Authum Investment and Infrastructure Limited

'Know Your Customer' (KYC) and Anti Money Laundering (AML) Policy

Reviewed on 13/02/2023

Amended upto February 2023

'Know Your Customer' (KYC) and Anti Money Laundering (AML) Policy

Authum Investment and Infrastructure Limited, in compliance with RBI Master Direction DBR. AML. BC. NO. 81/ 14.01.001/ 2015-2016 dated February 25, 2016 and the various circulars issued from time to time, is adopting the following KYC policies:

The company shall follow customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. The policy is based on Anti Money Laundering (AML) standards.

1. Information collected from the customer for the purpose of opening of account shall be kept as confidential and not shall divulge any details thereof for cross selling or any other purposes without the express permission of the customer. Information sought from the customer shall be relevant to the perceived risk, shall not be intrusive, and shall be in conformity with the guidelines issued by RBI from time to time. Any other information from the customer shall be sought separately with his /her consent and after opening the account.

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

(i) Customer Acceptance Policy;
(ii) Customer Identification Procedures;
(iii) Monitoring of Transactions; and
(iv) Risk management.

3. For the purpose of the KYC policy, a 'Customer' means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

4. Customer Acceptance Policy (CAP):

The company has a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy has the following aspects of customer relationship in the company.

(i) No account shall be opened in anonymous or fictitious/ benami name(s);

(ii) Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk; customers requiring very high level of monitoring, shall, if considered necessary, be categorised even higher;

(iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank of India from time to time;

(iv) The company shall not open an account where it is unable to apply appropriate customer due diligence measures i.e. the company is unable to verify the identity and /or obtain

documents required as per the risk categorisation due to non cooperation of the customer or non reliability of the document/information furnished to the company.

(v) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity;

(vi) Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations or with the sanctions lists circulated by Reserve Bank of India etc.

(vii) No transaction or account based relationship would be undertaken without following the CDD procedure.CDD Procedure would be followed for all the joint account holders, while opening a joint account.

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

(ix) Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

The company shall prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the company. However, while preparing customer profile the company would take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

The customer would be categorized under a risk category as per Annexure-1 at the time of availing a loan.

The adoption of customer acceptance policy must not result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged.

5. Customer Identification Procedure (CIP):

Customer Identification Procedure as per section 16 of Master Direction on KYC to be carried out at different stages i.e. while establishing a relationship; carrying out a financial transaction or when the company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data or when the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold limit as may be specified.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information.

The company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship. Being satisfied means that the company should be able to satisfy the competent authorities that due diligence was observed based on the risk profile of

the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to the company and a burdensome regime for the customers. 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, the 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, (iii) 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 in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annexure - 2.

If the company accepts such accounts in terms of the Customer Acceptance Policy, the company shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are. An indicative list of the nature and type of documents/information that shall be relied upon for customer identification is given in the KYC Documentation Policy.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on customer due diligence done by a third party, subject to the following conditions:

(a) Necessary records or the information of such customers' due diligence carried out by the third party is immediately obtained by the Company or from the Central KYC Records registry.
(b) Adequate steps are taken to satisfy that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
(c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
(d) The third party shall not be based in a country or jurisdiction assessed as high risk.
(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures would be with the Company.

6. Periodic Updation:

Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers subject to the following procedure:

(a) Company shall carry out
   I. CDD as per extant requirement of RBI KYC Master Direction, at the time of periodic updation. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained
   In case of Legal entities, Company shall review the documents sought at the time of opening of account and obtain fresh certified copies.
(b) Company may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication/Offline Verification unless there are sufficient reasons that physical presence of the account holder/holders is required

to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

(c) Company shall ensure to provide acknowledgment with date of having performed KYC updation.

(d) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

Process for periodic review and re-verification of KYCs:

1. Customers are classified in to three categories at the time of on-boarding in our loan generation system (creation of prospect number) as defined in the Annexure-1 (High, Medium or Low) above.
2. Operations team shall send loan book to the Risk team for each product on a half yearly basis
3. Basis this, risk team finalizes the customers for whom re-verification of the KYC documents has to be performed as per the RBI guidelines.
4. Communications are sent to all such customers through e-mails & SMS to update their KYC documents.
5. List of customers where e-mail or SMS is not delivered is shared with respective Business Heads for updating the contact details/ collection of documents.
6. On collection of the documents the same is sent to Ops team for storage.
7. RMU team updates the Risk Team & Compliance team via mail on receipt of the KYC documents.
8. Compliance team along with risk team on a periodic basis follow up with respective Business teams for updating the contact details/ collection of the KYC documents for the pending cases & collection/ updation is done on best effort basis.

Where the Company is unable to obtain KYC documents from the customers, the Company shall not sanction any additional facility, renew any existing facility nor shall provide any new loan until fresh KYC documents are provided by the customer.

7. Digital KYC:

In case the Company is carrying out verification through digital KYC, process as specified under **Annex 3** shall be followed.

8. Video – Customer Identification Process (VCIP):

Company may undertake live V-CIP, to be carried out by an official of the Company, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. The official of the Company performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information as below:
   • Banks: can use either OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) may be used by banks for aiding the V-CIP.
   • REs other than banks: can only carry out Offline Verification of Aadhaar for identification.

ii. Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

iv. The official of the Company shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the

identification details in Aadhaar/PAN shall match with the details provided by the customer.

v. The official of the Company shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

vi. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

vii. RE shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. Company shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

viii. To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the V-CIP application before rolling it out.

ix. The audiovisual interaction shall be triggered from the domain of the Company itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

x. Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xi. Company are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the RE.

xii. Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of RBI KYC Master Direction.

9. Monitoring of Transactions

The company shall pay special attention to all complex, unusually large transactions including RTGS transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The company shall prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. The transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the company. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.

The extent of monitoring shall be aligned with the risk category of the customer. High-risk accounts shall be subjected to intensified monitoring. The company shall set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. The company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. The records of transactions in the accounts shall be preserved and maintained as required under PML Act, 2002. The company shall report the transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, to the appropriate authority.

A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, shall be put in place. Every customer once being stamped into a risk category would further be subjected to change of his risk profile depending on the repayment history and DPDs which are as under:

Logic for change in risk gradation is mentioned as below:

Criteria for change in risk gradation	**Existing category**	**Revised category**
Reported as SMA – 1 & 2 as per reporting to RBI. (Half yearly basis)	Low	Medium
	Medium	High
	High	High

The Company shall continue to maintain proper record of all cash transactions (deposits and withdrawals) of Rs.10 lakh and above. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling/ head office on a periodic basis.

10. Risk Management:

For risk management, the Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perception. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in

The company's internal audit functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the internal audit function would provide an independent evaluation of the company's own policies and procedures, including legal and regulatory requirements. The audit machinery shall be staffed adequately with individuals who are well versed in such policies and procedures. Concurrent/ Internal Auditors shall 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 Audit Committee of the Board on periodic intervals.

The company shall have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policy and implement the same consistently.

11. Customer Education:

Implementation of KYC procedures requires the company to demand certain information from customers, which may be of personal nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The company shall prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff shall be specially trained to handle such situations while dealing with customers.

12. Introduction of New Technologies:

The company shall pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent its use in money laundering schemes.

13. KYC for the Existing Accounts:

The company shall also apply this policy to the existing customers on the basis of materiality and risk. However, transactions in existing accounts shall be continuously monitored and any unusual pattern in the operation of the account shall trigger a review of the CDD measures.

The company shall consider applying monetary limits to such accounts based on the nature and type of the account. All the existing accounts of companies, firms, trusts, charities, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'.

14.Applicability to branches and subsidiaries outside India:

The policy shall also apply to the branches (if any) and majority owned subsidiaries located abroad (if any), especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same would be brought to the notice of Reserve Bank.

15. Appointment of Principal Officer & Designated Director:

The company has appointed a senior management officer designated as Principal Officer & Designated Director. Principal Officer &Designated Director shall be located at the head office of the company and shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

The name, designation and address of the Principal Officer & the Designated Director shall be communicated to the FIU-IND.

16. The Company shall allot Unique Customer Identification Code (UCIC) to all their customers while entering into any new relationships.

17.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:

(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:
(i) the nature of the transactions;
(ii) the amount of the transaction and the currency in which it was denominated;
(iii) the date on which the transaction was conducted; and
(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.

Kindly note that the records referred to in rule 3 shall be maintained for a period of 10 years from the date of cessation of transaction between the client and the Company.

18. Reporting to Financial Intelligence Unit - India:

The Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof. (such as cash transaction report, suspicious transaction report etc).

19. Obligation under International Agreements communications from International Agencies

Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, it does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

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

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

The procedure laid down in the UAPA Order dated February 2, 2021 shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

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.

FATF recommendations:

(a) 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. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

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

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

20. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules as amended from time to time, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be.
In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the dates mentioned in KYC Master Direction as per (e) and (f) of respectively at the time of periodic updation as specified in point no 6 (Periodic updation) or earlier, when the updated KYC information is obtained/received from the customer.

(i) Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

(ii) Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to Company, with an explicit consent to download records from CKYCR, then Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

i. there is a change in the information of the customer as existing in the records of CKYCR;
ii. the current address of the customer is required to be verified;
iii. the Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client. (Amended vide amendment dated December 18, 2020)

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

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

(b) The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise will be determined by the Board of the Company, in alignment with the outcome of the risk assessment exercise. However, it will be reviewed at least annually.

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

Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and will have Board approved policies, controls and procedures in this regard. Further, Company will monitor the implementation of the controls and enhance them if necessary. (Inserted vide amendment dated April 20, 2020)

Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs):

In case a person who desires to open an account is not able to produce documents, as specified in Section 16, Company may at their discretion open accounts subject to the following conditions:

a) The Company shall obtain a self-attested photograph from the customer.

b) The designated officer of the Company certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
c) The account shall remain operational initially for a period of twelve months, within which CDD as per Section 16 shall be carried out.
d) Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.
e) The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.
f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.
g) The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

KYC verification once done by one branch/office of the Company shall be valid for transfer of the account to any other branch/office of the same Company, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

Secrecy Obligations and Sharing of Information:

(a) Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the company and customer.
(b) Information collected from customers for the purpose of opening of loan account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
(c) While considering the requests for data/information from Government and other agencies, Company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy as applicable to the Company being NBFC-ND-SI.
(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 bank requires disclosure and
    iv. Where the disclosure is made with the express or implied consent of the customer.
(e) Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

All other regulatory changes in this regard will stand updated in the policy from time to time.

The Company reserves the right to amend /alter /modify the policy as from time to time, not affecting/sacrificing the underlining spirit of the code. The Company shall abide by all guidelines, directives, instructions and advices of Reserve Bank of India as shall be in force from time to time. The contents in this document shall be read in conjunction with these guidelines, directives, instructions and advices. The Company shall apply better practice so long as such practice does not conflict with or violate Reserve Bank of India regulations.

Annexure 1

Risk categorization criteria

All customers will be evaluated on a set of pre defined parameters as detailed below and accordingly classified into any of the following categories:
1. Low Risk
2. Medium Risk
3. High Risk – This category of customers will not be actively sourced by the company. Any customer, identified as High Risk, can be funded by the company basis exceptional comfort and availability of justifying mitigates. The extent and nature of due diligence will be the highest for this category.

Low Risk:
Ø All salaried profiles
Ø Small proprietors, partners having established businesses with clearly identifiable, related and relatively stable source of income since the last 2/3 years as the case maybe
Ø Standard of living that is consistent with income sources established through both documents and visits to business place with no sudden threat to financial health Ø Face to face customer (unless specifically identified as high or medium risk)
Ø Customer whose source of income can be easily identified and transactions in whose accounts by and large conform to the known profile (unless specifically identified as high or medium risk)
Ø Government departments & Government owned companies, regulators and statutory bodies

Medium Risk:
Ø Customers belonging to Negative Profile with deviations in recent banking behaviour (EMI bounce/ cheque return). In event of both deviations not being met, the customer shall not be classified as medium risk
Ø Customers belonging to Negative Area (as defined by Risk/ Collections team on periodic basis)
Ø Customers (self-employed individuals) having outstanding contracts with Government departments/ Government owned agencies
Ø Customers belonging to Caution Profile (as defined on periodic basis)
Ø Stability of place of residence/office not established
Ø Customers with inconsistent incomes year on year.
Ø Bullion dealers (including sub dealers) and jewellers with turnover not exceeding Rs 10 Crores.
Ø High Net Worth customers (Customers that have relationship values across various banks/FIs in excess of Rs 10 Crs)
Ø Trusts, Charities, NGOs and other organizations receiving donations –NGOs promoted by the United Nations will be classified as low risk
Ø Large Companies with close family shareholding or beneficial ownership

High Risk:
Ø Country of origin not established
Ø Customers with current business/ residence vintage of less than six months. In case of salaried professionals, high risk categorisation for employment experience of less than six months
Ø Firms with "sleeping partners"
Ø Politically Exposed Persons and related individuals/entities.
Ø Any other adverse public information related to individuals / entities should be categorised as high risk

Ø Non-Resident customers (Main applicant)
Ø High Net Worth customers (Customers that have relationship values across various banks/FIs in excess of Rs 20 crs)

Annexure "2"

Customer Identification Requirements – Indicative Guidelines

Trust/Nominee or Fiduciary Accounts:

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The company should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, the company shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, 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', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

Accounts of companies and firms

The company shall be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the company. The company shall 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 shall be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

Client accounts opened by professional intermediaries:

When the company has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

The company may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. The company shall also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds. Where funds held by the intermediaries are not co-mingled at the company 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, the company shall still look through to the beneficial owners. Where the company 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.

Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The company should 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. The company 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 open an account for PEP should be taken at a senior level which should be clearly spelt out in Customer Acceptance policy.

The company shall also subject such accounts to enhanced monitoring on an ongoing basis.

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 shall be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented shall be insisted upon and, if necessary, additional documents shall be called for. In such cases, the company shall also require the first payment to be effected through the customer's account with any bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the company may have to rely on third party certification/introduction. In such cases, it shall be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

Annexure 3

Digital KYC Process

A. The 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 the REs.
B. The access of the Application shall be controlled by the REs 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 REs to its authorized officials.
C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Company or vice-versa. The original OVD shall be in possession of the customer.
D. The Company must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a watermark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
E. The Application of the 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.
F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/eAadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the RE shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.
J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the RE. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

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

L. The authorized officer of the Company shall check and verify that:-
   (i) information available in the picture of document is matching with the information entered by authorized officer in CAF.
   (ii) live photograph of the customer matches with the photo available in the document.; and
   (iii) all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the Company who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer. Banks may use the services of Business Correspondent (BC) for this process.

For any clarifications please send an email to info@authum.com

If any employee comes across any such instances, they should immediately report them to email id: info@authum.com