KNOW YOUR CUSTOMER POLICY (KYC POLICY)

CONTENT

1. PREAMBLE:

The Reserve Bank of India (RBI) has issued comprehensive 'Know Your Customer Directions - 2016' (KYC) directions to all Non-Banking Financial Companies (NBFCs) in the context of the recommendations made by the Financial Action Task Force (FATF) and Prevention of Money-Laundering Act, 2002 (PMLA) standards and Combating Financing of Terrorism (CFT) policies as these being used as the International Benchmark for framing the stated policies, by the regulatory authorities. In view of the same, **Sampati Securities Limited** (**"the Company"**) has adopted the said KYC guidelines with suitable modifications depending on the activity undertaken by it. The Company has ensured that a proper policy framework on KYC and PML measures are formulated in line with the prescribed RBI guidelines and duly approved by its Loan & Risk Committee (**"Committee"**).

2. OBJECTIVES, SCOPE AND APPLICATION OF THE POLICY:

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better which in turn will help it to manage its risks prudently. Thus, the KYC policy has been framed by the Company for the following purposes:

a) To prevent criminal elements from using Company for money laundering activities;
b) To enable Company to know and understand its Customers and their financial dealings better which, in turn, would help the Company to manage risks prudently;
c) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;
d) To comply with applicable laws and regulatory guidelines;
e) To ensure that the concerned staff are adequately trained in KYC/PML/CFT procedures. This KYC Policy is applicable to all branches/offices of the Company and is to be read in conjunction with related operational guidelines issued from time to time. This Policy includes ten (10) key elements:
    a. Customer Acceptance Policy (CAP);
    b. Customer Identification Procedures (CIP);
    c. Monitoring of Transactions;
    d. Risk Management;
    e. Training Programme;
    f. Internal Control Systems;
    g. Record Keeping;
    h. Appointment of Designated Director;
    i. Appointment of Principal Officer;
    j. Reporting to FIU - India.

3. DEFINITION OF CUSTOMER:

For the purpose of Company's KYC policy a 'Customer' means a Person as defined under Know Your Customer Guidelines issued by RBI (and any amendment from time to time by RBI) which are at present as under:-

a) A person or entity that maintains an account and/or has a business relationship with the Company;
b) A Person who has a Registered Account with Company and has a financial transaction or activity with the Company;
c) A Person on whose behalf the Registered Account is maintained (i.e. the beneficial owner);
d) Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law;
e) Any other Person connected with a financial transaction which can pose significant reputation or other

risks to Company, say a wire transfer or issue of high value demand draft as a single transaction.

A "Person" shall have the meaning as defined under KYC policy of RBI *(and any amendment from time to time by RBI)* which at present is as follows:

'Person' shall include:

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 person (a to e);
g) any agency, office or branch owned or controlled by any one of the above persons (a to f).

Other terms not specifically defined here shall have the same meaning as assigned to them under the KYC Directions, 2016 or the PMLA.

4. KEY ELEMENTS:

A. Customer Acceptance Policy ("CAP"):

1. The Company's CAP lays down the criteria for acceptance of Customers. The guidelines in respect of Customer relationship in the Company broadly includes the following:

a) No account is to be opened in anonymous or fictitious/benami name(s)/entity (ies);

b) No account is to be opened when unable to apply CDD measures, due to non-cooperation or non reliability of the documents / information furnished

c) Accept Customers only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks before opening a new account are to be ensured so 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, etc;

c) Classify Customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of Customers. Also, a profile of each Customer will be prepared based on risk categorization. Customer requiring very high level of monitoring, e.g. Politically Exposed Persons as explained in **Annexure I** may, if considered necessary, be kept in the High Risk Category.

d) Documentation requirements and other information to be collected in respect of different categories of Customers depending on perceived risk and compliances with Prevention of Money Laundering Act, 2002 (PMLA) and RBI/ Company's guidelines/instructions.

e) Not to open an account or close an existing account (except as provided in this Policy), where identity of the account holder cannot be verified and/or documents/information required could not be obtained/confirmed, as per the risk categorization, due to non-cooperation of the Customer or non - reliability of the data/ information furnished to Company.

f) Implementation of CAP should not become too restrictive and result in denial of the Company services to general public.

g) The decision to open an account for Politically Exposed Person (PEP) should be taken at a senior level. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

h) Circumstances in which a Customer is permitted to act on behalf of another person/ entity shall be clearly spelt out in conformity with the established law and practice and shall be strictly followed so as to avoid occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.

2. The Company shall prepare a profile for each new Customer during the credit appraisal based on risk categorization as mentioned in this Policy in **Annexure I**. The Customer profile shall contain the

information relating to the Customer's identity, social and financial status and nature of employment or business activity. The nature and extent of due diligence will depend on the risk perceived by Company. At the time of credit appraisal of the Customer the details are recorded along with his profile based on the documents provided by the Customer and verified by Company either by itself or through third party sources. The documents collected will be as per the product norms as may be in practice. However, while preparing Customer profile, the Company shall seek only such information from the Customer which is relevant to the risk category and is not intrusive. Any other information from the Customer should be sought separately with his/her consent and after opening the Registered Account.

The Customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or for any other purposes.

3. As per KYC policy, for acceptance and identification, Company's Customers shall be categorized based on perceived risk broadly into three categories - A, B & C. Category A includes High Risk Customers, Category B contain Medium Risk Customers while Category C Customers include Low Risk Customers. None of the Customers will be exempted from Company's KYC procedure, irrespective of the status and relationship with Company or its Promoters. The above requirement may be moderated according to the risk perception as explained in **Annexure I**.

4. (i) **High Risk - (Category A):**

High Risk Customers typically includes:

a) Non-Resident Customers;
b) High net worth individuals without an occupation track record of more than 3 years;
c) Trust, charitable organizations, Non-Government Organization (NGO), organizations receiving donations;
d) Companies having close family shareholding or beneficial ownership;
e) Firms with sleeping partners;
f) Politically exposed persons (PEPs) of Indian/ foreign origin;
g) Non Face to face Customers;
h) Person with dubious reputation as per public information available;
i) Customers with Suspicious Transactions
j) Customers from FATF high risk jurisdiction and increased monitoring jurisdiction
k) High-risk Industry (e.g. Arms and Ammunition business, Lottery, Gambling, Gems and Jewellery business etc.)

(ii) **Medium Risk - (Category B):**

Medium risk Customers will include:

a) Salaried applicant with variable income/ unstructured income receiving Salary in cheque;
b) Salaried applicant working with Private Limited Companies, Proprietary, Partnership firms;
c) Self- employed professionals other than HNIs.
d) Self-employed customers with sound business and profitable track record for a reasonable period;
e) High Net worth individuals with occupation track record of more than 3 years;

(iii) **Low Risk-(Category C):**

Low Risk individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and all other person not covered under above two categories. Customer carrying low risk may include the following:

a) Salaried employees with well-defined salary structures for over 5 years;
b) People working with government owned companies, regulators and statutory bodies, MNC's, rated companies public sector units, public limited companies etc. In the event of an existing Customer or the beneficial owner of an existing account subsequently becoming a PEP, the Company will obtain senior management approval in such cases to continue the business relationship with such person, and also undertake enhanced monitoring as indicated and specified in **Annexure I**;

c) People belonging to lower economic strata of the society whose accounts show small balances and low turnover;
d) People working with Public Sector Units;
e) People working with reputed Public Limited Companies and Multinational Companies;
f) For Persons availing the social loan from the Company through CASHe, the categories of High Risk, Medium Risk and Low Risk Customers is detailed in **Annexure III**.

B. **Customer Identification Procedures ("CIP"):**

1. Customer Identification means identifying the Customer and verifying his/her identity by using reliable, independent source documents, data or information. Company shall obtain sufficient information necessary to verify the identity of each new Customer along with brief details of its promoters and management, wherever applicable, whether regular or occasional and the purpose of the intended nature of business relationship as specified in **Annexure I** and **Annexure IV**. The requirement as mentioned herein may be moderated according to the risk perception for e.g. in the case of a public listed company it may not be necessary to identify all the shareholders.
2. Besides risk perception, the nature of information/documents required would also depend on the type of Customer (individual, corporate etc). For Customers that are natural persons, Company shall obtain sufficient identification data to verify the identity of the Customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Company shall;
   i) verify the legal status of the legal person/ entity through proper and relevant documents;
   ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person,
3. understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements keeping in view the provisions applicable of Prevention of Money Laundering & its Rules and as per guidance note issued in this respect are indicated in **Annexure I**. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in **Annexure II**. The Company will frame internal guidelines based on its experience of dealing with such persons/entities, normal prudence and the legal requirements.
4. For Persons availing the Personal and Business loan from the Company, the details of Customer Identification Procedures and documents required are listed in **Annexure III**.
5. The Company will formulate and implement a Customer Identification Programme to determine the true identity of its Customers keeping the above in view. The Policy shall also cover the Identification Procedure to be carried out at different stages, i.e. while establishing a relationship; carrying out a financial transaction or when there is a doubt about the authenticity/veracity or the adequacy of the previously obtained Customer Identification data.

Important: The Company shall periodically update Customer Identification Data after the transaction is entered. The periodicity of updating of Customer Identification data shall be once in ten years in case of Low Risk Category Customers and once in two years in case of High and Medium Risk Categories.

C. **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 endeavors 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 basis 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 carry out the periodic review of risk categorization of transactions/customer's accounts and the need for applying enhanced due diligence measures at a periodicity of not less than once in six months. Company shall explore the possibility of validating the new account opening applications with various watch lists available in public domain, including RBI watch list.

D. Customer Due Diligence (CDD) Procedure

Procedure for obtaining identification/ Customer Due Diligence (CDD) Procedure:
For Individuals: For undertaking CDD, Company shall obtain the following from individual while establishing account-based relationship or while dealing with the individual who is beneficial owner, authorised signatory or power of attorney holder related to any legal entity:
(a) The Aadhaar number:

i. Where borrower is desirous of receiving any benefit or subsidy under any scheme any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 ; or
ii. He decides to submit his Aadhaar number voluntarily to Company notified under the first proviso to sub-section (1) of section 11A of the PML Act
Note: A borrower may submit only the "proof of possession of Aadhaar number" s.t. any other OVD containing the details of his identity and address has been submitted.

The KYC identifier with an explicit consent to download records from CKYCR. Company shall retrieve KYC records online from the CKYCR in accordance with section "CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)"

(b) The Permanent Account Number or Form No. 60 if PAN is not available; and

(c) Such other documents including in respect of the nature of business and financial status of the customer.

Points to be noted:
Where the customer has submitted,

i) Aadhaar number under (a) above, then Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the UIDAI. Further, in such a case, if customer wants to provide a correspondence/current address, different from the address as per Aadhaar, then he shall give a self-declaration to that effect to Company.

ii) Any OVD or proof of possession of Aadhaar number where offline verification cannot be carried out, then Company shall carry out verification as specified under Digital KYC process.

iii) KYC Identifier, the Company shall retrieve the KYC Records online from the CKYCR in accordance to with paragraph CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)
Officially Valid Document (OVD): OVD includes:

- PAN
- Passport
- Driving licence,
- Proof of possession of Aadhaar number (in such a form as is issued by the Unique Identification Authority of India)
- Voter's Identity Card issued by the Election Commission of India

Note:

- Aadhaar number should be masked at every stage during the customer loan life cycle. In cases where a copy of the Aadhaar is uploaded, the first 8 digits should be masked with a black font, leaving only the last 4 digits visible. Additionally, wherever the Aadhaar number is captured, only the last 4 digits should be displayed.

E. Digital KYC Process

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.

Digital KYC Process

a) Company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of Company.

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

c) The customer, for the purpose of KYC, shall visit the location of the authorized official of Company or vice-versa. The original OVD (ID & Address proof document) shall be in the possession of the customer.

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

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

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

g) Subsequent to all these activities, the Application shall give information about the completion of the process.

F. Requirements/ obligations under International Agreements

(A) Communication from international Agencies

(i) Company shall ensure adherence to provisions and ongoing screening of Unlawful Activities (Prevention) (UAPA) Act, 1967 or Weapons of mass destruction act, 2005, United Nations Security Council (UNSC, UNSCRs circulated by the Reserve Bank, Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007 and amendments thereto, wherever applicable.

(ii) Company will take measures to ensure that there is no account/relationship opened in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC) from time to time. The Company shall verify the aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, on a daily basis, and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.

The Company shall report the details of accounts resembling any of the individuals / entities in the lists to FIU-IND in addition to advising the Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021.

(B) Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967 - Company shall follow the relevant procedure laid down in the UAPA Order dated February 2, 2021, wherever applicable.

(C) Order to freeze assets under section 12A of WMD Act, 2005 is received from the CNO, Company shall take necessary to comply with the order. Company shall undertake countermeasures when called upon to do so by any international or intergovernmental organization of which India is a member and accepted by the Central Government.

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

G. Secrecy Obligations and Sharing of Information

(a) Company maintained secrecy regarding the customer information which arises out of the contractual relationship between the SSL and customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

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

(d) The exceptions to the said rule shall be as under:
i. Where disclosure is under compulsion of law
ii. Where there is a duty to the public to disclose,
iii. The interest of SSL requires disclosure and
iv. Where the disclosure is made with the express or implied consent of the customer.

H. Risk Management:

The Management of the Company under the supervision of the Board of Directors and the Loan and Risk Committee shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility will be explicitly allocated within the Company for ensuring that the policies and procedures as applicable to Company are implemented effectively. The Company shall devise procedures for creating Risk Profiles of their existing and new Customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

I. Training Programme:

Company shall have an ongoing employee training programs so that the members of the staff are adequately trained in KYC/ PML/ CFT procedures. Training requirements shall have different focuses 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.

J. 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.

K. Record Keeping:

1. Maintenance of records of transactions: The Company shall maintain proper record of the transactions as required under Section 12 of the PMLA read with Rule 3 of the Prevention of Money Laundering Rules, 2005 (PML Rules) as mentioned below:
   a) All cash transactions of the value of more than Rupees Ten Lakhs (Rs. 10, 00, 000/-) or its equivalent in foreign currency, though by policy the Company neither accept cash deposits nor in foreign currency.
   b) All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakhs (Rs. 10,00,000/-) or its equivalent in foreign currency where such series of transactions have taken place within a month.
   c) All transactions involving receipts by non-profit organizations of Rupees ten lakhs or its equivalent in foreign currency.
   d) All cash transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place; any such transactions.
   e) All suspicious transactions whether or not made in cash and in manner as mentioned in the PML Rules framed by the Government of India under PMLA. An Illustrative List of suspicious transaction pertaining to financial services is given in **Annexure IV**.
2. Records to contain the specified information

The Records referred to above in Rule 3 of PML Rules to contain the following information:

a) the nature of the transactions;
b) the amount of the transaction and the currency in which it was denominated;
c) the date on which the transaction was conducted;
d) the parties to the transaction.

3. Maintenance and preservation of records Section 12 of PML Act requires the Company to maintain records as under:

a) records of all transactions referred to in clause (a) of sub-section (1) of Section 12 read with Rule 3 of the PML Rules is required to be maintained for a period of five (5) years from the date of transactions between the customers and Company.

b) records of the identity of all Customers of Company are required to be maintained for a period of five (5) years from the date of cessation of transactions between the Customers and Company .

c) Company shall take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

L. Appointment of Designated Director:

The Company shall designate either Managing Director or Whole-Time Director who shall be responsible to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money-Laundering Act, 2002 and the Rules made there under.

M. Appointment of Principal Officer:

Company shall designate a senior employee as 'Principal Officer' (PO) who shall be located at the Head/Corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. PO shall maintain close liaison with enforcement agencies, NBFCs and any other institution which are involved in the fight against money laundering and CFT.

N. Reporting to Financial Intelligence Unit - India:

O. The PO shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIUIND) as advised in terms of the PML Rules, in the prescribed formats as designed and circulated by RBI at the following address:

Director,
Financial Intelligence Unit India,
6th Floor, Hotel Samrat,
Chanakyapuri, New Delhi - 110 021

The employees of Company shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

5. GENERAL:

1. Customer Education:

Company shall educate Customers on the objectives of the KYC programme so that Customer understands and appreciates the motive and purpose of collecting such information. The Company shall prepare specific literature/ pamphlets, terms and conditions etc. so as to educate the Customer about the objectives of the KYC programme. The front desk staff shall be specially trained to handle such situations while dealing with Customers.

2. 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 favor 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.

3. **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.

4. 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 Chairman & Managing Director or key managerial persons authorized for the purpose.

5. 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.

6. Updation in KYC Policy of Company

PO shall, after taking the due approval from the Committee, make the necessary amendments/modifications in the KYC/ PML/ 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.

Encl: Annexure I to Annexure IV

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 non-face-to-face Customers:

In the case of non-face-to-face Customers apart from applying the usual Customer Identification Procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In the case of cross-border Customers, there is the additional difficulty of matching the Customer with the documentation and the NBFCs may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

3. **Trust/Nominee or Fiduciary Accounts:**

Branch/offices shall determine whether the Customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, they shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the Persons on whose behalf they are reacting, as also obtain details of the nature of the trust or other arrangements in place. The Company shall take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any Person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a foundation, branches shall take steps to verify the founder managers/ directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the Customer Identification Procedures.

4. 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.

5. 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 rely 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

Customer Identification Procedure Features to be verified and Documents that may be obtained from Customers

Customers/ Clients	(Certified copy of any one of the following officially valid document)
Individuals (Applicant/ Co - Applicant) - Proof of Identity and Address	a) *Passport; b) PAN Card; c) Voter's Identity Card; d) Driving License; e) Identity card (subject to the Company's satisfaction); f) Aadhar Card; g) Letter from a recognized public authority or public servant verifying the identity and residence of the Customer to the satisfaction of the Company. a) Telephone bill; b) Bank Account Statement; c) Letter from any recognized d) public authority; e) Electricity bill; f) Letter from employer (subject to the Company's satisfaction). Any one document which provides Customer information to the satisfaction of the Company will suffice. One recent photograph except in case of transactions referred to in Rule 9 (1) (b) of the PML Rules.
Accounts of Companies - Name of the company. - Principal place of business. - Mailing address of the company. - Telephone/Fax Number.	a) Certificate of incorporation and Articles of Association; b) Resolution of the board of directors to open an account and identification of those who have authority to operate the account; c) Power of attorney granted to its managers, officers or employees business on its behalf; d) An officially valid document in respect of mangers, officers or employees holding an attorney to transact on its behalf e) Copy of PAN allotment letter f) Copy of telephone bill
Accounts of Partnership firms	a) Registration certificate, if registered; b) Partnership deed; c) Power of attorney granted to a partner or an employee of the firm to transact business on its behalf d) Any officially valid document identifying the partners and the persons holding the Power of attorney and their addresses; e) Telephone bill in the name of firm/partners

Accounts of Trusts and foundations Names of trustees, settlers, beneficiaries and signatories.	a) Certificate of registration, if registered; b) Trust Deed; c) Power of attorney granted to transact business on its behalf; d) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding power of attorney, founders/ managers/ directors and their addresses; e) Resolution of the managing body of the foundation/association; f) Telephone bill.
Accounts of unincorporated association or a body of individuals	a) Resolution of the managing body of such association or body of individuals; b) power of attorney granted to him to transact on its behalf; c) 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 as association or body of individuals.
Accounts of Proprietorship Concerns Proof of the name, address and activity of the concern	a) 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 b) Registration certificate (in the case of a registered concern) c) Certificate/licence issued by the Municipal authorities under Shop & Establishment Act, d) Sales and income tax returns e) CST/VAT certificate f) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities g) Licence/certificate of practice issued in the name of 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. h) In cases 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.

**compulsory in case of non-resident individuals.*

If any of the above documents are in any language other than English, it shall be translate d into English along with a certificate from translator / notary public.

*'**Officially valid document**' is defined to mean the passport, the driving license, the permanent account number card, the Voter's Identity Card issued by the Election Commission of India or any other document as may be required by the Company .

ANNEXURE III

This Annexure does not refer to documentation and KYC procedure for Customers that are legal persons or entities. As and when the Personal or business Loan shall be accessible to non-individuals, applicable KYC Policy for the same shall be included herein in terms of the RBI guidelines.

Customer Identification Procedure Features to be verified and Documents that may be obtained from Customer:

Categorization of Clients

While accepting and executing a client relationship the Company has adopted a risk based approached as under:

	Low Risk Customer	Medium Risk Customer	High Risk Customer
Definition	a) Customers like Salaried people- wherein all their income and expenses details are transparent and well structured. b) Wherein only customers basic requirements of verifying the identity and location are to be met.	Customers those are less risky in nature as compare to high risk customers - can be categorised as Medium Risk.	Customers that are likely to pose a higher than average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc.
List of Customers as per Risk category	a) Salaried employees whose salary structures are well defined, b) People belonging to lower economic strata of the society whose accounts show small balances and low turnover, c) Government departments & Government owned companies, regulators and statutory bodies, etc. d) Micro/ Small/ Medium enterprises filing regular ITR, good banking relationship, existing trade records with any Financial institutions etc.	a) Client with over investment of Rs. 50 Lakh where identity and sources of wealth are not supported by public documents like income returns, registered conveyance deeds etc. b) Clients with sudden spurt in volumes or investment without apparent reasons. c) Clients who trade in derivatives. d) Customers having speculative income. e) Person in business/industry or trading activity where scope or history of unlawful trading / business activity dealings is more, etc.	a) Non-resident customers, b) High net worth individuals, c) Trusts, charities, NGOs and organizations receiving donations, d) Companies having close family shareholding or beneficial ownership, e) Firms with 'sleeping partners', f) Politically exposed persons (PEPs) of foreign origin, g) Non-face to face customers, and h) Those with dubious reputation as per public information available, etc. i) NPA customers

Customer shall submit the following documents (self-attested):

a) Photo Identity Proof - PAN Card
b) Latest salary slip
c) Permanent Address Proof - Any one (1) of:
   - Aadhar Card;

- Passport;
- Driving License;
- Voter's Identity Card.

If Current Address is different from Permanent Address, then additionally:

- Utility Bill- Electric/landline phone bill/ Gas Bill of current address (not more than 2 months old).
- Leave and License Agreement/Rent Agreement.
- Salary slip (if it contains the current office address of the Borrower).

d) Current Photograph as a selfie.

e) Latest Statement of the Customer's Bank showing Salary Credit.

In case the Customer does not have any of the above mentioned valid documents for verification, then Customer can submit proof of address and identity of a close relative with whom the prospective Customer is living together with a written declaration from such relative stating the prospective customer is a relative and is staying with him / her.

For the aforesaid purpose, a close relative includes husband, wife, son, daughter and parents etc. who live with their wife, husband, father/mother, daughter and son.

Verification Process:

1. PAN Card shall be verified electronically from Income Tax Website so as to ascertain correctness of PAN Number and corresponding name from Income Tax web site. The said verification may be carried out by the Company itself or through an independent Agency.
2. Similarly AADHAR & Voters ID shall be verified through Independent Agency.
3. Utility Bills and Passport will be used to verify address.
4. Customer will electronically upload his selfie on the CASHe app.
5. Bank Statement will be used to verify Customer's Account Number with the respective Bank of the Customer.

All Documents uploaded should be self-certified. Additional documents may be called for, if necessary.

First payment made by Customer should be effected through Customer's account with a Bank with whom Customer has completed all KYC requirements.

ANNEXURE IV

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:
   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 bonafide 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 doubt about beneficial ownership;
   k) Encashment of loan through a fictitious bank account;
   l) Sale consideration quoted higher or lower than prevailing area prices;
   m) Request for payment in favor of third party with no relation to transaction;
   n) Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent;
   o) Multiple funding involving NGO, Charitable organization, small and medium establishments, self-help groups, micro finance groups, etc;
   p) Frequent request for change of address;
   q) Over-payment of installments with a request to refund the overpaid amount.