. • With multiple funding / venture capital investment rounds.	Unlisted Companies: • With projected business valuation of more than $500 million. • With medium to low probability of getting listed on a recognised Stock Exchange in India within the next 3 years. • With fewer funding / venture capital investment rounds.	Unlisted Companies: • With no possibility of getting listed on a recognised Stock Exchange in India within the next 3 years.

Low-Risk Customers	Medium-Risk Customers	High-Risk Customers
Salaried Employees: • Whose salary structure is well-defined. • Who are employed with low-risk unlisted companies with valuation above $500 million.	• High Net Worth Individuals (HNWIs)	• Individuals with dubious reputation as per public information available or commercially available watch lists. • Non-face-to-face customers. • Customers who are close relatives of PEPs.

		• Individuals specifically identified by regulators, FIU and other competent authorities as high-risk.

ANNEXURE-B

List of KYC Documents for Customers

A. Permanent Account Number (with photo and signature) or Form 60.

B. One certified copy of an Officially Valid Document (OVD") containing details of the borrower's identity for legal name, and any other names used and address:

- Proof of possession of Aadhaar number in such form as are issued by the Unique Identification Authority of India
- Valid Indian Passport (with photo and signature)
- Valid Voter's ID card issued by the Election Commission of India
- Valid Permanent Driving License (with photo and signature)
- Letter issued by the National Population Register containing details of name and address.

In case of OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVD for limited purpose of proof of address:

- Bank Account Statement
- Letter from any recognised public authority
- Utility Bill not more than two months old (electricity, telephone, post-paid mobile phone, piped gas, water bill) of any service provider
- Property or Municipal tax receipt

A copy of the borrower's marriage certificate issued by the State Government or Gazette notification representing the change in name of the borrower along with a certified copy of the OVD in the existing name of the person shall be obtained for proof of address and identity to establish an account-based relationship or to periodically update records in case the borrower change their names on account of marriage or otherwise.

The following documents may be obtained in addition to OVD subject to the satisfaction of the Company:

1. Property (including land) registration document containing photograph, name, signature and address.
2. Letter from employer (subject to satisfaction of the Company).

Signature Proof:

1. Valid Indian Passport
2. Valid PAN card
3. Valid Permanent Driving license
4. Banker's letter/ verification letter/ ECS verification in original on Bank's letter head bearing the authorising officer's name and signature along with the stamp of the bank. In case the Bank refuses to give the signature verification on the Bank's letter head, then Signature/ ECS verification shall be obtained in the format prescribed for the said purpose.
5. Property registration document containing photograph, name, signature and address

ANNEXURE-C

Procedure for Obtaining Identification Information for Undertaking CDD

The Company shall obtain the following information from an individual while establishing an account-based relationship:

a) From an individual who is eligible for enrolment of Aadhaar, the Aadhaar number; the Permanent Account Number (PAN) or the equivalent e-document thereof or Form No. 60 as defined in Income Tax Rules, 1962, as amended from time to time, the proof of possession of Aadhaar number where offline verification can be carried out or not; and such other documents including in respect of the nature of business and financial status of the client, or the equivalent e-documents thereof as may be required by the Company.

   Provided, where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an OVD or the equivalent e-document thereof containing details of identity and address and one recent photograph shall be obtained.

   Provided that where the customer has submitted:

   a) Aadhaar number as mentioned above to the Company, the Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.
   b) Proof of possession of Aadhaar where offline verification can be carried out, the Company shall carry out offline verification.
   c) Equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and any rules issued there under and take a live photo as specified under Annex I of the Master Direction.
   d) Proof of possession of Aadhaar number where offline verification cannot be carried out, the Company shall carry out verification through an application developed by the Company for this purpose.

"Explanation- Obtaining a certified copy by reporting entity shall mean comparing the copy of officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the reporting entity"

Provided further, that from an individual, who is not a resident or is a resident in the State of Jammu and Kashmir or Assam or Meghalaya, and does not submit the Permanent Account Number where its client submits his Aadhaar number, ensure such client to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15).

Provided that in case the OVD submitted 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 2: Customers, at their option, shall submit one of the five OVDs.

Explanation 3: Equivalent e-document has also been permitted for accounts of non-individual customer.

b) In case the identity information relating to the Aadhaar number or Permanent Account Number submitted by the customer does not have current address, an OVD as defined in Section 3(p) shall be obtained from the customer for this purpose.

"Provided that in case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:

a. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
b. Property or Municipal tax receipt;
c. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
d. 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:

Provided that the client shall submit updated officially valid document with current address within a period of three months of submitting the above documents."

c) The Company, at the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication.

Provided:

i. Yes/No authentication shall not be carried out while establishing an account-based relationship.
ii. In case of existing accounts where Yes/No authentication is carried out, the Company shall ensure to carry out biometric or OTP based e-KYC authentication within a period of six months after carrying out yes/no authentication.
iii. Where OTP based authentication is performed in 'non-face to face' mode for opening new accounts, the limitations as specified in Section 17 shall be applied.
iv. Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators/ Biometric enabled ATMs.

Explanation 1: While seeking explicit consent of the customer, the consent provisions as specified in Section 5 and 6 of the Aadhaar (Authentication) Regulations, 2016, shall be observed.

Explanation 2: The Company shall allow the authentication to be done at any of its branches.

d) The customer shall submit Permanent Account Number or Form No. 60, referred to in Section 15(a) above, the Permanent Account Number/ Form 60 at the time of commencement of an account-based relationship with the Company, the Customer shall submit the same within a period of six months from the date of the commencement of the account-based relationship. In case the customer fails to submit Permanent Account Number/Form 60 within the

aforesaid six months period, the said account shall cease to be operational till the time Permanent Account Number/ Form 60 is submitted by the customer.

Explanation: In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

e) The Company shall duly inform the customer about this provision while opening the account.

f) The customer, shall submit the Permanent Account Number, except one who is a not a resident or resident in the State of Jammu and Kashmir or Assam or Meghalaya, already having an account based relationship with the Company, shall submit his Permanent Account Number or Form No.60, on such date as may be notified by the Central Government, failing which the account shall temporarily cease to be operational till the time the Permanent Account Number or Form No. 60 is submitted by the client:

Provided that before temporarily ceasing operations for an account, the reporting entity shall give the client an accessible notice and a reasonable opportunity to be heard.

Explanation– For the purpose of this clause, "temporary ceasing of operations" in relation an account means the temporary suspension of all transactions or activities in relation to that account by the reporting entity till such time the client complies with the provisions of this clause;

g) If a client has an existing account based relationship with a reporting entity, gives in writing to the reporting entity that he does not want to submit his Permanent Account Number or Form No.60, as the case may be, the client's account with the reporting entity shall be closed and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the client in the manner as may be determined by the regulator.
Provided that the Company shall serve a notice for the compliance before such date.

h) The Company shall ensure that introduction is not to be sought while opening accounts.

i) Lastly, in case where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature. Further, the account shall remain operational only on annual submission of certificate of proof of address issued by the officer in-charge of the jail.

ANNEXURE-D

DIGITAL KYC PROCESS

a) A Digital KYC Application (KYC App) for digital KYC process will be made available at customer touch points and undertaken only through the authenticated application of the Company.

b) Access of the KYC App will be controlled and it will be ensured that it is not used by any unauthorised person.

c) KYC App will be accessed only through Login-ID and Password, Live OTP or Time OTP controlled mechanism given to the authorized officials of the Company

d) Customer, for KYC, will follow a digital journey in the backend of high secured KYC App platform, including face scanning PAN/Aadhaar verification and penny-drop bank account verification.

e) KYC App will have a water-mark in readable form having CAF number, GPS coordinates, authorised official's name, unique employee Code and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

f) KYC App will have a feature such that only live photograph of the customer is captured and not printed or video-graphed photograph.

g) Background behind the customer must be white and no other person must come into frame

h) Live photograph of original OVD or proof of possession of Aadhaar (if offline verification is not being done) placed horizontally, will be captured vertically from above and water-marking as stated above will be done. No skew or tilt in the mobile device will be there while capturing the live photograph of the original documents.

i) Live photograph of customer and original documents will be captured in proper light so that they are clearly readable and identifiable.

j) All the entries in the CAF will be made as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details will be auto-populated by scanning the QR code instead of manual filing the details.

k) 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' will be

sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF.

l) In case, the customer does not have his/her own mobile number, mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF.

m) In any case, the mobile number of authorised officer registered with the Company will not be used for customer signature.

n) It must be verified that mobile number used in customer signature is not mobile number of authorized officer.

o) Authorized officer will provide a declaration about capturing live photograph of customer and original document. For this purpose, authorised official will be verified with OTP sent to the mobile number registered with the Company. This OTP validation is to be treated as authorized officer's signature on the declaration. Live photograph of authorized official will also be captured in the authorized officer's declaration.

p) Subsequent to all these activities, the KYC App will give information about the completion of the process and submission of activation request to an activation officer of the Company, and also generate transaction-ID/reference-ID number of the process. Authorized officer will intimate the details regarding transaction-ID/reference-ID number to customer for future reference.

q) Authorized officer of the Company will also verify that

   a. The information available in picture of document is matching with information entered in CAF.

   b. The live photograph of the customer matches with the photo available in the document.

   c. All the necessary details in CAF including mandatory fields are filled properly.

r) On Successful verification, the CAF will be digitally signed by authorized officer of the Company and the print of CAF will bear signatures/thumb-impression of customer at appropriate place.

s) The signed document will be scanned and uploaded in system and the original hard copy will be returned to the customer.