THE ARYA VAISHYA COOPERATIVE BANK LTD.,
REGISTERED OFFICE, HOSUR, HUBBALLI- 580021

KYC & AML POLICY

Reserve Bank of India has issued regulatory guidelines on know your customer norms/Antimoney Laundering (AML)Standards/combating of Financing of Terrorism(CFT) from time to time, This master circular consolidates all guidelines issued by Reserve Bank of India on KYC/AML/CFT norms up to June 30,2008. Banks were advised to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. These know your customer guidelines have been revised in the context of Recommendation made by the Financial Action Task Force(FATF) on Anti Money Laundering (AML) Standards and on Combating Financing of Terrorism(CBT) Detailed guidelines based on the Recommendation of the Financial Action Task Force and the paper issued on Customer Due Diligence(CDD) for banks by the Basel Committee on Banking supervision with the indicative suggestions wherever considered necessary have been issued the policy frame work on know your customer and Anti money Laundering measures are put in plan as below for the purpose to adopt these norms with effect from 01-04-2018

Definition of Customer:

For the purpose of KYC policy a customer is defined as :

1) A person of entity that maintains an account /or has a business relationship with us.
2) One on whose behalf the account is maintained (i.e. beneficial owner)
3) Beneficious of transactions consolidated by professional informatives. Share or stock brokers charted Accountants solicitors as formatted under the law.
4) Any person or entity connected with a financial transaction which can loose significant reputation or other risks to the bank, say a transfer or issue of a high value demand draft as a single transaction.

General:

1) The information collection from the customer for the purpose of opening of account is to be transacted as confidential and details these of are not to be divulged for cross selling or any other like purposes ensure that information sought from the customer is relevant to the perceived risk, is not introgive, and is in conformity with the guidelines issued in this regard and any other information from the customer should be sought separately with his/her consent and after opening the account.
2) It should be ensured that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of traveler cheques for value of Rs. Fifty thousand and above is effected by debit to the customers account or against cheques and not against cash payment.

3) It should be ensured that the provision of foreign contribution(Regulation)Act 1976, as amended from time to time whenever applicable are strictly adhered to

2.2 KYC POLICY

Our bank has framed KYC policies incorporating the following Key elements:

a) Customer acceptance policy
b) Customer identification procedures
c) Monitoring of transaction and
d) Risk management.

2.3 Customer Acceptance Policy(CAP)

a) our bank has to develop a clear customer acceptance policy laying down explicit criteria for acceptance of cutoemrs. The customer acceptance policy will ensure that explocit guidelines. Are in the place on following aspects of customer relationship in the bank. As such the following shall be compliet by “staff of the bank” under customer acceptance policy.

i) No account should be opened in anonymous or fictitious/benami name(s):
ii) 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 ternover, social and financial status etc to be enable categorization of customers in to low, medium and high risk.

Level 1 (Low risk):

Regular customer with good track record or performance in the past as also in the present with reasonable good operations in the account without any return of cheques presented in the clearing for the purpose of risk categorization, individual (other than high net worth) and entities whose identities and sources of wealth can be easily identifies, and transactions in whose accounts lay by and large conform to the known profile, amy be categorized as under, low risk illustrative examples of low risk customers could be salaried employees whose salary structures and well defined, people belonging to lower economic state of the society whose accounts show small balances and low turnover government departments and government owned companies regulators and statutory bodies etc. in such cases the policy may require that only the basic requirements of verifying the identify and location of the customer are to be met.

Level II(Medium Risk)

Those customers wherein there is loan a/c in the payament of the principal or payament of interest in the loan account and keeping the current and savings bank account in operative or there are huge operations in the savings and current account disproportionate to the known sources of income.

Level III(High Risk)

(i) Are those customers where there are no good operations in the account, which bring a political

influence for non-payment of interest , non-payment of the principal in the loan account, keep the current and savings bank accounts without any operations. Frequent return of cheques, frequent request for temporary overdraft in the current account as also heavy cash remittance as also withdrawal on a continued basis who come under the high risk category.

(ii) Customers who are likely to pose a higher than average risk to the bank should be categorized as medium or high risk depending on cutomers background nature & location of activity. Country of origin, sources of funds and his client profile etc should apply enhanced due diligence measures based on the risk assessment. Thereby requiring intensive “due diligence” for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence include(a) non resident customers. (b) high net worth individual (c) trusts, charities NGOs and organizations receiving donations(d) companies having close family share holding 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.

(iii) Documentation requirements and their information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirement of PML Act 2002 and instruction/guidelines issued by Reserve Bank from time to time should be kept in mind by the staff of the Bank while opening any type of deposit account.

(iv) The staff shall not 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 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. The staff incase fails to get the required information for opening the deposit account, should be highly polite even in rejecting the request of the customer to open a deposit account. Hence it is always necessary for the staff to bring in such instances to the notice of the manager whose responsibility will be to convince the depositor for furnishing the required information or politly reject opening of deposit accounts explaining the reasons for such a decision.

(v) Operations of deposits accounts under power of attorney should be dealt with very cautiously by the

members of staff. All necessary formalities for opening the accounts should be followed without which such account should not be opened. In case of any problem in getting the information or advise of the customers to said customers has to taken to the Manager, whose responsibility is to either collect the required information or politely request the customer his inability to either open an account or allow operations in the account. All relevant law and practice under the banking practice should be adhered to while dealing the such customers.

(vi) The staff of the bank should not open the accounts without ensuring that the identity of the customer matches with documentary evidences submitted by him. This will ensure that no person with any criminal background or in an unauthorized manner opens and operate an account in the bank.

(vii) The staff concened should prepare a profile for each new customer based on the risk perception as given above. The customer profle may contain information relating to customers identity, social/financial status, nature of business activity information about is clients business and their location etc. the nature and extent of due diligence will depend on the risk perceived by the bank. However while preparing customer profile staff should take care to seek only such information

from the customer, which is relevant to the risk category and is not intrusive.

Incendentally the customer profile is a confidential document and details contained there in should not be deverged for cross selling or any other purposes.

(viii) It is important for the staff of the bank to bear in mind that the adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of banking serves to general public, expecially to those, who are financially or socially disadvantaged.

Customer identification procedure(CIP)

The customer identification procedure is to be carried out at different stage i.e.. while establishing a banking relationship carrying out a financial transation or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. It means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Staff concern need to obtain sufficient information necessary to establish to their satisfaction the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. In other words that the staff must be able to satisfy the competent authorities that due diligence was oserved based on the risk profile of the customer in compliance with the extent

guidelines in place. This perception is to avoid disproportionate cost to bank and a burdensome regime for the customers.

Besides risk perception the nature of information/documents required to be obtained by the staff would also depend on the type of customer(individual, corporate etc.) For the customers that are natural persons, the bank should 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 bank should(i) verify the legal status of the legal person/entity through proper and relevant documents (ii) verify that any person to act on behalf of the legal person/entity is so authorized and identity 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 case. Especially legal persons requiring an extra elements of caution are as under:-

Customer identification requirements- Indicative guidelines.

1. Trust/Nominee or Fiduaciary Accounts.:- There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Staff concerned should determine whether the customer is acting on behalf or another person as trustee/nominee or any other intermediary. If so, they should 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, staff should take reasonable precaustions to verify the identity of the trustee and the settlers of trust(including any person settling assets into the trust)granters protectosrs, beneficiaries and signatories.

2. Accounts of companies and firms. : staff concened need to be vigilant against business entities being used by individuals as a front for maintaining acconts with banks. They should examine the control structure of the entity determine the source of funds and identify the natural persons who have a controlling interests and which comprise the management.
3. Client accounts opened by professional- intermediaries. :- when the staff has knowledge or reason to believe that the client account opened by a professional intermediaries is on behalf of a single clent that clent must be identified by the said staff.
4. The staff concened should make a periodical updation of customer identification data(including photographs) after the account is opened depending the risk factor involved in individual deposit accounts. However if any observation in respect of the customers are noticed or observed at any point of time the same should updated immediately.
5. Accordingly, the KYC/procedure also provides for opening accounts for those persons who intend to keep balances not exceeding rupee fifty thousand (Rs. 50,000/) in all their accounts taken together and the total credit in all the

accounts taken together is not expected to exceed rupees on lakh(R.s 1,00,000/-) in a year. In such cases, if a person who wants to open an account and is not able to produce documents staff concened should open an account for him, subject to introduction from another account holder who has been subjected to full KYC procedure. The introduces account with the bank should be at least six months old and should show satisfactory transactions, photograph of the customer who proposes to open the account and also his address needs to be certified by the introducer, or any other evidence as to the identity and address of the customer to the identity and address of the customer to the satisfaction of the bank.

iii) While opening accounts as described above, the customer should be made aware that if at any point of time, the balances in all his/her accounts with the bank(taken together) exceeds Rupees Fifty thousand (Rs. 50,000/-) or total credit in the account exceeds Rupeesone lakh(Rs. 1,00,000/-) in a year, no further transactions will be permitted until the full KYC norms are complied with.

iv) In order not to inconvenience the customer, the bank must notify the customer when the balance reaches Rs. Forty thousand(Rs. 40,000/-) or the total credit in a year reaches Rs. Eighty thousand (Rs.80,000/) that appropriate documents for conducting the KYC must be submitted otherwise operations in the account will be stopped.

Monitoring of Transactions.

The staff concerned of the Bank should on an ongoing monitor the operations in all the deposit account to reduce the risk involved. Staff concerned should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible(lawfull purpose. High-risk accounts have to be subjected to intensified monitoring.

Closure of accounts.

Where the staff concerned is unable to apply appropriate KYC measures due to non-furnishing of information and for non cooperation by the customer, the bank should consider closing the account or terminating the banking/business relationship after issuing due notice to the customers explaining the reasons for taking such a decision such decisions will be taken by the manager of the bank.

Introduction of new technologies.

Banks should pay special attention to any money laundering threats that may arise from clearing, RTGS etc. the staff of the bank in charges of investments issue of demand drafts, pay orders, etc., should be carefull in ensuring the money belong to the customers and the same should be verified periodically.

Principal officer.

In terms of the requirement of the extent instructions of RBI, our bank has appointed the manager designating him as principal officer. He is responsible for monitorising and reporting of all transactions and sharing of information as required under the law.

He will maintain close bison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combaling financing of terrorism, he will be responsible for times submission of CTR,STR and reporting of counterfeit note to FIU-IND.

Maintenance of records of transactions/information to be preserved/maintenance and preservation of records/cash and suspicious transactions reporting of financial intelligence unit india(FIU-INDIA)

(i) Maintenance of records of transactions.

Bank will introduce a system for maintain proper record of transactions prescribed under Rule 3 in respect of a) all transactions of the value of more than rupees ten lakh or etc., equilent in foreign currency b) all series of cash transactions integrally connected to each other which have been valued below ruppes ten lakh or etc. equilent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh c) all cash transactions where forged or counterfeet currency notes or bank notes have been used as genine and where any forgery of a valuable security or a document has taken place facilitating the transaction. d) all suspicious transactions whether or not made in cash and by way of as mentioned in the rules. As of now the software developed by the bank includes all the above

provisions based on which the monthly return is being submitted to the government.

ii) information to be preserved.

Staff may keep the following instructions for preservation of records in this regard as per requirements of rule 3;

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

iii) maintenance and preservation of records.

a) Manager may maintain the records containing information in respect of transactions referred to in rule 3 above. Bank should take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrived easily and quickly whenever required or when requested by the competent authorities, further, bank should maintain for at least ten years from the date of cessation of transaction between the bank and the client all necessary records of transaction both domestic or internal which will permit reconstruction of individual transactions (including the amounts and types of currency involves if any) so as to provide, if necessary evidences for prosecution of persons involved in criminal activity.

b) The manager has been advised to ensure that records pertaining to the identification of the customer and his address(e.g. copies of documents like passport identity cards-driving licenses, PAN card utility bills etc.) obtained while opening the account and during the course of business relationship are properly preserved for at least ten years after the business relationship is ended. The identification records and transaction data should be made available to the competent authorites upn request.

c) The manager has also been to pay special attention to all complex, unusual large transactgions and all unusual patterns of transactions which have no apparent economic or visible lawfull purpose it is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purposr ther of should, as for as possible, be examined and the findings at branch as well as principal officer level should be properly recorded such records and related documents should be made available to help auditors in their day to day work relating to scrutiny of transactions and also to reserve bank/other relevant authorites. These records as per the extent instructions are required to be preserved for ten years as is required under PMLA 2002. The manager has been advised to take action accordingly.

Reporting to financial intelligence unit-india.

a. In terms of the PMLA Rules, bank is required to report information relating to cash and suspicious transactions

to the directors. Financial intelligence unit-india(FIU-IND) in respect of transactions referred to in rule 3 at the following address.

Directo, FIU-IND, Financial Intelligence Unit India, 6th floor, “hotel Samrat”, Chanakya puri, New Delhi- 110021.

The managers have been advised to go through the contents of the instructions in this regard and be prompt in compiling the information and furnishing the same to the government as per annexure enclosed.

The bank has to procure a software or adopt CBS for compiling and forwarding the information to the governement.

Customer education/employees training/the staff of the bank will be deputed on a continuing basis for various training programmes including the one on KYC/AML.

ANNEX-1

Customer Identification procedure.

Features to be verified and documents that may be obtained from customers features documents.

Accounts of individuals.

1. Legal name and any other names used .
2. Correct permanent address.

i) PASS Port, ii) PAN card iii) Voters identity card. Iv) driving licence. V) identity card(subject to the banks satisfaction) vi) letter from a recognized public authority or public servent verifying the identity and residence of the customer to the satisfaction of bank. Vii) telephone bill

viii) bank account statement ix) letter from any recognized public authority x) electricity bill xi) letter from employer(subject to satisfaction of the bank.(any one document which provides customer information to the satisfaction of the bank will suffice.)

Accounts of companies:- 1) Name of the company 2) principal place of business. 3) Mailing address of the company 4) telephone/Fax number 5) certificate of incorporation and memorandum & articles of association. 6) resolution of the board of directors to operate an account and identification of those who have authority to operate the accounts. 7) power of attorney granted to its manager officers or employees to transact business on etc. behalf. 8) copy of PAN allotement letter. 9) copy of the telephone bill .

Accounts of partnership firms.:- 1) Legal Name 2) Address 3) Name of all partners and their address 4) telephone numbers of the firm & partners 5) registration certificate if registered 6) partnership deed 7) power of attorney granted to a partners or an employee of the firm to transact business on its behalf. 8) any officially valid document identifying the partners and the persons holding the power of attorney and their address. 9) telephone bill in the name of firm/partners.

Accounts of trusts and foundations. :- 1) name of trustees, settlers, beneficiaries and signatories. 2) names and address

of the founder the managers/directors and the beneficiaries. 3) telephone/fax numbers. 4) certificate of registration, if registered 5) powers of attorney granted to transact business on its behalf any officially valid document to identify the trustees, settlers, beneficiaries and those holding power of attorney founders/managers/directors and their addresses.6) resolution of the managing body of the foundation/association. 7) telephone bill

Annex-II

1. Cash transaction report(CTR) 2) summery of CTR. 3) electronic file structure (CTS) 4) suspicious transaction report(STR) 5) electronic file structure STR 6) counter feir tcurrency report(CCR) 7) summery of CCR. 8) electronic file structure- CCT.

It is to be downloaded from internet from the site given above and enclosed to the policy on KYC.

Hubli.

Date :30-05-2024 Gen. Manager Director Director Chairman