THE VISAKHAPATNAM COOPERATIVE BANK LTD
VISAKHAPATNAM

KYC/AML/CFT POLICY

REVIWED ON 23.03.2025

KYC/AML/CFT POLICY

Contents

BANK'S POLICY ON KNOW YOUR CUSTOMER (KYC) AND ANTI MONEY LAUNDERING MEASURES (AML)

PREAMBLE

1. Reserve Bank of India issued several guidelines on 'Know Your Customer' norms and advised Banks to follow certain customer identification procedure for opening of accounts and monitoring transactions of suspicious nature for the purpose of reporting it to appropriate authority. RBI has also advised the Banks to put in place the systems and procedures to help control financial frauds, identify money laundering and suspicious activities and to have careful scrutiny / monitoring of large value of cash transactions.

2. Reserve Bank of India advised all Banks to ensure that a proper policy frame work on 'Know Your Customer' and 'Anti-Money Laundering' measures is to be formulated and put in place with the approval of the Board, in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Finance of Terrorism (CFT).

Objective

3. The objective of this policy is to prevent our Branches from being used, intentionally or unintentionally, by criminal elements for money-laundering activities. KYC procedures enable our Branches to know/understand their customers their financial dealings better which in turn help them manage their risks prudently. In tune with the instructions of the Reserve Bank of India, this policy is being dealt with in five chapters as under:

Section A	:	Introduction, background and appointment of Money - Laundering; Reporting Officer (MLRO) and Deputy Money-Laundering; Reporting Officer (DMLRO).
Section B	:	Customer Acceptance Policy.
Section C	:	Customer Identification Procedures.
Section D	:	Monitoring of Transactions.
Section E	:	Risk Management.
Section F	:	Modalities of implementing Bank's policy & Review Reporting
Section G	:	AML Rules

Section-H : Money Mules

SECTION - A

1. What is Money Laundering?

1.1. Money laundering is the process whereby proceeds of crimes such a drug trafficking, smuggling (alcohol, arms), kidnapping, gambling, robbery, counterfeiting, bogus invoicing, tax evasion, misappropriation of public funds and the like are converted into legitimate money through a series of financial transactions making it impossible to trace back the origin of funds.

1.2. Most often, such clandestine deals are the first step in using the banking system to launder or clean up the cash obtained from trade of illegal goods or services. Once the money is placed within the Bank, it goes through an intricate web of transactions, better known as layering that leave no audit trail. Conversion of this unofficial or black money into official currency thereby 'changing its color' is called money laundering.

1.3. To launder large sums of unaccountable money, one has to go through the Bank, generally in stages described as below.

* Placement - Physically disposing of cash derived from illegal activities.

* Layering - Where the depositor does a series of transactions so that one cannot detect the source or link up with the origin of money integration. In short, the process of transferring funds through various accounts to disguise its origin. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

* Integration - Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds. In short, the creation of legitimate explanation for the source of funds.

1.4. Salient features of the report submitted by the Working Group

* Each bank should have a Board approved policy covering Anti-Money Laundering Measures.

* "Know Your Customer" (KYC) Guidelines may be adopted by the Banks on the lines suggested by the Working group.

* Emphasis is laid down on monitoring of transactions for detection of suspicious activities.

* Appointment of Money Laundering Reporting Officer (MLRO) and Deputy Money Laundering Reporting Officer (DMLRO).

* MLRO and DMLRO should be officials of sufficient seniority, independence of branch operations, free to act on their own authority and should report directly to the Top Management.

* It is necessary that the person appointed as MLRO has sufficient operational experience and investigative mind.

* Both the MLRO and DMLRO are responsible to establish the relevant policies, procedures and controls and ensure their maintenance, which aim to deter criminal elements from using the products and services of the Bank for laundering proceeds of crime.

* MLRO will be instrumental in activating "Know Your Customer" procedures.

* MLRO will initiate follow up action on unusual or suspicious activity and co-ordinate with the branch functionaries in deciding on the desirability of continuing the account with increased caution and monitoring or to close the account.

* Both MLRO and DMLRO are responsible for preparation of adequate training material for the operating staff and take such steps as necessary to ensure that arrangements are made to train the concerned staff members.

1.5 Appointment: In terms of the measures suggested, the Assistant Secretary at Head Office is appointed as MLRO and the co-ordination Manager is appointed as DMLRO. The secretary will undertake internal investigations and to have liaison with the Law Enforcement Agencies on receipt of references of suspicious activities from MLRO / DMLRO.

SECTION – B

3. Customer Acceptance Policy

3.1. For the purpose of KYC Policy, a customer may be defined as:

* A person or entity that maintains an account and / or has a business relationship with the bank;

* One on whose behalf the account is maintained (i.e., the beneficial owner);

* Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

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

3.2. Following are the explicit guidelines given to ensure the customer relationship in the Bank.

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

b) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc, to enable categorization of customers into low, medium and high risk;

c) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the guidelines issued by Reserve Bank from time to time;

d) To open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and / or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data / information furnished to the bank. Such decision to close an account may be taken at Central Office after giving due notice to the customer explaining the reasons for such a decision, as a built-in measure to avoid harassment of those customers;

e) 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 and practice of banking 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 and

f) 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 etc.

g) Branches are advised to prepare a profile for each new customer based on risk categorization. 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.

h) The nature and extent of due diligence will depend on the risk perceived by the branch. However, while preparing customer profile, branches should 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.

3.3. For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk.

3.4. Illustrative examples of low-risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc.

3.5. Customers that are likely to pose a higher-than-average risk to the bank 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. Branches are advised to apply enhanced 'due diligence' measures based on the risk assessment, for higher risk customers, especially those for whom the sources of funds are not clear.

3.6. Examples of customers requiring higher due diligence may include (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.

a) Indicative guidelines on Risk categorization are furnished in Annexure-X

3.7. It is important to bear in mind by the branches that its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

3.8. Accounts of Politically Exposed Persons (PEPs) resident outside India. Politically exposed persons are individuals 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 Corporation, important political officials, etc.

3.9. The branches 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.

4.0. The branches should 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 Head Office lever.

4.1. The branches should also subject such accounts to enhanced monitoring on an on-going basis. The above norms are applicable to the accounts of the family members or close relatives of PEPs also.

SECTION - C

4. CUSTOMER IDENTIFICATION PROCEDURES

4.1 Customer identification means identifying the customer and verifying his/her identity by using reliable independent source documents data or information. The Branches need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer and the purpose of the intended nature of banking relationship. Due diligence is to be 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 Banks and a burdensome regime for the customers.

4.2 For customers who are natural persons, the branches should obtain sufficient identification data to verify the identity of the customer, his address/location and also his recent photograph. For customers who are legal persons or entities, the branches should (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 and (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control legal person.

4.3 Introduction / Identification of Accounts

Identification is the act of establishing who a person is. In the context of KYC (Know your customer), identification means establishing who a person purport to be. This is done by recording the information provided by the customer covering the elements of his identity (i.e., name and all other names used, and the address at which they can be located). Following are some of the documents which the branches can accept for establishing identity of a person:

4.4

* Passport
* Driving License
* Identity Card of any Institution
* PAN Card

* Voter's Identity Card
* Other documentary evidence in support of the person's residential address in addition to the above, such as ration card, electricity bill or telephone bill.

4.4.1 Branches may accept video-based KYC compliance. This may be included.

4.4.2 Branches should comply with C_KYC procedure by submitting all the documents to central office as instructed in various circulars issued by central office.

4.5 Verification of identity is the process of proving whether a person actually is who he claims to be. In the context of KYC, verification is the process of seeking satisfactory evidence of the identity of those with whom the branch does business. This is done by carrying out checks on the correctness of the information provided by the client. The best available evidence of identity should be obtained, having regard to the circumstances of each client and their country of origin. Some forms of proof 8 of identity are more reliable than others, and in some case, it will be prudent to carry out more than one verification check.

4.6 Guidelines on Introduction

Branches generally insist on "introduction" by a known person. Introduction is a process of ascertaining the identity of a person and his acceptability for establishing business relationship. Before opening an account, the branches must get true identity of the intending customer verified. When the branch opens an account in the name of a customer, it has to render a number of services, including collection of cheques, in the ordinary course of business. It is, therefore, essential that the branch is aware of the credentials of the prospective customer such as his profession, business address, etc. Proper introduction and verification of antecedents of account holder in each and every account are, therefore, essential.

4.7 Proper Introduction

It is necessary that the person introducing the applicant to the branch must himself be a respectable person. He should also be known to the Banker. The introducer should know the intending customer. The introducer should sign bank's forms in token of his verifying the identity of the applicant. Oral introduction of a person desirous to open an account with the bank would not constitute a proper introduction.

4.8 KYC Guidelines go beyond merely establishing the identity of the person and satisfying about his credentials. The due diligence expected under KYC invokes going into the purpose and reasons for opening the account, anticipated turn-over in the account, source of wealth (net-worth) of the person opening the account and the source or funds flowing into the account. While opening new accounts, the branches in addition to routine procedures, make their efforts to get documents for identification and proof

of residence having present and permanent addresses along with telephone numbers etc., from the account-openers. Particulars of other accounts with any other banks, Permanent Account Number (PAN) given by Income Tax Authorities, Registration Certificate in the case of partnership firms and Certificate of Incorporation, Memorandum & Articles of Association from Companies and Resolution by Boards for accounts of Companies should be obtained. The branches should prepare a customer profile containing the expected activities of his business. They should collect additional details such as: -

* Employment details such as job specifications, name and address of the employer, length of service etc.;
* Details about source of income and annual income;
* Details of assets owned such as house, vehicle etc;
* Other personal details such as qualification, marital status etc.

4.9. (i) Banks should collect only 'mandatory' information for KYC purpose which the customer is obliged to give while opening an account at the time of opening the account/during periodic updation. Other 'optional' customer details / additional information, if required, may be obtained separately only after the account is opened with the explicit consent of the customer. The customer has a right to know what is the information required for KYC that she / he is obliged to give and what is the additional information sought by the bank that is optional.

(ii) Banks should keep in mind that the information (both 'mandatory' - before opening the account as well as 'optional' – after opening the account with the explicit consent of the customer) collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Banks should, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard.

4.10 Banks should introduce a system of periodical updation of customer identification data (including photographs) after the account is opened. The periodicity of such updation should as follows.

(i) Full KYC exercise will be required to be done at least every two years for high-risk individuals and entities.

(ii) Full KYC exercise will be required to be done at least every eight years for medium risk and at least every ten years for low-risk individuals and entities.

4.11 Positive confirmation (obtaining KYC related updates through e-mail / letter / telephonic conversation / forms / interviews / visits, etc.), will be required to be completed at least every two years for medium risk and at least every three years for low-risk individuals and entities.

4.12 Fresh photographs will be required to be obtained from minor customers on their becoming major.

Primary (Urban) Co-operative Banks (UCBs) would need to continue to carry out
on-going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and, wherever necessary, the source of funds.

As advised earlier, the process of risk categorization and compiling / updating profiles of all of the existing customers should be completed by Primary (Urban) Co-operative banks in all respects by now.

4.13 Acceptance of Aadhaar letter / e-KYC service (on-line Aadhaar authentication) of UIDAI for KYC purposes

Physical Aadhaar card / letter issued by UIDAI containing details of name, address and Aadhaar number received through post should be accepted as an 'Officially Valid Document'. Unique Identification Authority of India (UIDAI) has advised Reserve Bank that banks are accepting Aadhaar letter issued by it as a proof of identity but not of address, for opening accounts. As indicated at paragraph 2.5 (vii) above, if the address provided by the account holder is the same as that on Aadhaar letter, it may be accepted as a proof of both identity and address.

4.14 Further, in order to reduce the risk of identity fraud, document forgery and have paperless KYC verification, UIDAI has launched its e-KYC service. Accordingly, it has been decided to accept e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process ("which is in an electronic form and accessible so as to be usable for a subsequent reference") may be treated as an 'Officially Valid Document' under PML Rules. In this connection, it is advised that while using e-KYC service of UIDAI, the individual user has to authorize the UIDAI, by explicit consent, to release her or his identity / address through biometric authentication to the bank branches/ business correspondents (BCs). The UIDAI then transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the bank / BCs, which may be accepted as a valid process for KYC verification. The broad operational instructions to banks on Aadhaar e-KYC service are enclosed as Annex. V. UCBs are advised to have proper infrastructure in place to enable biometric authentication for e-KYC.

4.15 Alternatively, UCBs may accept e-Aadhaar downloaded from UIDAI website as an officially valid document subject to the following.

4.16 If the prospective customer knows only his / her Aadhaar number, the UCB may print the prospective customer's e-Aadhaar letter in the UCB directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the paragraph 2.5 (ix) (b) above.

4.17 If the prospective customer carries a copy of the e-Aadhaar letter in the UCB directly from the UIDAI portal' or adopt e-KYC procedure as mentioned in the paragraph 2.5 (ix) (b) above; or confirm identity and address of the resident through simple authentication service of UIDAI.

(a) Henceforth, customers may submit only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation. In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months.

(b) In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the UCB may take a declaration of the local address on which all correspondence will be made by them with the customer. No proof is required to be submitted for such address for the purpose of correspondence. This address may be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of (i) letters, cheque books, ATM card, (ii) telephonic conversation, (iii) visits etc. In the event of change in this address due to relocation or any other reason/s, customers may initiate the new address for correspondence to the UCB within two weeks of such a change.

4.18 Opening of Bank Accounts for foreign students studying in India

The following are the procedures for opening bank accounts of foreign students who are not able to provide an immediate address proof while approaching a bank for opening bank account.

a) UCBs may open a Non-Resident Ordinary (NRO) bank account of a foreign student on the basis of his / her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution.

b) Within a period of 30 days of opening the account, the foreign student should submit to the branch where the account is opened, a valid address proof giving local address, in the form of a rent agreement or a letter from the educational institution as a proof of living in a facility provided by the educational institution. UCBs should not insist on the landlord visiting the branch for verification of rent documents and alternative means of verification of local address may be adopted by banks.

c) During the 30-day period, the account should be operated with a condition of allowing foreign remittances not exceeding USD $ 1,000.00 into the account and a cap of monthly withdrawal to Rs. 50,000.00 pending verification of address.

d) 'On submission of the proof of current address, the account would be treated as a normal NRO account, and will be operated in terms of instructions contained in RBI's Master Circular on Non-Resident Ordinary Rupee (NRO) Account No. RBI/2013-14/2 Master Circular No. 2/2013/14 dated July 1, 2013 issued by our Foreign Exchange Department, Central Office and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000 may also be kept in view.

e) Students with Pakistani nationality will need prior approval of Reserve Bank of India for opening the account.

4.19 KYC norms for Foreign Portfolio Investors (FPIs) for purpose of investment in Portfolio Investment Scheme (PIS) only

FPIs have been categorized by SEBI based on their perceived risk profile as detailed in Annex X. In terms of Rule 9 (14) (i) of the Prevention of Money Laundering (Maintenance of

Records) Rules, 2005 (Rules), simplified norms have been prescribed for those FPIs who have been duly registered in accordance with SEBI guidelines and have undergone the required KYC due diligence / verification prescribed by SEBI through a Custodian / Intermediary regulated by SEBI. Such eligible / registered FPIs may approach a bank for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the Reserve Bank of India (as detailed in Annex VII) would be required. For this purpose, banks may rely on the KYC verification done by the third party (i.e., the Custodian / SEBI Regulated Intermediary) subject to the conditions laid down in Rule 9(2) [(a) to (e)] of the Rules.

In this regard, SEBI has been requested to advise Custodians/ Intermediaries regulated by them to share the relevant KYC documents with the banks concerned based on written authorization from the FPIs. Accordingly, a set of hard copies of the relevant KYC documents furnished by the FPIs to the Custodians / Regulated Intermediaries may be transferred to the concerned bank through their authorized representative. While transferring such documents, the Custodian / Regulated Intermediary shall certify that the documents have been duly verified with the original or notarized documents have been obtained, where applicable. In this regard, a proper record of transfer of documents, both the level of the Custodian / Regulated Intermediary as well as at the bank, under signatures of the officials of the transferor and transferee entities, may be kept. While opening bank accounts for FPIs in terms of the above procedure, banks may bear in mind that they are ultimately responsible for the customer due diligence done by the third party (i.e. the Custodian / Regulated intermediary) and may need to take enhanced due diligence measures, as applicable, if required. Further, banks are required to obtain undertaking from FPIs or Global Custodian acting on behalf of the FPI to the effect that as and when required, the exempted documents as detailed in Annex VII will be submitted.

It is further advised that to facilitate secondary market transactions, the bank may share the KYC documents received from the FPI or certified copies received from a Custodian / Regulated Intermediary with other banks/ regulated market intermediaries based on written authorization from the EPI. The provisions as detailed above are applicable for both new and existing FPI clients. These provisions are applicable only for PIS by FPIs.

4.19 a. While opening account of SHG the branches should conduct due diligence in respect of all the members.

4.20. While opening operative accounts branches should obtain KYC documents, Pass port size photos and C-KYC application. The same should be sent to EDP department, Head Office as per the guidelines issued in circular no.45 dt.25.02.2019.

(This provision is included as per Board Resolution No. VII (4) Dt. 25.08.2019.

Features to be verified and documents to be obtained from customers

Individual Accounts Legal name	i) Passport (ii) PAN Card (iii) Voter's Identity Card

and any other names used. Correct permanent address	(iv) Driving License (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of branch i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Letter from employer (subject to satisfaction of the branches) (any one document which provides customer information to the satisfaction of the branch will suffice.
Partnership firms Legal name Address Names of all partners and their address Telephone numbers of the firm and partners	i) Registration certificate if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (i) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses and (v) Telephone bill in the name of firm / partners
Company Accounts Name of the company Principal place of business Mailing address of the company Telephone / Fax Number	i) Certificate of incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill.
Accounts of trusts & foundations Names of trustees, settlers, beneficiaries and signatories. Names and addresses of the founder, the manager/directors and the beneficiaries. Telephone / fax numbers	(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlers and their addresses (iv) Resolution of the managing body of the foundation / association and (v) Telephone bill

SECTION - D

5. MONITORING OF TRANSACTIONS

5.1 The objectives of the KYC frame work are in two folds, (i) to ensure appropriate customer identification and (ii) to monitor transactions of a suspicious nature.

5.2 It should be ensured that the procedure adopted does not lead to denial of access to the general public for banking services.

5.3 Ongoing monitoring is an essential element of effective KYC procedures. The branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account.

5.4 The branches should pay special attention to all complex, unusually large transactions and unusual patterns which have no apparent economic or visible lawful purpose.

5.5 Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the branch. The branches should take note that high account turn over inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.

5.6 The branches should 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.

5.7 An indicative list of suspicious activities

a) corporate accounts where deposits or withdrawals are primarily in cash.

b) corporate accounts where deposits, withdrawals and remittances, transfers from / made to sources apparently unconnected with the corporate business activity / dealings.

c) unusual applications for D.D/T. T/P. O against cash.

d) Accounts with large volume of credits through D.D/T. T/P. O

e) A single substantial cash deposit composed of many high denomination notes.

f) Frequent exchanges of small denomination notes for large denomination notes or vice-versa.

g) Multiple accounts under the same name and sudden surge in activity level.

h) Sending or receiving frequent or large volumes of cross border remittances.

i) Remittances received by T.T./D.D./P.O. from various centers and in turn remitting the consolidated amount to a different account/centre on the same day leaving minimum balance in the account.

ANNEXURE - XI

The Visakhapatnam Co-operative Bank Ltd.,
CUSTOMER PROFILE

Nature of the Account:

Name :

Father's Name :

Address **Tel. No.**
Mobile No.:

Occupation :

Nature of Business :

Location of Business:

Annual Income :

i) Passport ii) PAN Card iii) Voters Identity vi) Driving License v) Identity Card (subject to the Bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the branch. **No.**

---

i) Telephone Bill ii) Bank Account Statement iii) Letter from any recognized public authority iv) Letter from employer (subject to satisfaction of the branches) (any one document which provides customer information to the satisfaction of the branch will suffice) **No.**

Branch Manager's Remarks:

As per KYC Guidelines of RBI and Bank's Internal Guidelines, the above customer account is categorized as ..... ( )

Branch Manager

ANNEXURE – X
RISK CLASSIFICATION OF ACCOUNTS

1	High Risk	1. Customers engaged in professions where money laundering possibilities are high. e.g., Antique dealers, Money Service Bureaus, Money Exchangers, Dealers in Arms etc 2. Customers who live in high-risk countries (i.e. Afghanistan, Angola, Armenia, Cuba, Egypt, Guatemala, Iraq, Kazakhstan, Libya, Myanmar, Nigeria, Philippines, Russia, Zimbabwe etc)

		3. Politically Exposed Persons resident outside India. 4. Individuals with net worth Rs 5 crores and above, whose source of funds is not known 5. Bullion dealers and Jewelry Dealers 6. Organizations receiving donations under FCRA 1976 7. Non-Face to Face customers 8. Real Estate Dealers.
2	Medium Risk	1. Customers living in medium risk countries (i.e All countries in Africa, other than High Risk Countries 2. Individuals having credits of Rs. 50 lakhs and above in a year. 3. Firms and Companies having credits exceeding their annual turnover by more than 20% 4. Clubs, Societies & Coop Credit Societies, Trusts: Credits exceeding their annual receipts by 20%
3	Low Risk	1 All other Customers. 2 Customers with aggregate credits similar to their known sources of income. 3 Firms and Companies where credits are similar to annual turnover 4 Accounts of Govt. Departments, Local Bodies, Schools, Gram Panchayaths, Zilla Parishads etc 5 All borrowal accounts where due diligence is done 6 Trusts of Temples, Regulators and Statutory Bodies. 7 All other cases, where branch feels that the account does not pose money laundering problems.

Note: The above categorization is only indicative. Branch Manager can take a view on categorization of any particular account having regard to nature of business of the client and expected transactions in the account.

5.8 Trigger Limits:

The Bank is negotiating with soft ware vendor for fixing Account wise trigger limits for monitoring. As it is likely to take some more time for fixing the same, Bank has already put in place a control mechanism by requiring all transactions of Rs.10 lakhs and above authorization by two officers in the branch. If the branch is having only one officer, the transaction is being escalated to Central Office for second

authorization. The second authorization is given only after subjecting the transaction for close scrutiny.

5.9 Monitoring Procedure

a) Branches are required to issue traveler's cheques, demand drafts, main transfers and telegraphic transfers for Rs. 50,000/- and above only by debit to customers' accounts or against cheques and not against cash received. Branches should ensure to get the Permanent Account Number of the customer / applicant while issuing demand drafts / pay orders for amount Rs. 10,000/- and more. If the applicant is not an account holder, a photo copy of the PAN Card should be filed with the application.

a.a.) The name of the purchaser shall be incorporated on the face of the demand draft, pay order, bankers' cheque by the issuing branch. These instructions shall take effect from 15 September 2018 (added on 09-09-2018 as per RBI Circular)

b) Branches are required to keep a close watch on cash withdrawals and deposit of Rs. 10 lakhs and above in deposit and loan accounts and keep record of details of these large cash transactions in a separate register.

c) Branches are required to report all cash deposits and withdrawals of Rs. 10 lakh and above as well as transactions of suspicious nature with full details in fortnightly statements to Deputy Money Laundering Reporting Officer Head office, who would consolidate and report the transactions to the 'Top Management'.

5.10 Internal Control System

Duties and responsibilities should be explicitly allocated for ensuring that policies and procedures are managed effectively and that there is full commitment and compliance to an effective KYC program in respect of both existing and prospective deposit accounts. Zonal / Group Offices will periodically monitor strict adherence to the laid down policies and procedures by the officials at the branch level.

6.0 Terrorism Finance

Lists of terrorist entities, as notified by the Govt. of India, are communicated to all the branches and they may exercise caution if any transaction is detected with such entities. The branches should ensure that such lists are consulted with their controlling authorities in order to determine whether a person / organization involved in a prospective or existing business relationship appears on such a list. Branches should report accounts suspected to belong to terrorist entities or transactions of suspicious nature, to the Deputy Money Laundering Reporting Officer at Head Office.

6.1 Internal Audit / Inspection

a) An independent evaluation of the controls for identifying high value transactions should be carried out on a regular basis by the internal audit department.

b) Concurrent / internal auditors to specifically scrutinize and comment on the effectiveness of the measures taken by branches in a adoption of KYC norms and steps taken prevention of money laundering.

6.2 Adherence to Foreign Contribution Regulation Act (FCRA), 1976

a) Branches should also adhere to the instructions on the provisions of the Foreign Contribution Regulation Act, 1976 cautioning banks to open accounts or collect cheques only in favour of foreign organizations, which are registered under the Act by Govt. of India. A certificate to the effect that the organization is registered with the Govt. of India should be obtained from the concerned foreign organizations at the time of opening of the account or collection of cheques.

6.3 Record Keeping: In the case of wire transfer for transactions, the records of electronic payments and messages must be treated in the same way as other records in support of entries in the accounts. All financial transactions records should be retained for at least five years after the transaction has taken place and should be available for perusal and scrutiny of audit functionaries as well as regulators as and when required.

6.4 Training of staff and management

All the operating and management staff should fully understand the need for strict adherence of KYC norms. Hence there should be ongoing training program so that staff members are adequately trained for their roles and responsibilities in complying with Anti-Money Laundering guidelines and for implementing KYC policies consistently. The training shall review applicable money laundering laws and recent trends in money laundering activity with reference to our Bank's policies and procedures to combat money laundering including how to recognize and report suspicious transactions.

SECTION - E

7.0. RISK MANAGEMENT

7.1 Risk is the result of uncertain future'. Risk Management is identification, measurement, monitoring and control of risks by systematic actions, in a planned manner, through proper understanding and communication.

7.2 The risk management is a Board driven function and at present, the senior executives headed by the Chairman and Executive director deals with different types of market

risks. Since the size of the bank is small the same body comprising the referred officials shall be called the Risk Management committee.

i) Chief Executive Officer

ii) Co-ordination Manager

iii) Officer in HO

7.3 The objective in introducing the Risk Assessment System is to put in place a tool for an ongoing assessment of risk elements inherent in Bank's advances so that the operating functionaries would be regularly put on alert and appropriate measures could be initiated to reduce / eliminate risk.

7.4 The risks faced by Bank of our type and have been broadly categorized as, Credit Risk, Market Risk and Operational Risk.

7.5 Credit Risk Management:

a) Delegation of powers for undertaking lending and non-lending business has been put in place.

b) Prudential exposure limits of counter party exposure for banks and other borrowers, groups, industry etc. as per RBI guidelines are in place.

c) Credit Risk Measurement process is in tune with the regulatory requirements such as selection criteria, credit appraisal, approach to interest rates on advances, follow up, supervision, monitoring and control, periodicity of inspection etc., have been put in place.

d) Effective credit risk assessment allows our bank to reduce risk and potential NPAs. Once the branches understand their risks and cost, they will be able to determine the most profitable business, and price products according to risks.

e) The threat of bad loans rears its head through the entire credit cycle. There are five crucial areas that credit Risk Management should focus on:

* Periodically inspect collaterals to check gradual erosion in value.
* Build information system that continuously tracks credit risk.
* Monitor concentration of exposure across the product portfolio.
* Tackle Non-Performing loans quickly and effectively.

f) Pricing is now mainly dependent on the purpose of loan and the security offered as security. We may have to shift to pricing based on Credit Risk Assessment (CRA) even though value of an account is an indispensable factor that also goes on to determine the price...

7.6 Market Risk

a) Asset Liability Management Committee deals with different types market risks.

b) Sanction of advances both funds based and non based are dealt with in detail in the Bank's Credit Policy document.

7.7 Operational Risk Management

a) Guidelines for internal control, system and procedures for various business segments are already in place. These controls inter alia include segregation of duties, reporting system as well as various other checks and balances.

b) System of credit audit and stock audit for compliance of terms of sanction, monitoring of weak assets on the basis of early warning signals is in place. Similarly written instruction/guidelines on inspection, insurance etc. are issued to branches from time to time.

c) Concurrent/internal auditors should 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 may be put before the Audit Committee of the Board on quarterly intervals.

d) Information Technology: Instructions Regarding Security, back up and Disaster Recovery for strict compliance are issued from time to time by Head Office.

7.8 The in-house Training College should have an ongoing employee training program so that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for dealing with new customers. Needless to emphasize that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

7.9 Customer Education: Implementation of KYC procedures requires the branches to demand certain information from customers which may be of personal nature or which have hitherto never been called for. This may lead to sometimes a lot of questioning by the customer as to the motive and purpose of collecting such information. The customers should be educated about the objectives of KYC program by issuing specific literature/pamphlets etc. The staff needs to be specially trained to handle such situations while dealing with the customers.

8.0 KYC for the Existing Accounts:

a) Branches are advised to comply with the instruction/guidelines issued by RBI in applying the KYC norms to all the existing customers in a time bound manner.

b) The branches should monitor the transactions in the existing accounts of any unusual pattern in the operation. It should be ensured that 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 a natural / legal person and those of the 'beneficial owners.

c) The branches may also ensure that term/recurring deposit accounts or accounts of similar nature are treated as new accounts at the time of renewal and subjected to KYC procedures.

d) Where the branch is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-cooperation by the customer, the branch may consider recommending closure of the account or terminating the banking/business relationship explaining the reasons for taking such a recommendation. Final decisions need to be taken at Head Office.

9.0 Usage of 'At par' Cheque facility extended to Cooperative Banks by Scheduled Commercial Banks

UCBs are advised to utilize the 'at par' cheque facility only for the following purposes:

i) for their own use.

ii) for their account holders who are KYC compliant provided that all transactions of '50,000.00 or more should be strictly by debit to the customer's account.

iii) for walk-in customers against cash for less than Rs. 50,000.00 per individual.

In order to utilize the 'at par' cheque facility in the above manner, UCBs should maintain

i) Records pertaining to issuance of 'at par' cheques covering inter alia applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque.

ii) Sufficient balances / drawing arrangements with the commercial bank extending such facility for purpose of honoring such instruments.

UCBs should also ensure that all 'at par' cheques issued by them are crossed 'account payee' irrespective of the amount involved.

UCBs are advised to make use of more efficient means of remittances for the customers like NEFT or RTGS by providing such services directly or by becoming sub-members of banks providing such services as per regulations in this regard issued by RBI time to time.

10. Reporting of Cross Border Wire Transfer Report on FINnet Gateway

With the amendments to Prevention of Money Laundering (PML) Rules, notified by the Government, of India vide Notification No. 12 of 2013 dated August 27, 2013 and in terms of amended Rule 3, every reporting entity is required to maintain a record of all transactions including the record of all cross-border wire transfers of more than Rs. 5 lakh or its equivalent in foreign currency, where the place of either origin or destination of the fund is in India. FIU-IND has advised that the information of all such transactions may be furnished to Director, FIU-IND by 15th of the succeeding month. It is advised that the 'Transaction Based Reporting Format' (TRF) already developed by FIU-IND and being used for reporting Cash Transaction Reports (CTRs), Suspicious Transaction Reports (STRs) and Non-Profit Organizations Transaction Reports (NTRs) may be used for reporting the Cross Border Wire Transfers. The information may be furnished electronically in the FIN-Net module developed by FIU-IND. All UCBs are accordingly advised to take action as required by FIU-IND and ensure that reports are submitted in time as per the schedule. The format along with sample data filled in as an illustration is available in the 'Downloads' section of the FIU-IND website (http://fiuindia.gov.in).

11. Designated Director

UCBs should nominate a Director on their Boards as "Designated Director" to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012 provides for "Powers of Director to impose fine", As per Section 12 (2) of the Act, if the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may

(a) Issue a warning in writing; or

(b) Direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

(c) Direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

(d) By an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure."

(e) As per clause no.8 of Master Circular No.81 Dt.21.07.2018 Senior Management is constituted as follows:

Specifying as to who constitute Senior Management for the purpose of KYC compliance	Senior Management for the purpose of KYC compliance consists of the following officers 1.Chief Executive Officer 2.General Manager 3.Nodal Officer for KYC 4.Incharge Officer for IT 5.Incharge Officer for HR
Allocation of responsibilities for effective implementation of policies and procedures	Nodal Officer and In charge Officer of IT
Independent evaluation of compliance function of the Bank policies and procedures, including legal and regulatory requirements	Chief Executive Officer and General Manager

Risk Categorization for various Customers

We are classifying all the accounts/customers into High Risk, Medium Risk and Low Risk as per KYC Guidelines. We are also reviewing and updating the Risk Categorization on quarterly basis basing on the account turnover and other parameters. As per the Existing risk categorization, saving and Current accounts with a turnover upto Rs.10 lakhs are classified in the Low risk and if the turnover exceeds 10 lakhs they are being classified under medium risk. As System is taking the turnover as the sum of debits and credits in the account, many customers are being classified in the medium risk even though the total sum of credits in the accounts does not exceeds Rs. 10 Lakhs. Hence we may change the risk categorization condition in respect of "Savings and Current accounts" as Low Risk for those customers where the account turnover does not exceeds Rs. 20 lakhs. With the proposed change in the risk categorization, the risk profiles of various customers will be as follows

Existing Risk Classification:

Risk Categorization			
parameter	**HIGH**	**MEDIUM**	**LOW**
Account Status	Example:- NIL		Example:- NIL
Customer Master - Customer Type **And** **Account Master – Account Type** **(Ind-Customer Type -4th Screen and** **Others – Constitution - 4th Screen)**	22-BANK DIRECTOR 35-BULLION DEALERS 36-ANTIQUE DEALERS 37-STOCK/SHARE BROKERS 38-NON-FACE TO FACE CUSTOMER (POA HOLDER) 39-POLITICALLY EXPOSED PERSON 40-REAL ESTATE DEALERS 43-POLITICALLY EXPOSED PERSON 52-SCRAP DEALERS	4-TRUST ACCOUNT 5-REG SOCIETY 28-NPO 29-REG CO.OP SOC ENGAGED IN BANK BUSS 41-CO-OP SOCIETIES 42-CO-OP CREDIT SOCIETIES 48-CHARITABLE TRUST 51-RELIGIOUS ORGANISATIONS	1-NORMAL 2-STAFF 3-PENSION 8-H.U.F. (KARTA) 9-MINOR ACCOUNT 11-RFC 13-SENIOR CITIZEN 14-ASSOCIATION 15-BANK 21-SBNF-SPECIAL 23-GROUP 24-UNION 26-INSTITUTIONAL BULK DEPOSIT 27-SPECIAL MINOR(10-18 YRS) 32-FOUNDATION 33-PUBLIC LTD COMPANY 34-PRIVATE COMPANY
Product Code	Any GL Code	Any GL Code	Any GL Code
Account Turnover			
Saving Account	Above Rs. 50.00 Lakhs	Above Rs. 10.00 Lakhs Up to Rs. 50.00 Lakhs	Up to Rs. 10.00 Lakhs
Current Account	Above Rs. 50.00 Lakhs	Above Rs. 10.00 Lakhs up to Rs. 50.00 Lakhs	Up to Rs. 10.00 Lakhs

	CC/OD	More Than 5 times of sanction limit		Up to 5 times of sanction limit

Revised Risk Classification from 01/04/2024:

Revised Risk Categorization with effect from 01/04/2024				
parameter		**HIGH**	**MEDIUM**	**LOW**
	Account Status	Example: - NIL		Example: - NIL
	Customer Master - Customer Type **And** **Account Master – Account Type** **(Ind-Customer Type -4th Screen and** **Others – Constitution - 4th Screen)**	22-BANK DIRECTOR 35-BULLION DEALERS 36-ANTIQUE DEALERS 37-STOCK/SHARE BROKERS 38-NON-FACE TO FACE CUSTOMER (POA HOLDER) 39-POLITICALLY EXPOSED PERSON 40-REAL ESTATE DEALERS 43-POLITICALLY EXPOSED PERSON 52-SCRAP DEALERS	4-TRUST ACCOUNT 5-REG SOCIETY 28-NPO 29-REG CO.OP SOC ENGAGED IN BANK BUSS 41-CO-OP SOCIETIES 42-CO-OP CREDIT SOCIETIES 48-CHARITABLE TRUST 51-RELIGIOUS ORGANISATIONS	1-NORMAL 2-STAFF 3-PENSION 8-H.U.F. (KARTA) 9-MINOR ACCOUNT 11-RFC 13-SENIOR CITIZEN 14-ASSOCIATION 15-BANK 21-SBNF-SPECIAL 23-GROUP 24-UNION 26-INSTITUTIONAL BULK DEPOSIT 27-SPECIAL MINOR(10-18 YRS) 32-FOUNDATION 33-PUBLIC LTD COMPANY 34-PRIVATE COMPANY
	Product Code	Any GL Code	Any GL Code	Any GL Code
	Account Turnover			
	Saving Account	Above Rs. 50.00 Lakhs	**Above Rs. 20.00**	**Up to Rs. 20.00 Lakhs**

			Lakhs Up to Rs. 50.00 Lakhs	
	Current Account	Above Rs. 50.00 Lakhs	**Above Rs. 20.00 Lakhs** up to Rs. 50.00 Lakhs	**Up to Rs. 20.00 Lakhs**
	CC/OD	More Than 5 times of sanction limit		Up to 5 times of sanction limit

SECTION - F

Modalities of Implementing Bank's Policy on Know Your Customer (KYC) and Anti Money Laundering Measures (AML)

1. In tune with the guidelines prescribed by Reserve Bank of India, a separate policy on KYC & AML was prepared and the same was approved by the Board during its meeting held on 09.03.2011. The modalities of implementing the guidelines laid down in the policy Vis - a - Vis the detailed guidelines given by RBI in this subject are furnished below.

2. Need for prevention of Money - Laundering Activities

2.1 To protect Bank from

a) Reputation Risk.
b) Operation Risk. (Where chances of fraud come to light)
c) Legal Risk. (Leads to litigation)
d) Concentration Risk. (Affects Balance Sheet)
e) Compliance Risk. (Non-compliance leads to penalties)

2.2 It is obligatory on each bank as per the Prevention of Money Laundering Act, to report the Suspicious Activities and Cash transactions involving Rs. 10 lakh and above to the RBI. Probing of such transactions and respective customers is to be looked into by the investigative and law enforcement agencies.

3.0 Customer Profile: As part of Customer Acceptance Policy and Monitoring of suspicious Transactions (laid down in the main policy), each branch has to prepare the 'Risk Profile' of each customer and classify them as

a) Low Profile Customer (Level - I),
b) Medium Profile Customer (Level - II),
c) High Profile Customer (Level - III),

Based on the location, turnover, socio-economic status and based on the Risk Categorization mentioned herein below. The branch should exercise 'due diligence' while monitoring the transactions based on the data collected. Risk Categorization.

Categorization	Description	Due diligence level to be applied

Low Risk (Low profile Customer)	Salaried Accounts, Customers and firms with low-income turnover, Agricultural Customers, Accounts of Government Departments, PSUs, Regulatory bodies, SEBI etc. Customers having credit - debit summation of below Rs. 10 lakhs in a year	Basic level.
Medium Risk (Medium Profile Customer)	**Customers, Companies and firms having turn over of above Rs. 10 lakh and up to Rs. 50 lakhs in their accounts**	**Enhanced level**
High Risk (High Profile Customer)	Companies, Institutions and Firms having turn over of Rs. 50 lakh and above in their accounts.	Enhanced level

3.1 The Officer, authorizing the opening of the account should prepare the customer profile in the given format and sign the document. The customer profile contains information relating to customer identity, social/financial status nature of business activity, information about his business and their location etc. It is to be noted that the customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purpose.

4. Monitoring of Transactions

a) unusual and large value of Cash Transactions.

b) Transactions of suspicious nature.

c) Terrorism Finance.

4.1 Cash Transactions:

All Branches are advised to exercise 'due diligence' in the process of monitoring of transactions based on customer profiles prepared. In case of suspicious activities branches should exercise 'enhanced due diligence' and arrange to report then and there. The entire approach is Risk Based. For instance, if there is a sudden increase of deposit in an account from Rs. 10,000/- to Rs. 50 lakh and above, the branch should be in a position to give satisfactory explanation before the Law Enforcement Agencies. Such transactions are to be reported to the Head Office immediately.

4.2 It is mandatory on the part of all branches to issue TC's, DD's, MT's and TT's for Rs. 50,000/- and above only by debit to customer's account or against cheques but not against cash.

4.3 The branches should open a separate Register (if not done already) for recording cash withdrawals and deposits of Rs. 10 lakh & above and monitor such transactions followed by reporting to Head office.

4.4 All branches are advised to monitor transactions of just below the threshold limits fixed above and submit reports to the controlling authority.

4.5 All Branches are advised to monitor transactions of just below the threshold limits fixed above and submit reports to the controlling authority.

4.6 Transactions of suspicious nature:

The branches should look for unusual / irregular suspicious transactions. If the business activity goes out of the activity already declared by the customer and compiled in the customer profile and the transactions though apparently found legal and if there is no business logic, such transactions are to be monitored as suspicious. An indicative list of suspicious activities has been furnished below.

List of suspicious activities:

a) Corporate accounts where deposits or withdrawals are primarily in cash.
b) Corporate Accounts where deposits, withdrawals and remittances, transfers from/made to sources apparently unconnected with the corporate business activity/dealings.
c) Unusual applications for DD/TT/PO against cash
d) Accounts with large volume of credits through DD/TT/PO.
e) A single substantial cash deposit composed of many high denomination notes.
f) Frequent exchanges of small denomination notes for large denomination notes or vice versa.
g) Multiple accounts under the same name and sudden surge in activity level.
h) Sending or receiving frequent of large volumes of cross border remittances.
i) Remittances received by TT/DD/PO from various centre and in turn remitting the consolidated amount to a different account/sender on the same day leaving minimum balance in the account.

4.7 Terrorism Finance:

Lists of terrorist entities as notified by the Government from time to time are communicated to all Branches and has also been dealt with in the policy document.

Subject	**Reporting to HO**
To report Cash Transactions of Rs. 10 lakh and above the transactions just below the threshold limit	Fortnightly basis, (on or before 15th of every month
To report suspicious Cash Transactions of Rs. 10 lakhs and above and the transactions just below the threshold limit	On Quarterly basis (on or before 10th of January, April, July & October
Suspicious Activity Report (SAR) i.e.	To report as and when detected by SAR

Transactions of suspicious nature	

1. Maintenance of Records in respect of Non-Profit Organizations and filing of Non-Profit

2. Organization Transaction Reports (NTRs) to FIU-IND

In view of the Government of India Notification No. 13/2009/F.No.6/8/2009-ES dated November 12,2009 amending the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance or Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, UCBs should maintain proper record of all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency and to forward a report to FIU-IND of all such transactions in the prescribed format every month by the 15th of the succeeding month. UCBs should maintain these records for a period of ten years from the date of transactions.

9. Maintenance of Records and filing of Suspicious Transactions Reports (STRs) to FIU- IND in Respect of Walk-in Customers

Transactions carried out by a non-account-based customer, that is a walk-in customer, where the account of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. Further, if a bank has reason to believe that a customer is internationally structuring into a series of transactions below the threshold of Rs. 50,000.00 (Rupees Fifty Thousand) the bank should verify identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

The e-KYC service of the UIDAI is to be leveraged by UCBs through a secured network.

Any UCB willing to use the UIDAI e-KYC service is required to sign an agreement with

the UIDAI. The process flow to be followed is as follows:

1. Sign KYC User Agency (KUA) agreement with UIDAI to enable the UCB to specifically access e-KYC service. UCBs to deploy hardware and software for deployment of e-KYC service across various delivery channels. These should be Standardization Testing and Quality Certification (STQC) Institute, scanners at bank branches / micro-ATMs / BC points as per UIDAI standards. The current list of certified biometric scanners is given in the link below: http://www/stqc.gov.in/sites/upload_files/stqc/files/UID_Auth_Certlist_250613.pdf.

2. Develop a software application to enable the use of e-KYC across various Customer Service Points (CSP) (including bank branches, BCs etc.) as per UIDAI defined Application Programming Interface (API) protocols. For this purpose, UCBs will have to develop their own software under the broad guidelines of UIDAI. Therefore, the software may differ from UCB to UCB.

3. Define a procedure for obtaining customer authorization to UIDAI for sharing e-KYC data with the UCB. This authorization can be in physical (by way of a written explicit consent authorizing UIDAI to share his / her / Aadhaar data with the UCB / BC for the purpose of opening bank account) / electronic form as defined by UIDAI from time to time.

4. Sample process flow would be as follows:

a. Customer walks into CSP of a UCB with his / her 12-digit Aadhaar number and explicit consent and requests to open a bank account with Aadhaar based e-KYC

b. UCB representative manning the CSP enters the number into bank's e-KYC application software.

c. The customer inputs his / her biometrics via a VUIDAI compliant biometric reader (e.g. fingerprints on a biometric reader).

d. The software application captures the Aadhaar number along with biometric data, encrypts this data and sends it to UIDAI's Central Identities Data Repository (CIDR).

e. The Aadhaar KYC service authenticates customer data. If the Aadhar number does not match with the biometrics, UIDAI server responds with an error with various reason codes depending on type of error (as defined by UIDAI).

f. If the Aadhaar number matches with the biometrics, UIDAI responds with digitally signed and encrypted demographic information [Name, year / date of birth, Gender, Address, Phone and email (if available)] and photograph. This information is captured by UCB's e-KYC application and processed as needed.

g. UCB's server's auto populates the demographic data and photograph in relevant fields. It also records the full audit trail of e-KYC viz. source of information, digital signatures, reference number, original request generation number, machine ID for device used to generate the request, date and time stamp with full trail of message routing, UIDAI encryption date and time stamp, UCB's decryption date and time stamp, etc.

h. The photograph and demographics of the customer can be seen on the screen of computer at bank branches or on a hand-held device of BCs for reference.

i. The customer can open bank account subject to satisfying other account opening requirements.

ANNEXURE-VI

Category	**Eligible Foreign Investors**
I	Government and Government relate foreign investors such as foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International/ Multilateral Organizations / Agencies.
II	a. Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance / Reinsurance Companies, Other Broad-Based Funds etc. b. Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers / Advisors, Portfolio Managers etc. c. Broad based funds whose investment manager is appropriately regulated. d. University Funds and Pension Funds. e. University related Endowments already registered with SEBI as FII/Sub Account.
III	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments Charitable Societies / Trust, Foundations Corporate Bodies, Trusts, Individuals Family Offices, etc.

KYC documents for eligible EPIs under PIS FPI Type				
Document Type		Category I	Category II	Category III
Entity Level	Constitutive	Mandatory Documents	Mandatory	Mandatory
		(Memorandum and Articles of Association, Certificate of Incorporation etc.)		
	Proof of address	Mandatory (Power of Attorney {PoA} address is acceptable as address proof)	Mandatory (Power of Attorney address is acceptable as address proof)	Mandatory other than Power of Attorney
	PAN Card	Mandatory	Mandatory	Mandatory
	Financial Data	Exempted*	Exempted*	Mandatory

	SEBI Registration Certificate	Mandatory	Mandatory	Mandatory
	Board Resolution	Exempted*	Mandatory	Mandatory
Senior Management (Whole Time Directors / Partners / Trustees / etc.)	List	Mandatory	Mandatory	Mandatory
	Proof of Identity	Exempted*	Exempted*	Entity declares* on letter head full name, nationality, birth or submits photo identity proof
	Proof of Address	Exempted*	Exempted*	Declaration on Letter Head*
	Photographs	Exempted	Exempted	Exempted*
Authorized Signatories	List and Signatures	Mandatory-list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory
	Proof of Identity	Exempted*	Exempted*	Mandatory
Address	Proof of	Exempted*	Exempted* on Letter Head*	Declaration
	Photographs	Exempted	Exempted	Exempted*

6. Record of Non-Profit Organizations

As per the existing guidelines, Branches should maintain record of all transactions involving receipts by Non-Profit Organizations of value more than Rs. 10 lakhs and forward a report to FIU-IND every month. Accordingly, we may advise the branches to introduce a register as per the following format and furnish its copy to us once in a month.

Register of Transactions involving Receipts by Non-Profit Organizations of Value more Than Rs. 10 lakhs

Date	Name of the Non-Profit Organization	Amount (Only above Rs 10 lakhs)	Received From	Remarks

SECTION - G

AML RULES

1. Our Bank will not have any accounts or relationship with Shell Banks, nor Bank will undertake any transactions with or on behalf of Shell Banks. (A shell Bank is a Bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with any regulated group.)
2. Bank will maintain the record relation to transactions with customers for a period of 10 years from the date of transaction and records relating to identification of customer and address will be preserved for a period of 10 years after the business relationship is ended.
3. Bank will have in place for identification of those customers, on whose behalf accounts are maintained and operated
4. Bank assesses the affiliates and their customers' AML Policies and practices.
5. Bank undertakes AML training programmes for employees covering identification and reporting of transactions, to regulatory authorities, typologies of forms of money laundering involving our products, internal policies to prevent money laundering.

SECTION-H

MONEY MULE ACCOUNTS

As per the directives from the Reserve Bank of India (RBI) Bank has released Standard Operating Procedures(SOP) for dealing with Money Mules .We once again reiterate that these are all individuals or entities who transfer illegally obtained funds on behalf of others, often unknowingly, or in exchange for a financial incentive. These funds are typically from fraudulent activities, and money mules act as intermediaries, making it harder for authorities to trace the funds.

Branches/Head Office/IT Dept to arrange awareness campaigns that help customers recognize the risks of becoming a money mule. The campaigns often focus on warning signs such as receiving unsolicited requests to transfer money on behalf of someone else.

- The IT Dept at our HO, should release all such awareness videos thro' our social media platforms off and on.

- In addition to the above, Branches are advised to educate the customers informing them of risks of becoming a money mule.

Continue to create awareness among the customers for NOT sharing the OTP, Login Credentials and other banking security information and NOT to send money as initial deposit, commissions or transfer fee to anyone claiming to provide huge usually unrealistic, returns from known or unknown organizations /persons

Part of SOP on money mules, the following transactions are to be monitored to identify and reporting on Money mules. This is part and parcel of KYC/AML policy.

- All the newly opened accounts are to be closely monitored for high value transactions. (both Credit & Debit).

- Transfer of funds to multiple accounts from our account is to be monitored.

- Multiple inward transfers in a group or section of accounts.

- Where ever with drawls happening immediately after crediting in the accounts.

- Frequent with drawls in cash.

- Accounts opened and closed with short duration.

- High value transactions in all the newly opened accounts/ suspicious accounts.

- Break down of large transactions into smaller amounts to avoid depositing thresholds.

- Layering through multiple accounts: Transferring funds between multiple accounts (within the same bank or different banks to obscure the Audit Trial.

- Complex fund movement between related parties or entities.

- Transactions conducted through accounts of unrelated third parties without a clear business relationship.

- Exception transactions are to be examined in case of abnormally frequent and large transactions in domestic bank accounts being carried out from locations including

from overseas jurisdictions, not matching to the location/ economic/financial profile of the customer.

- Monitor Cash withdrawals through overseas ATMs and ATMs outside the state where customer resides. Especially transactions happened at Dubai, Kazakhstan, Thailand.

- Carry out enhanced due diligence in current accounts where in there are huge volume of transactions, inconsistent with the declared turnover or business profile. It was observed by RBI, that current accounts opened by sole proprietorship firms using MSME certificate are used to transfer/Layer the proceeds of Crime.

- Branches are further advised to generate Exceptional Transaction report along with day end reports and should be placed before the Branch Head for scrutiny and Instructions.

Chief Executive Officer