

KNOW YOUR CUSTOMER (“KYC”) AND
ANTI MONEY LAUNDERING (“AML”) POLICY

VERSION CONTROL

Version	Creation / Updation Date	Effective Date	Description of the Version
1.0	17 August 2018	20 August 2018	New document
2.0	25 Feb2019	26Feb2019	Revised document
3.0	15 June 2021	17 June 2021	Revised document

INDEX

Preamble.....	4
Part 1 : (a) Abbreviations used and their meaning statutory/regulatory or otherwise.....	5
Part 1 : (b) Definitions used in the Policy.....	6
Part 2 : The Company's KYC/AML policy.....	11
A. Background.....	11
B. Policy Review.....	11
C. Policy Objectives.....	11
D. Scope and Applicability.....	12
E. Key Elements.....	12
i. Customer Acceptance Criteria/Policy ("CAP").....	12
ii. Customer Identification Procedures ("CIP").....	13
iii. Risk management.....	17
iv. Monitoring of Transactions.....	19
F. Ongoing due diligences.....	19
G. Identification of beneficial owner.....	19
H. Training Program.....	19
I. Internal Control System.....	19
J. Record Management.....	19
K. Reporting to Financial Intelligence Unit- India.....	21
L. General.....	21
i. Introduction to new technologies.....	21
ii. Applicability to Branches and Subsidiaries outside India.....	21
iii. Closure of Accounts/Termination of Financing/Business Relationship.....	21
iv. KYC for Existing Accounts.....	21
v. Miscellaneous Issues.....	21
vi. Updating KYC Policy of company.....	22
Part III Annexures.....	23
Annex 1 CUSTOMER IDENTIFICATION REQUIREMENTS (INDICATIVE GUIDELINES).....	23
Annex 2 ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTION PERTAINING TO FINANCIAL SERVICES.....	24

Know Your Customer/Anti Money Laundering Policy

Preamble:

1. Financial Action Task Force (FATF) is an inter-governmental global policy making body, established in 1989 to set standards and promote 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. It has developed a series of recommendations that are recognised as international standard. FATF issued a revised Guidance in 2017 reinforcing the risk-based approach (RBA), as an underlying principle of all AML/CFT systems.
2. Government of India as a member of this body, legislated the Prevention of Money Laundering Act, 2002, with RBI as implementing agency. All Non-banking Financial Companies (NBFCs) were covered under PMLA through an amendment in 2005, and the Rules for maintenance of records.
3. Section (3) of The Prevention of Money Laundering Act, 2002, hereinafter referred to as PMLA as amended up to date provides for stringent punishment for the offence of money-laundering and defines it in a broad and inclusive manner thus:

“Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering.”
4. The wording of the Act and RBI’s regulatory directions amended latest on May 10, 2021, leave no room for complacency in this vital area of a financial institution’s operations. Kashi Capital Private Limited (hereinafter referred to as “the Company”), despite its focused customer segmentation and stringent screening procedures, recognizes its susceptibility to such risks in its operations. The Company recognizes that a good corporate citizenship is achieved proactively through adopting a transparent and effective compliance strategy, while keeping the business strategy in view.
5. Clear understanding of the customers it is dealing with makes good business sense. Also, the need for integrating into its business practices - translated through operational procedures - appropriate measures to prevent the use of the Company for money laundering both as a reputation risk management strategy and a compliance endeavour cannot be overemphasized.
6. The Company also recognizes the imperative of the integration of the relevant statutory and regulatory expectations of reporting, maintaining and making availability of the relevant documents to relevant authorities into the operational business processes of customer identification, verification and on-going monitoring of transactions.
7. The Company is conscious of the risk profile of its target market segments, that are predominantly underprivileged/underserved but with great business potential. In order not to deny this segment financial access, which is a part of the Company’s mission of “wisely nurturing growth” while remaining compliant, endeavour shall be in providing appropriate training in technology and banking habits. The Company shall implement proportional operational initiatives to adhere to the stringent regulations with its limited resources at present in tune with the customer risk profile.
8. The Company recognizes that training its employees in this vital endeavour constitutes not only a key element of sustainable business strategy, but also as a compliance requirement.
9. This document, enumerating its KYC/AML Policy stance, is issued in this background, structured as:

Part I : (a) Abbreviations used and their meaning statutory/regulatory or otherwise; and

(b) Definitions used in the policy.

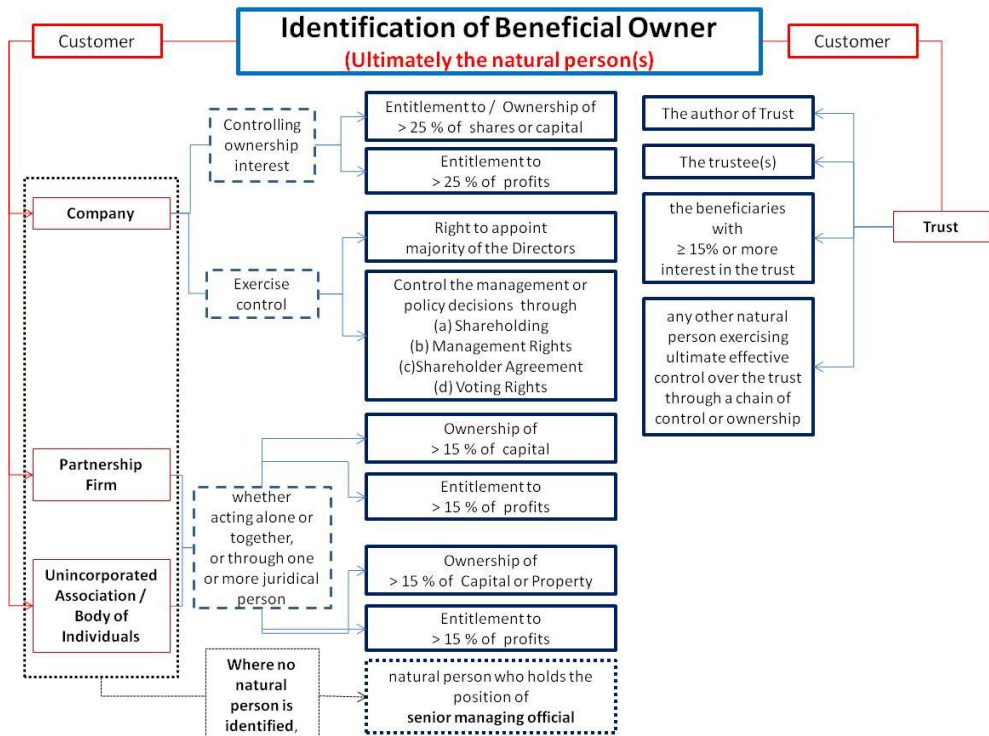
Part II : The Company’s KYC/AML policy framework; and

Part III: Annexures

No.	Abbreviation	Description
1	AAR	Aadhaar Authentication Rules,2016
2	AML	Anti-Money Laundering
3	BO	Beneficial Owner
4	BoI / BoP / Aop	Body of Individuals / Body of Persons /Association of Persons
5	CAP	Customer Acceptance Policy
6	CDD	Customer Due Diligence
7	CERSAI	Central Registry of Securitization Asset Reconstruction and Security Interest of India
8	CFT	Countering Financing Terrorism
9	CIDR	Central Identities Data Repository
10	CIP	Customer Identification Procedures
11	CKYCR	Central Know Your Customer Registry
12	CRS	Common Reporting Standards
13	CST	Central Sales Tax
14	CTR	Cash Transaction Report
15	DD	Designated Director
16	DGFT	Director General of Foreign Trade
17	ECS	Electronic Clearing System
18	EDD	Enhanced Due Diligence
19	e-KYC	electronic-Know Your Customer
20	FATCA	Foreign Account Tax Compliance Act
21	FATF	Financial Action Task Force
22	FIU-India	Financial Intelligence Unit-India
23	GST	General Sales Tax
24	IA	Internal Audit
25	ID	Identification Document
26	IEC	Importer Exporter Code
27	IGA	Inter Government Agreement
28	IMPS	Immediate Payment System
29	IRM	Integrated Risk Management
30	KYC	Know Your Customer
31	KYCD	Know Your Customer Directive, 2016
32	MoT	Monitoring of Transactions
33	NBFC	Non-banking Financial Company
34	NEFT	National Electronic Funds Transfer
35	NPO	Non-Profit Organization
36	NREGA	National Rural Employment Guarantee
37	ODD	Ongoing Due Diligence
38	OTP	Onetime Password
39	OVD	Officially Valid Document
40	PAN	Permanent Account Number
41	PEP	Politically Exposed Persons
42	PML (MoR)	Prevention of Money Laundering (Maintenance of Records) Rules, 2005
43	PMLA	Prevention of Money Laundering Act, 2002
44	PO	Principal Officer
45	RE	Regulated Entities
46	RM	Risk Management
47	RTGS	RealTime Gross Settlement
48	SA	Small Account
49	SDD	Simplified Due Diligence
50	SEBI	Securities Exchange Board of India

51	STR	Suspicious Transaction Report
52	UCIC	Unique Customer Identification Code
53	TDFOSBSA	(Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, The Aadhaar Act
54	UIDAI	Unique Identification Development Authority of India
55	VAT	Value Added Tax

Part I: (b) Definitions used in the Policy:

No.	Term	Meaning/Definition
1	Aadhaar number	An identification number issued to an individual by UIDAI on receipt of the demographic information and biometric information, to a resident Indian constituting a OVD for identity and address. (as per the provisions of the clause (a) of section 2 of Aadhaar Act, 2016)
2	“Act” and “Rules”	PMLA, 2002 and the PML (MoR) Rules, 2005, respectively and amendments thereto.
3	Authentication	in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar Act 2016
4	Beneficial Owner	The ultimate natural person who controls the relevant business organisation or association of persons including Societies and Trusts. Please refer to Figure 1. Figure 1 Identification of Beneficial Owner
		
5	Biometric information	Includes photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by AAR, 2016 (as defined in the Section 2(g) of the Aadhaar Act)
6	Central Identities Data Repository”	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, (as defined in Section 2(h) of the Aadhaar Act)
7	Central KYC Records Registry	An entity to receive, store, safeguard and retrieve the KYC records in digital form of a customer. (as defined under Rule 2(1)(a) of the AAR,2016)

No.	Term	Meaning/Definition
8	Certified Copy	Obtaining a certified copy by the RE 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 RE as per the provisions contained in the Act
9	Customer	means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
10	Customer Due Diligence (CDD)	means identifying and verifying the customer and the beneficial owner.
11	Customer identification	means undertaking the process of CDD
12	Demographic information	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; (as defined in Section 2(k) of the Aadhaar Act.)
13	Designated Director	A person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules. Explanation: 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. The name, designation and address of the Designated Director shall be communicated to the FIU-IND. In no case, the Principal Officer shall be nominated as the 'Designated Director'.
14	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 RE as per the provisions contained in the Act.
15	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).
16	Enrolment number	Enrolment ID is a 28 digit Enrolment Identification Number allocated to residents at the time of enrolment of Aadhaar. (as defined in Section 2(1)(j) of the Aadhaar (Enrolment and Update) Regulation, 2016)
17	e-KYC authentication facility	A type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction; (as defined in Aadhaar (Authentication) Regulations, 2016)
18	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
19	Identity information	In respect of an individual, includes individual's Aadhaar number, biometric information and demographic information; (as defined in sub-section (n) of section 2 of the Aadhaar Act)
20	Officially Valid Document (OVD)	<ol style="list-style-type: none"> 1. the passport, 2. the driving licence, 3. the Voter's Identity Card issued by the Election Commission of India, 4. job card issued by NREGA duly signed by an officer of the State Government, 5. letter issued by the National Population Register containing details of name and address.

No.	Term	Meaning/Definition
		<p>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:-</p> <ul style="list-style-type: none"> 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 licence agreements with such employers allotting official accommodation; <p>c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified above</p> <p>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.</p> <p>Explanation 1.- 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>
21	Person	<ul style="list-style-type: none"> a. an individual, b. a Hindu undivided family, c. a company, d. a firm, e. an association of persons or a body of individuals, whether incorporated or not, f. every artificial juridical person, not falling within any one of the above persons (a to e), and g. any agency, office or branch owned or controlled by any of the above persons (a to f).
22	Principal Officer	<p>An officer nominated by the RE, responsible for compliance, monitoring transactions, and sharing and reporting information as per rule 8 of the Rules. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.</p>
23	Resident	<p>an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment for Aadhaar;</p> <p>(as defined under sub-section (v) of section 2 of the Aadhaar Act)</p>
24	Suspicious transaction	<ul style="list-style-type: none"> a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or b. appears to be made in circumstances of unusual or unjustified complexity; or c. appears to not have economic rationale or bona-fide purpose; or d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism. <p>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.</p>
25	Transaction	<ul style="list-style-type: none"> a. opening of an account; b. 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;

No.	Term	Meaning/Definition
		<p>c. the use of a safety deposit box or any other form of safe deposit;</p> <p>d. entering into any fiduciary relationship;</p> <p>e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or</p> <p>f. establishing or creating a legal person or legal arrangement.</p>
26	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
27	Yes/No authentication facility	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. (as defined in Aadhaar (Authentication) Regulations, 2016)
28	Customer	A person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
29	Walk-in Customer	A person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.
30	Customer Due Diligence	Identifying and verifying the customer and the beneficial owner using “Officially Valid Documents” as a “Proof of Identity” and “Proof of Address”.
31	Customer identification	Undertaking the process of CDD.
32	FATCA	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. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.
33	KYC Templates	Templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
34	Non-face-to-face customers	Customers who open accounts without visiting the branch/offices of the RE or meeting the officials of RE.
35	On-going Due Diligence	Regular monitoring of transactions in accounts to ensure that they are consistent with the customers’ profile and source of funds.
36	Periodic Updating	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.
37	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.
38	Shell bank	A bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.
39	Wire transfer	A transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

No.	Term	Meaning/Definition
40	Domestic and cross-border wire transfer	When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.

Part II : The Company's KYC/AML policy framework

Know Your Customer/Anti Money Laundering Policy

A. Background:

1. In terms of the powers vested in it as implementing agency under the Prevention of Money Laundering Act, 2002, as amended from time to time, the Reserve Bank of India had issued directions under Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016, vide RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 DATED February 25, 2016 (Updated as on May 10, 2021). The regulatory context is indicated in the said direction as follows: -

“In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, 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. REs shall take steps to implement provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).”

2. Kashi Capital Private Limited (Kashi Capital or the company) is a private limited company incorporated under Companies Act, 2013 and registered with the Reserve Bank of India. The Company primary business is lending to individuals, non-individuals and businesses in both the unorganized and organized sector of the economy. Our customers use the money to expand their MSME businesses, to further diversify their business units/self-employed professions and meeting other personal expenses / financial needs. The provisions of the above Directions apply to the Company as a regulated entity specifically defined under paragraph 3 (b) (xiii) (c) of these directions.
3. The policy is set in the context of the Company's business strategy covering the target markets, simple loan products, geographic cohesion and above all, the profile of targeted customers mostly from underserved communities in Hindi heartland states. The nature of the Company's business strategy encourages small loans to economically weaker sections of customers in the Hindi heartland based on customer identification that predominantly relies on information in public domain through institutional mechanisms and disclosed voluntarily and verified during field visits on face to face interaction in the branches/offices and at place of business. Protecting the business and regulatory interests is embedded in the operational processes of the Company in selection, appraisal, reporting, monitoring and follow-up aspects of the company's lending function.
4. To guidelines under the PMLA and RBI's Master Direction on KYC/AML, the Company has appointed a Principal Officer. The current "Principal Officer" is Mr. Biplab Paul. ensure overall compliance with the obligations imposed under Chapter IV of the PML Act 2002, the "Designated Director" will be Mr. Rohit Kumar Singh.
5. From an organizational context for ensuring compliance to monitor the transactions and sharing and reporting information under regulatory
6. In summary, at the heart of KYC compliance is the identification of beneficial owner, who invariably is/natural person(s), through an appropriate and effective customer due diligence process and monitoring of transactions on an ongoing basis to prevent the Company being used for money laundering.

B. Policy Review:

7. This policy is a living document to be reviewed once in two years or at shorter intervals as warranted by the prevalent business/compliance environment/elements.
8. Whenever a need arises for a review of this Policy, the initiator shall approach the Principal Officer with a request, copying the same to the Designated Director and submit relevant information/data for the expected decision. All amendments shall be referred to the Risk Management Committee/Audit Committee for their concurrence before the amendments are recommended by the relevant Committee for approval of the Board of Directors.

C. Policy Objectives:

9. In the context of the foregoing, the "Know Your Customer Policy" (hereinafter referred to in this policy as "KYC Policy") of the Company is framed. The broad objectives of the policy are to:-
 - (i) Prevent the use of the Company or its resources as a vehicle for money laundering by a better understanding of its customers, their business and social standing;
 - (ii) Put in place an organization structure that ensures compliance with relevant regulatory requirements including:

- a. Designation of a Principal Officer;
 - b. Definition of Senior Management for the purposes of compliance with statutory and regulatory provisions;
 - c. Allocation of responsibilities for compliance of and reporting to various levels of management;
 - d. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures;
 - e. Ensuring integrity of KYC/AML compliance through reporting to Board, audit and independent review;
- (iii) Put in place preventive measures including:
- f. Customer Acceptance Policy including the elements of KYC tenets in the business policy/strategy;
 - g. Customer Identification Procedures;
 - h. Monitoring of transactions;
 - i. Risk Management through categorization of customers based on prescribed regulatory criteria;
- (iv) Provide guidelines on the identification of beneficial owners through structured processes through non-intrusive means to elicit reliable customer data for a prudent approach towards lending.
- (v) The guideline also mandates making reasonable effort 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.
- (vi) Put in place a monitoring and reporting mechanism for preventing the Company from being used for money-laundering including:
- a. Designate a Director as required under Para (4) of the KYCD, 2016 of RBI.
 - b. Defining "Senior Management" for reporting compliance with provisions of PML Act and Rules and relevant RBI Directions;
 - c. Designate a "Principal Officer" for ensuring reporting of transactions to appropriate authorities.
- (vii) business decision making, effective risk management and meet compliance requirements;
- (viii) Provide guidelines in line with the regulatory guidelines and statutory requirements for aligning the operational level implementation of the business strategy in alignment with KYC Policy.

D. Scope and Applicability:

10. The KYC Policy shall be applicable across the Company, i.e. in all branches and administrative/registered offices, wherever there are customer dealings in any mode.
11. These guidelines are applicable to walk-in customers as well as non-face-to-face customer dealings.
12. These guidelines are not intended to deprive legitimate aspirants for credit because of their inability to produce officially valid documents for their identification. Alternate documented process of customer due diligence shall be adopted by the operating management, but subject to reporting and approval of Senior Management/ Chief Operating Officer/ Managing Director/Chief Executive Officer/Executive Chairman.

E. Key Elements:

Policy Components:

13. The KYC policy, both as an effective risk management measure and regulatory compliance, incorporates the following elements: -
 - i. Customer Acceptance Criteria/Policy ("CAP");
 - ii. Customer Identification Procedures ("CIP");
 - iii. Risk management; and
 - iv. Monitoring of Transactions.

i. Customer Acceptance Criteria/Policy ("CAP"):

14. Before establishing an account relationship, the customers shall be classified depending upon their constitution as natural person(s) or legal entity(ies), to facilitate compliance with this policy and the RBI directions on the subject.
15. The customer identification process shall comprise the obtaining and verification of the documents that establish the identity and address of the natural persons who are the beneficial owners.
16. The focus of the process shall be to assess the beneficial owners as indicated in term 4 "Beneficial owner" under table "Part 1: (b) Definitions used in the Policy".
17. The Company shall carry out full scale customer due diligence (CDD) before opening an account. When the true identity of the account holder is not known, the Company shall file Suspicious Transaction Reporting ("STR").

No account shall be opened in fictitious/anonymous/benami names or where the company is unable to do customer due diligence either on account of non-cooperation of the customer or non-reliability of the documents/ information given by customer.

18. CDD Procedure is followed for all the joint account holders, while opening a joint account.
19. REs shall apply the CDD procedure at the UCIC (Unique Customer Identification Code) level. Thus, if an existing KYC compliant customer of a RE desires to open another account with the same RE, there shall be no need for a fresh CDD exercise.
20. Based on the RBI Master Directions, Customer Acceptance Policy shall not result in denial of financial facility to members of the general public, especially 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.

ii. Customer Identification Procedure (“CIP”):

21. 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 person. The Company shall obtain enough information necessary to establish the identity of each customer and the purpose of the intended nature of business relationship. The Company believes that CIP is an important aspect of knowing its customers and will be undertaken on the commencement of a loan account opening for a customer. Hence 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)
22. The operating management shall certify the documentation after comparison with the originals that the documentation in respect of the identity and address of the customer have been obtained and verified physically with specific reference to compliance with KYC policy, in accordance with credit acquisition/appraisal processes while forwarding the credit proposal of the prospective borrowers.
23. No credit approval shall be accorded until the confirmation of certification with regard to the customer identification process has been obtained from the relevant operating management executive.
24. Any and all exceptions, if at all granted, shall be permitted only by the Managing Director/Head of the Credit Risk, recording in writing, the reasons and circumstances under which such exceptions were necessitated/permitted. Such permissions shall be placed to the Board for their review, in a consolidated manner at quarterly intervals.
25. In all such cases, the customer identification procedures shall be completed within a week from the date of such grant of exception, in any case within the lower of seven days or before the disbursement of loan with compliance being reported to the authority permitting such exceptions and the Principal Officer. Indicative guidelines for Customer Identification requirements are given in annexure I.
26. In cases where the customer is unable to produce an OVD to the satisfaction of the Company, alternate methods of customer identification to the satisfaction of Senior Management may be adopted, subject to a review of the customer due diligence process within 30 days. All such customers shall be put under High Risk category and shall be under enhanced due diligence, for at least -2- loan cycles completed.

Customer Due Diligence (“CDD) Procedure

The Company shall take reasonable measures to verify the true identity of all customers who transact with the Company. The Company shall design and implement specific due diligence standards and procedures that are appropriate given the respective nature of the businesses, customers and associated risks. While establishing an account-based relationship, the following due diligence procedure shall be adhered, depending upon the type of customer with whom such relationship is being established: These procedures would include a) Identification b) Verification and C) Resolution of Discrepancy.

a) Identification: Depending on the type of customer the following documents would be required for identification and proof of address

Customers/Clients	Self-Attested Document
Individuals (Applicant/ Co – Applicant) - Proof of Identity and Address	1. **Eligible for Enrolment of Aadhaar and the customer has enrolled: a. Where an Aadhaar number has been assigned; <ul style="list-style-type: none"> • Aadhaar number; • One Recent photograph; and

	<ul style="list-style-type: none"> • Either <ul style="list-style-type: none"> ▪ Permanent Account Number (PAN) or ▪ Form No. 60 <p>b. Where an Aadhaar number has not been assigned:</p> <ul style="list-style-type: none"> • Proof of application for enrolment within preceding -6- (six) months; and • Either <ul style="list-style-type: none"> ▪ Permanent Account Number (PAN) ▪ or ▪ Form No. 60; and ▪ Certified copy of an OVD containing details of identity and address; and ▪ One recent photograph. <p>2. Individuals not producing Aadhaar – Persons from Jammu & Kashmir/Meghalaya</p> <ul style="list-style-type: none"> • Certified copy of an OVD containing details of identity and address; and • One recent photograph. <p>3. Individuals Not Eligible for Enrolment of Aadhaar and Non-residents:</p> <ul style="list-style-type: none"> • Either <ul style="list-style-type: none"> ▪ Permanent Account No. (PAN); or ▪ Form 60; • One recent photograph; and • Certified copy of an OVD containing details of identity and address; • A declaration that the individual is not eligible for Aadhaar. <p>In case the identity information relating to Aadhar number or Permanent Account number submitted by customer does not have current address, one or more of the following an OVD(Officially Valid Document) shall be obtained by customer for this purpose :</p> <ol style="list-style-type: none"> i. *Passport; ii. Driving License; iii. Voter Identity Card Issued by the Election Commission of India; iv. Job Card issued by NREGA duly signed by an officer of the State Government; <p>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 limited purpose of proof of address:</p> <ol style="list-style-type: none"> i. Utility Bill (Not more than -2- (two) months old of any service provider: <ul style="list-style-type: none"> ▪ Electricity;
--	---

	<ul style="list-style-type: none"> ▪ Telephone; ▪ Piped Gas; ▪ Water Bill; <p>ii. Property or Municipal Tax Receipt;</p> <p>iii. Pension Payment or Family Pension Payment Orders (PPO) issued to employees of Government Employees or Public Sector Undertakings, if they contain the address.</p> <p>iv. Letter of allotment of accommodation or Leave and licence agreement to employees issued by State/Central Government Departments, statutory/regulatory bodies, Public Sector Undertakings, Scheduled Commercial Banks, Financial Institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.</p> <p>Provided further that customer shall submit Aadhaar or OVD with current address within a period of 3 months of submitting the above documents.</p> <p>*Compulsory in case of Non-Resident Individuals. ** Where a customer eligible for Aadhaar enrolment and the Permanent Account Number fails to submit the Aadhaar number/PAN within six months from the date of establishing account-based relationship, only credits into the account shall be allowed till the time Aadhaar number and PAN/Form 60 is submitted by the customer.</p> <p>Note: An OVD with a changed name supported by a marriage certificate issued by the State Government or Gazette Notification indicating name change after marriage shall be accepted as identity document.</p>
<p>Accounts of Companies</p> <ul style="list-style-type: none"> – Name of the company. – Principal place of business. – Mailing address of the company. – Telephone/Fax Number. 	<ul style="list-style-type: none"> • Certificate of incorporation and Memorandum & Articles of Association; • Resolution of the board of directors to open an account and identification of those who have authority to operate the account; • Power of attorney granted to its managers, officers or employees to transact business on its behalf; • An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf; • Copy of PAN allotment letter; • Copy of telephone bill;
<p>Accounts of Partnership Firms</p>	<ul style="list-style-type: none"> • Registration certificate, if registered; • Partnership deed; • Power of attorney granted to a partner or an employee of the firm to transact business on its behalf; • Any officially valid document identifying the partners and the persons holding the power of attorney and addressees; • Telephone bill in the name of firm/partners.

Accounts of Trusts and foundations – Names of trustees, settlers, beneficiaries and signatories.	<ul style="list-style-type: none"> • Certificate of registration, if registered; • Trust deed; • Power of attorney granted to transact business on its behalf; • Any officially valid document to identify the trustees, settlers, beneficiaries and those holding power of attorney, founders/managers/directors and their addresses; • Resolution of the managing body of the foundation/association; • Telephone bill
Accounts of unincorporated association or a body of individuals	<ul style="list-style-type: none"> • Resolution of the managing body of such association or body of individuals; • Power of attorney granted to him to transact on its behalf; • An officially valid document in respect of the person holding an attorney to transact on its behalf and such other information as may be required by company to collectively establish the legal existence of such an association or body of individuals.
Accounts of Proprietorship concerns Proof of the name, address and activity of the concern	<p>Apart from customer identification procedure as applicable to the proprietor any two of the following documents in the name of the proprietary concern would suffice</p> <ul style="list-style-type: none"> • Registration certificate (in case of a registered concern) • Certificate/licence issued by the municipal authorities under shop & establishment act • Sales and income tax returns • GST certificate • 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/Licence/certificate of practice issued in name pf the proprietary concern by any professional body incorporated under a statute. • The 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. <p>In case where the company is satisfied that it is not possible to furnish two such documents, it would have the discretion to accept only one of those documents as activity proof. In such cases, the company however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.</p>

The company may go for offline verification mode for Aadhaar, as per extant rules and regulations. The company may avail services of Business Correspondent (BC) for the same. However, the same will be in line with the RBI Master Circular on KYC guidelines. Alternatively the verification through “Digital KYC” – introduced by RBI in 2016 and with subsequent amendments to the Master Directions 2016, the customer identity can be verified through capturing a live photo of the customer and officially valid document where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is taken by the authorised officer of the RE as per the provisions contained in the master circular

b) Verification: The company will ensure that verification of customer identity should occur before transacting with the customer. The acceptable methods of verification of customer identity may include verification through

documents and/or non-documentary verification methods that are appropriate given the nature of the business and its associated risks.

b1. Verification through documents: 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. The company representative shall compare the certified copy of OVD document collected with the original and record the same on the copy.

b2. Verification through non-documentary methods: These methods may include, but are not limited to:

b2.1. Visiting or contacting a customer:

b2.2. 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 independent sources

b2.3. Checking references with other financial institutions: or

b2.4. Obtaining a financial statement.

If a full KYC verification is done by a branch, head office or regional office and is not due for a periodic updation for an account: then it is valid for a transfer to another branch/office or the company. Verification can also be done via Digital KYC - the customer identity can be verified through capturing a live photo of the customer and officially valid document where offline verification cannot be carried out, along with longitude and latitude of the location where such live photo is taken by the authorized officer of the RE as per the provisions contained in the master circular.

3.Resolution of Discrepancies:

If there are information discrepancy amongst documents regarding true identity, the company will try to resolve the same through available means. If the issue is not resolved the company may decline doing business with the customer.

Enhanced Due Diligence ("EDD) Procedure

Kashi Capital Is primarily engaged in funding micro and small businesses with a special focus on unregistered / unbanked / underbanked customers. Typically, the profile of the customers that we serve are not of potential high risk of political corruption, money laundering, or terrorist financing. As a thumb-rule we do not typically transact with such high-risk customers. However, if during the credit appraisal process we find a person or business to be potentially high risk then the company shall conduct Enhanced Due Diligence which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence.

iii. Risk Management:

27. For the purposes of this Policy, the Company's customers shall be categorized into ascending stages of risk level .The risk categories shall generally and broadly be based on perceived/prescribed levels of risk, evaluated on parameters, inter alia, the customer identity established and verified, social/financial status, nature of business activity, locational characteristics, additional information provided by the accredited rating agencies and publicly available and/or obtained during the course of non-intrusive credit investigation processes. Where businesses believe that a particular customer falling under a category mentioned below is in his judgement falling in a different category, he may categories the customer so, so long as appropriate justification is provided in the customer file.
28. At this nascent phase of the Company's operations, the rationale for the risk categorization is to ensure that while the Company remains compliant with the legal and regulatory requirements with regard to the KYC/AML requirements, the consciously targeted customers who are otherwise deserving to be provided finance but find it difficult to access the formal sector, are not denied access to credit solely because of the challenges in meeting these stringent requirements.
29. The list of customers under each category is illustrative and not exhaustive. All cases requiring further deliberation at the level of Senior Management shall be referred to the Head of Credit Risk, who in consultation with the Senior Management and with their approval, advise the respective rationale for the categorization to the initiator of the deliberations. Any amendments to the risk categorization that may be warranted by business exigencies, but within the regulatory and statutory guidelines, shall be decided by an appropriate Senior Management Committee/Designated Director, who shall ensure that the amendments are presented for ratification of the Board –post facto – for suitable amendment and inclusion in the KYC Policy.
30. Categorizing customers by Risk:

Risk Level (Ascending)	Risk Category	Risk Description	Level of Customer Due Diligence At the time of commencing an account-based relationship – (Customer Onboarding)	Subsequent Updating
Category A	Low Risk	<ol style="list-style-type: none"> 1. Fully compliant CIP result and 2. verification complete and satisfactory; 3. Operations in the account satisfactory; 4. Individuals (other than High Net Worth) 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 5. People belonging to lower economic strata of the society whose accounts show low turnover and small balances 6. Salaried employees with well-defined salary structure 	<p>periodic monitoring /review of changes in risk level.</p> <p>Where a change in the risk level occurs, – the level of CDD being commensurate with the risk level to which the customer has moved on updating details.</p>	<p>Every -10- (ten) years from the date of Onboarding.</p> <p>Updating shall be done as applicable to risk Level/Category to which the Customer has moved.</p>
Category B	Medium Risk	<p>CIP result and verification complete after some additional effort but satisfactory; Operations in the account satisfactory but warrant ongoing monitoring on a moderate scale;</p> <ul style="list-style-type: none"> • High Net worth Individuals (Definition as income of more than INR 1 Crore per month) • Non-banking financial institutions; • Stock Brokers; • Importers/Exporters; • Dealers in white goods; • Wholesale dealers in Electronics; • Little known notaries and law firms 	<p>Trade reference check in the case of commercial lending; Carry out tele verification if deemed necessary.</p>	<p>Every -8- (eight) years from the date of Onboarding.</p>
Category C	High Risk	<p>CIP result and verification complete, but inherent difficulties in authentication of either identification or address proof or issues arising out of caveats in credit reference report regarding KYC aspect.</p> <ul style="list-style-type: none"> • PEPs, • Non-resident Indians, • Unincorporated bodies or Trusts), • Professional intermediaries, • Non-face-to-face customers, • Customers dealing in antiques/arms, • Partnership firms with sleeping partners, 	<p>Ongoing due diligence and enhanced monitoring.</p>	<p>Update required at each renewal/review of the loan account.</p>

		<ul style="list-style-type: none"> • Closely held family owned companies, • Casinos, • Customers dealing in cash intensive businesses such as realtors, jewellers and the like. • Customers who are unable to provide satisfactory demographic and biometric information at the level relevant to the credit decision. • All others not covered in any of the above 2 categories until, they are categorized in any one of these categories based on their satisfying the CAP and CIP. 		
--	--	---	--	--

iv. Monitoring of Transactions:

Ongoing monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account. Company shall make endeavours to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular/pattern of activity can be identified. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. Company may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of Company. Higher risk accounts shall be subjected to intense monitoring. Company shall set key indicators for such accounts on basis of the background of the customer, country of origin, sources of funds, the type of transactions involved and other risk factors which shall determine the extent of monitoring. Company shall explore the possibility of validating the new account opening applications with various watch lists available in public domain, including RBI watch list. An Illustrative List of suspicious transaction pertaining to financial services is given in Annexure II.

F. On-going due diligence:

Ongoing due diligence of customers to ensure that the customers' transactions are consistent with their knowledge about the customers' business and risk profile and the source of funds.

- Transactions of customers categorised as High risk, shall be monitored more intensively than the customers categorised as Medium/Low risk.
- Annual review of risk categorization of customers shall be undertaken to ensure that customer due diligence process stays appropriate for the customer's risk categorization.
- Update of customer due diligence process shall be done based on risk profile of the customer as follows:

Risk Category	Periodic Update (at the least)	Individuals	Legal entities
High	once in -2- years	<ul style="list-style-type: none"> • PAN verification • Aadhar number authentication • If Aadhaar does not contain current address an OVD containing current address may be obtained. • Certified copies of OVD containing identity and address not eligible to obtain Aadhaar. 	Documents sought at time of opening of account and obtain fresh certified copies.
Medium	once in -8- years	<ul style="list-style-type: none"> • PAN verification • Aadhar number authentication • If Aadhaar does not contain current address an OVD 	Documents sought at time of opening of account and obtain fresh certified copies.

		containing current address may be obtained. <ul style="list-style-type: none"> • Certified copies of OVD containing identity and address not eligible to obtain Aadhaar. 	
Low	once in -10- years	i. Where there is a change in identity and/or address: <ul style="list-style-type: none"> • Certified copies of OVD containing identity and address; ii. Where there is no change in identity and/or address: <ul style="list-style-type: none"> • Self-certification to that effect. 	Documents sought at time of opening of account and obtain fresh certified copies.

G. Identification of Beneficial Owner:

While it is unlikely that the Company will establish, on a regular basis account-based relationship in respect of Legal Entities, the customer due diligence measures while establishing an account-based relationship with a:

- i. Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps to verify the beneficial owner(s)' identity shall be undertaken except where, the customer or the owner(s) of beneficial interest is a company listed on a stock exchange or a subsidiary of such a listed company.
- ii. Trust/Nominee of a fiduciary accounts where the customer is acting as a trustee/nominee or any other intermediary, evidence to the satisfaction of the Company, of the intermediary(ies) and of the persons on whose behalf they are acting, as also the details of the nature of trust or other arrangements in place shall be obtained.

H. Training Program:

Company shall conduct employee training programs so that the members of the staff are adequately trained in KYC/ AML/ CFT (Combating the Financing of Terrorism) procedures. Training requirements shall have different focus for front line staff, compliance staff and officer/ staff dealing with new Customers so that all those concerned fully understand the rationale behind the KYC Policies and implement them consistently. The front-line staff shall be specially trained to deal with issues arising from lack of customer education.

I. Internal Control System:

The Company's Internal Audit and Compliance functions will evaluate and ensure adherence to the KYC Policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Management of the Company under the supervision of the Committee shall ensure that the audit function is staffed adequately with skilled individuals. Internal Auditors will 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 shall be put up before the Committee along with their normal reporting frequency. Further, the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel so as to ensure that person of criminal nature/ background do not get an access, to misuse the financial channel.

J. Record Management:

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. The Company shall,

- a) maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least five years from the date of transaction;
- b) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
- c) make available the identification records and transaction data to the competent authorities upon request;
- d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

- e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
- e (i). the nature of the transactions;
 - e(ii)ii. the amount of the transaction and the currency in which it was denominated;
 - e(iii). the date on which the transaction was conducted; and
 - e(iv). the parties to the transaction.
- f) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
- g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

K. Reporting to Financial Intelligence Unit – India:

The PO shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIU-IND) as advised in terms of the PML Rules, in the prescribed formats as designed and circulated by RBI. The employees of Company shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

L. General:

i. Introduction of new technologies:

Company shall pay special attention to any money laundering threats that may arise from new or developing technologies including online transactions that may favour anonymity, and take measures, if needed, to prevent their use in money laundering. Company shall ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode for any amount is affected by cheques and not against cash payment.

ii. Applicability to Branches and Subsidiaries outside India:

This Policy shall also be applicable to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit as and when the Company opens overseas branches. When local applicable laws and regulations prohibit implementation of these guidelines, the same will be brought to the notice of RBI.

iii. Closure of Accounts/Termination of Financing/Business Relationship:

Where Company is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-operation by the customer, Company shall terminate Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of Executive Chairman, Managing Director or key managerial persons authorized for the purpose.

iv. KYC for the Existing Accounts:

While the KYC Policy will apply to all new Customers, the same would be applied to the existing Customers on the basis of materiality and risk. However, transactions with existing Customers would be continuously monitored for any unusual pattern in the operation of the accounts.

v. Miscellaneous issues:

The following points shall be adhered to, by the Company at appropriate levels of management:

- i. In terms of Section 51A of the Unlawful Activities Prevention Act, 1967 (UAPA, 1967), the Company shall ensure that no account is opened/operated/maintained in the name of individuals/entities appearing in the lists of individuals and entities suspected of having terrorist links, which are approved and periodically circulated by the United Nations Security Council under the following -2- lists:
 - a) The “ISIL (Da’esh) & Al-Qaida Sanctions List” available at:
<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-quaida-r.xsl>
 - b) The “1988 Sanctions List” available at:
<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-quaida-r.xsl>
- ii. Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 2, 2021.

- iii. In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/entities from time to time shall also be taken note of.
 - iv. Freezing of Assets under section 51A of Unlawful Activities (prevention) Act, 1967: the procedure laid down in the UAPA Order dated February 2, 2021(Annex II of Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 DATED February 25, 2016 (Updated as on May 10, 2021))shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.
 - v. The Company shall maintain confidentiality of the information as required under Section 45NB In The Reserve Bank of India Act, 1934.
 - vi. Senior Management shall ensure that the mandatory sharing of KYC data with Central KYC Records Registry (CKYCR), as mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be.
 - vii. The appropriate level of operating management should ensure that cheques, if any, received in repayment of loans drawn on banks should be submitted for settlement within -3- months from the date of cheque.
 - viii. In loan repayments, AC Payee cheques not in the name of the customer shall not be accepted.
 - ix. All cash transactions of ₹ 50,000 and above shall be supported by the PAN of the customer or form 60.
 - x. In case of direct payment to suppliers (on behalf of the customers) the Permanent Account Number (PAN) of the supplier shall be obtained from the customer.
 - xi. Where the customer does not have a PAN, then form 60 shall be obtained from the customer.
- vi. Update in KYC Policy of Company**
PO shall, after taking the due approval from the Committee, make the necessary amendments/modifications in the KYC/ AML/ CFT Policy or such other related guidance notes of Company, to be in line with RBI or such other statutory authority's requirements/updates/ amendments from time to time.

Part III : Annexures

ANNEXURE I CUSTOMER IDENTIFICATION REQUIREMENTS (INDICATIVE GUIDELINES)

1. 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. Branch/office shall gather sufficient information on any Person/Customer of this category intending to establish a relationship and check all the information available on the Person in the public domain. Branch/office shall verify the identity of the Person and seek information about the sources of funds before accepting the PEP as a Customer. The decision to provide financial services to an account for PEP shall be taken at a senior level and shall be subjected to monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

2.Accounts of companies and firms:

Branch/office need to be vigilant against business entities being used by individuals as a front for maintaining accounts with NBFCs. Branch/ office may examine the control structure of the entity, determine the source of funds 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 it shall not be necessary to identify all the shareholders.

3.Customer accounts opened by professional intermediaries when the branch/office has knowledge or reason to believe that the Customer account opened by a professional intermediary is on behalf of a single Customer, that Customer must be identified. Branch/office may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branch/office also maintain 'pooled' accounts managed by lawyers/ chartered accountants for funds held 'on deposit' for a range of Customer. Where funds held by the intermediaries are not co-mingled at the branch/office and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the branch/office, the branch/office shall still look through to the beneficial owners. Where the branch/ office relies on the 'Customer Due Diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the Customer lies with the branch/office.

ANNEXURE II

ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTION PERTAINING TO FINANCIAL SERVICES

Broad categories of reason for suspicion and examples of suspicious transactions for Non- Banking Financial Companies are indicated as under:

1. Identity of client:
 - a) False identification documents
 - b) Identification documents which could not be verified within reasonable time
 - c) Accounts opened with names very close to other established business entities.

2. Background of Client:

Suspicious background or links with known criminals.

3. Multiple Accounts:

Large number of accounts having a common account holder, introducer or authorized.

4. Signatory with no rationale:
 - a) Unexplained transfers between multiple accounts with no rationale.

5. Activity in accounts:
 - a) Unusual activity compared with past transactions- Sudden activity in dormant accounts;
 - b) Activity inconsistent with what would be expected from declared business.

6. Nature of transactions;
 - a) Unusual or unjustified complexity;
 - b) No economic rationale or Bona fide purpose;
 - c) Frequent purchases of drafts or other negotiable instruments with cash;
 - d) Nature of transactions inconsistent with what would be expected from declared business.

7. Value of Transactions:
 - a) Value just under the reporting threshold amount in an apparent attempt to avoid reporting.
 - b) Value inconsistent with the client's apparent financial standing.

8. Illustrative list of Suspicious Transactions:
 - a) Reluctant to part with information, data and documents;
 - b) Submission of false documents, purpose of loan and detail of accounts;
 - c) Reluctance to furnish details of source of funds of initial contribution;
 - d) Reluctance to meet in person, representing through power of attorney;
 - e) Approaching a distant branch away from own address;
 - f) Maintaining multiple accounts without explanation;
 - g) Payment of initial contribution through unrelated third-party account;
 - h) Suggesting dubious means for sanction of loan;
 - i) Where transactions do not make economic sense;
 - j) Where there is doubt about beneficial ownership;
 - k) Encashment of loan through a fictitious bank account;
 - l) Request for payment in favour of third party with no relation to transaction;
 - m) Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent;
 - n) Multiple funding involving NGO, Charitable organization, small and medium establishments, self-help groups, micro finance groups, etc;
 - o) Frequent request for change of address;
 - p) Over-payment of instalments with a request to refund the overpaid amount.
 - q) An employee whose lavish lifestyle cannot be supported by his / her salary or known sources of income