

PREVENTION OF MONEY LAUNDERING- PMLA POLICY

(Approved by the Board on May 30, 2013 and further amended on January 30, 2017)

Prevention of Money Laundering- PMLA Policy

1) Preamble

In terms of the Guidelines issued by the Reserve Bank of India on Know Your Customer (KYC) Standards and Anti Money Laundering (AML) measures, NBFCs are required to put in place a comprehensive policy frame work covering KYC Standards and AML Measures. The guidelines issued by the Reserve Bank of India take into account the recommendations made by the Financial Action Task Force (FATF) and inter government agency, on AML Standards and on combating financing terrorism. The guidelines also incorporate aspects covered in the Basel Committee document on customer due diligence which is a reflection of the International Financial Community's resolve to assist law enforcement authorities in combating financial crimes.

This policy document is prepared in line with the RBI guidelines and incorporate the Company's approach to customer identification procedures, customer profiling based on the risk perception and monitoring of transactions on an ongoing basis.

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities.

2) Definition of Money Laundering

Section 3 of the Prevention of Money Laundering [PML] Act 2002 has defined the "offence of money laundering" as under:

"Whoever directly or indirectly attempts to indulge or knowingly assists or knowingly is party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".

For the purpose of this document, the term money laundering would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of the funds.

3) Obligations under Prevention of Money Laundering [PML] Act 2002

Section 12 of PML Act 2002 places certain obligations on every banking company, financial institution and intermediary which include:

- a. maintaining a record of prescribed transactions
- b. Furnishing information of prescribed transactions to the specified authority
- c. Verifying and maintaining records of the identity of its clients
- d. Preserving records in respect of (a), (b), (c) above for a period of 10 years from the date of cessation of transactions with the clients

4) Policy Objectives

- a. To prevent criminal elements from using the Financial System for money laundering activities.
- b. To enable the Company to know/understand the customers and their financial dealings better, which in turn would help the Company to manage risks prudently.
- c. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- d. To comply with applicable laws and regulatory guidelines.
- e. To take necessary steps to ensure that the concerned staff are adequately trained in KYC/AML procedures.

5) **Compliance of KYC policy**

The Company will ensure compliance with KYC Policy through:

- (a) Head Compliance being 'Senior Management' for the purpose of KYC compliance.
- (b) Allocating responsibility for effective implementation of policies and procedures.
- (c) Independent evaluation of the compliance functions of Company's policies and procedures, including legal and regulatory requirements.
- (d) Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
- (e) Submission of quarterly audit notes and compliance to the Audit Committee

6) **Scope**

This policy is applicable to all branches/offices of the Company and is to be read in conjunction with related operational guidelines issued from time to time.

7) **Definition of term 'Customer':**

For the purpose of KYC policy, a 'Customer' may be defined as :

- a. a person or entity that maintains an account and/or has a business relationship;
- b. one on whose behalf the account is maintained (i.e. the beneficial owner);
- c. beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- d. any person or entity connected with a financial transaction which can pose significant reputational or other risks to the company

8) **Key Elements of the Policy**

KYC policy includes the following key elements:

- a. Customer Acceptance Policy
- b. Customer Identification Procedures
- c. Monitoring of Transactions
- d. Risk Management

9) **Customer Acceptance Policy**

The Company will:

- a. accept customers after verifying their identity as laid down in Customer Identification Procedures.
- b. carry out classification of customers into various risk categories and based on risk perception decide on acceptance criteria for each category of customers
- c. accept only clients in respect of whom complete KYC procedures has been completed. Client account shall not be opened in case the client fails to submit required documents and

- d. Photocopies of documents submitted by the clients shall be compulsorily verified with original, with signature of person verifying shall be put as proof verification.
- e. not open account in any anonymous or fictitious/ benami name(s);
- f. Not open an account or close an existing account where the company is unable to apply appropriate customer due diligence measures i.e. company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non cooperation of the customer or non reliability of the data/information furnished , after giving reasonable notice.
- g. apply 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.
- h. specify the mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- i.obtain 'Optional'/additional information, with the explicit consent of the customer after the account is opened.
- j. CDD (Customers Due diligence) Procedure is followed for all the joint account holders, while opening a joint account.
- k. specify circumstances in which, a customer is permitted to act on behalf of another person/entity.
- l. put in place Suitable system to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
- m. that the Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

10) Customer Identification Procedures

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

CGCL shall carry out customers' due diligence based on the risk profile of the customer. Apart from risk profile, the nature of information/documents required would also depend on the type of customer (Individual, Corporate etc.)

CGCL shall carry out customers' due diligence when it is Selling third party products as agents, selling their own products for more than rupees fifty thousand.

As also, CGCL shall carry out customers' due diligence when it has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

For customers that are natural persons, CGCL shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph, documents for verifying signature.

For customers that are legal persons or entities, CGCL shall (i) verify the legal status of the person/entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

Enhanced Due Diligence: CGCL shall adopt enhanced due diligence in case of all High risk customers as also in respect of a customers with specific types of relationships. Indicative list of legal persons requiring an enhanced due diligence are given in Annex-I for guidance.

Also, indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in the Annex-II.. The prior approval of Head- Compliance shall be necessary for accepting any document other than the one listed in Annex II

Unique Customer Identification Code for Customers (UCIC)

CGCL shall introduce Unique Customer Identification code identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers.

Further , while undertaking customer identification , the Company will ensure following ,;

- (a) Decision-making functions of determining compliance with KYC norms will not be outsourced.
- (b) Introduction will not be sought while opening accounts.
- (c) The customers shall not be required to furnish an additional OVD (Officially valid documents) , if the OVD submitted by the customer for KYC contains both proof of identity and proof of address.
- (d) The customers shall not be required to furnish separate proof of address for permanent and current addresses, if these are different. In case the proof of address furnished by the customer is the address where the customer is currently residing, a declaration shall be taken from the customer about her/his local address on which all correspondence will be made by the Company.
- (e) The local address for correspondence, for which their proof of address is not available, shall be verified through 'positive confirmation' such as acknowledgment of receipt of letter, visits to the place, or the like.
- (f) In case it is observed that the address mentioned as per 'proof of address' has undergone a change, Company shall ensure that fresh proof of address is obtained within a period of six months.

11) Monitoring of Transactions

Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or viable lawful purpose. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer will be subjected to detailed scrutiny.

After due diligence at the appropriate level in the Company, transactions of suspicious nature and/or any other type of transaction notified under PML Act, 2002 will be reported to the appropriate authority and a record of such transactions will be preserved and maintained for a period as prescribed in the Act.

12) Risk Management

While the Company has adopted a risk based approach to the implementation of this Policy. It is necessary to establish appropriate framework covering proper management oversight, systems, controls and other related matters.

The Principal Officer designated by the Company in this regard will have an important responsibility in managing oversight and coordinating with various functionaries in the implementation of KYC/AML policy.

Internal Audit shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the Audit Committee of the Board at periodic intervals.

13) Customer Due Diligence/Risk Categorization Of Customers:

All customers shall be categorized on the basis of the risk of money laundering or terrorist financing that they are likely to pose. The classification of customers into various risk categories shall be carried out based on risk perception and on acceptance criteria for each category of customers. The following guidelines shall be adopted while preparing separate guidelines for profiling customers based on risk categorization:

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

CGCL shall put in place process of identifying and applying enhanced due diligence in respect of Politically Exposed Persons (PEPs), customers who are close relatives of PEPs, and accounts of which PEP is the ultimate beneficial owner. Also, in the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, CGCL shall obtain senior management approval to continue the business relationship and subject the account to the due diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

Documentation requirements and other information to be collected in respect of different categories of customers shall be as per perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;

For the purpose of risk categorisation, 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 categorised as low risk. Illustrative examples of low risk customers could be Government departments & Government owned companies and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer are required to be met.

Company shall 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 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.

Periodic Updation

Company shall put in place a system of periodical updating of customer identification data after the account is opened. Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers subject to the following conditions:

- (a) Fresh proofs of identity and address shall not be sought at the time of periodic updation, from customers who are categorised as 'low risk', when there is no change in status with respect to their identities and addresses and a self- certification to that effect is obtained.
- (b) A certified copy of the proof of address forwarded by 'low risk' customers through mail/post, etc., in case of change of address shall be acceptable.
- (c) Physical presence of low risk customer at the time of periodic updation shall not be insisted upon.
- (d) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.
- (e) Fresh photographs shall be obtained from customer for whom account was opened when they were minor, on their becoming a major.

Part I - CDD Procedure in case of Individuals

Company shall obtain the following documents from an individual while establishing an account based relationship:

- (a) one certified copy of an OVD as mentioned in annexure II containing details of identity and address;
- (b) one recent photograph; and
- (c) such other documents pertaining to the nature of business or financial status specified in KYC policy.

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

The e-KYC service of Unique Identification Authority of India (UIDAI) will be accepted as a valid process for KYC verification under the PML Rules, as

- (a) the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process is treated as an 'Officially Valid Document', and
- (b) transfer of KYC data, electronically to the RE from UIDAI, is accepted as valid process for KYC verification.

Provided Company shall obtain authorization from the individual user authorizing UIDAI by way of explicit consent to release his/her identity/address through biometric authentication to the Company.

Company shall print/download directly, the prospective customer's e-Aadhaar letter from the UIDAI portal or e-KYC procedure as mentioned above shall be adopted, if such a customer knows only his/her Aadhaar number or if the customer carries only a copy of the e-Aadhaar downloaded from a place/source elsewhere.

A copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the 'officially valid document' in the existing name of the person shall be obtained for proof of address and identity, while establishing an account based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise.

In case the person who proposes to open an account does not have an OVD as 'proof of address', such person shall provide OVD of the relative as provided at sub-section 77 of Section 2 of the Companies Act, 2013, read with Rule 4 of Companies (Specification of definitions details) Rules, 2014, with whom the person is staying, as the 'proof of address'.

If an existing KYC compliant customer of a Company desires to open another account with the same Company, there shall be no need for a fresh CDD exercise.

Part II - CDD Measures for Sole Proprietary firms

For opening an account in the name of a sole proprietary firm, a certified copy of an OVD as mentioned in Annexure II containing details of identity and address of the individual (proprietor) shall be obtained.

In addition to the above, any two of the documents as prescribed in annexure II as a proof of business/activity in the name of the proprietary firm shall also be obtained:

In cases where the Company is satisfied that it is not possible to furnish two such documents, Company may, at their discretion, accept only one of those documents as proof of business/activity.

Provided Company undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part III- CDD Measures for Entities other than Individuals/ Sole Proprietary firms

- i) For opening an account of a company, one certified copy of each of the documents as per Annexure II shall be obtained:
- ii) For opening an account of a partnership firm, one certified copy of each of the documents as per Annexure II shall be obtained:
- iii) For opening an account of a trust, one certified copy of each of the documents as per Annexure II shall be obtained:
- iv) For opening an account of an unincorporated association or a body of individuals, one certified copy of each of the documents as per Annexure II shall be obtained:

Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the Rules to verify his/her identity shall be undertaken keeping in view the following:

- (a) Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
- (b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

On-going Due Diligence

Company shall undertake on-going due diligence of customers to ensure that its transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

The extent of monitoring shall be aligned with the risk category of the customer.

Explanation: High risk accounts have to be subjected to more intensified monitoring. i.e. A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures will be put in place.

Partial freezing and closure of accounts

- (a) Where Company is unable to comply with the CDD requirements mentioned at Part I to V above, it shall not open accounts, commence business relations or perform transactions. In case of existing business relationship which is not KYC compliant, Company shall ordinarily take step to terminate the existing business relationship after giving due notice.
- (b) As an exception to the Rule, Company shall have an option to choose not to terminate business relationship straight away and instead opt for a phased closure of operations in this account as explained below:
- i. The option of 'partial freezing' shall be exercised after giving due notice of three months to the customers to comply with KYC requirements.
 - ii. A reminder giving a further period of three months shall also be given.
 - iii. Thereafter, 'partial freezing' shall be imposed by allowing all credits and disallowing all debits with the freedom to close the accounts in case of the account being KYC non-compliant after six months of issuing first notice.
 - iv. All debits and credits from/ to the accounts shall be disallowed, in case of the account being KYC non-compliant after six months of imposing 'partial freezing',
 - v. The account holders shall have the option, to revive their accounts by submitting the KYC documents.
- (c) When an account is closed whether without 'partial freezing' or after 'partial freezing', the reason for that shall be communicated to account holder.

Enhanced Due Diligence Procedure

Accounts of non-face-to-face customers: Company shall include additional procedures i.e., certification of all the documents presented, calling for additional documents and the first payment to be effected through the customer's KYC complied account with another Company/Financial Institution, for enhanced due diligence of non-face to face customers.

Accounts of Politically Exposed Persons (PEPs)

Company shall have the option of establishing a relationship with PEPs provided that:

- (a) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
- (b) the identity of the person shall have been verified before accepting the PEP as a customer;
- (c) the decision to open an account for a PEP is taken at a senior level in accordance with the Company's Customer Acceptance Policy;
- (d) all such accounts are subjected to enhanced monitoring on an on-going basis;

- (e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, approval of Head Compliance is obtained to continue the business relationship;
- (f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

These instructions shall also be applicable to accounts where a PEP is the beneficial owner

Hiring of Employees and Employee training

- (a) Adequate screening mechanism as an integral part of personnel recruitment/hiring process shall be put in place.
- (b) Employee training programme will be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff will be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the Company, regulation and related issues will be ensured.

Adherence to Know Your Customer (KYC) guidelines

- (a) Persons authorised by Company for collecting the deposits and its brokers/agents or the like, shall be fully compliant with the KYC guidelines as applicable
- (b) All information shall be made available to the Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by the Company
- (c) The books of accounts of persons authorised by Company including brokers/agents or the like, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection whenever required.

14) Customer Education

The Company recognizes the need to spread awareness on KYC, Anti Money Laundering measures and the rationale behind them amongst the customers and shall take suitable steps for the purpose.

15) Introduction of New Technologies

Company will pay special attention to the money laundering threats arising from new or developing technologies and take necessary steps to prevent its misuse for money laundering activities. Company will ensure that appropriate KYC Procedures are duly applied to the customers using the new technology driven products.

16) KYC for the existing accounts

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

17) Principal Officer [Money Laundering Reporting Officer]

Company will designate a senior officer as Principal Officer who shall be responsible for implementation of and compliance with this policy. The illustrative duties of Principal Officer will be as follows:

- a. Monitoring the implementation of the Company's KYC/AML Policy.
- b. Reporting of transactions and sharing of the information as required under law
- c. Maintaining liaison with law enforcement agencies.
- d. Ensuring submission of periodical reports to the top Management / Board.

18) Reporting Requirements to Financial Intelligence Unit - India

Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Company will not put any restriction on operations in the accounts where an STR has been filed. Company shall keep the fact of furnishing of STR strictly confidential. Company will ensure that there is no tipping off to the customer at any level.

Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

CGCL shall adhere to requirements of reporting Cash Transactions Reports(CTR) & Suspicious Transactions Report(STR) , maintenance of records of transactions & preservation of information, reporting to FIU-IND

The Principal Officer shall be responsible for reporting of Suspicious transactions & Cash transactions of Rs.10 lakhs & above. The Indicative List of Suspicious Transactions is provided in Annex III for guidance in defining any transaction as suspicious in nature

Maintenance of records of transactions: CGCL shall maintain proper record of transactions prescribed under Rule 3, as mentioned below:

- a. all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- b. all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakhs;

- c. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- d. all suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act , 2002.

Information to be preserved: CGCL shall maintain the following information in respect of transactions referred to in Rule 3:

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

Maintenance & Preservation of Records: CGCL shall preserve account information related documents for at least ten years from the date of cessation of transaction between CGCL and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

CGCL shall ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, 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 Principal Officer of the company shall ensure that information relating to cash & suspicious transactions are reported to the Director, Financial Intelligence Unit – India (FIU – IND) at the following address:

**Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021**

The following reporting requirements shall be adhered to

- a. The cash transaction report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, individual transactions below rupees fifty thousand may not be included;
- b. The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction is received from a branch or any other office. Such report should be made available to the competent authorities on request;
- c. CCR(Counterfeit Currency Report) to be furnished to FIU-IND relating to all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions.
- d. The Principal Officer will be responsible for timely submission of CTR, STR and CCR to FIU-IND

19) Combating Financing Terrorism:

CGCL shall ensure that before opening any new account , name/s of the proposed customer does not appear in the updated list of individuals/entities in the United Nations website at

<http://www.un.org/sc/committees/1267/consolist.shtml>.

Further, CGCL shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to RBI and FIU-IND.

20) Other Instructions

Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

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

Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. However it is to be started as and when it becomes applicable to the Company

21) Review of the Policy

The policy will be reviewed as and when considered necessary by the Board.

ANNEXURE I Customer Identification requirements
(Indicative Guidelines)

1) Trusts/Nominees or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. It shall be determined whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting shall be insisted, as also shall obtain details of the nature of the trust or other arrangements in place. Due diligence in such cases shall be enhanced. CGCL shall take reasonable precautions to verify the identity of the trusts and the settlers of the trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of 'foundation', steps shall be taken to verify the founder managers / directors and the beneficiaries, if defined.

2) Transactions with companies and firms:

CGCL shall be vigilant against business entities being used by individuals as a "front" for transactions. CGCL shall examine control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements shall be moderated according to the risk perception i.e. in the cases of public limited company it will not be necessary to identify all the shareholders.

3) Transactions through the professional intermediaries:

CGCL does not hold "pooled" accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds etc. However, in cases where CGCL rely on the "Customers Due Diligence" (CDD) done by an intermediary, they shall satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirement. CGCL shall take the responsibility for knowing the customer.

4) Transactions with Politically Exposed Persons (PEPs) resident outside India:

Politically exposed persons are individuals who are or have been entrusted with prominent public functions' in a foreign country i.e. Heads of States or of Government, senior politicians, senior govt./judicial/military officers, senior executives of state owned corporation. It would be necessary to gather sufficient information on any person who is connected with the customer in any capacity and check all the information available on the person in the public domain. Identity of such person may be verified and information about sources of funds may be obtained before accepting PEP as a customer. Similarly the utilization of funds provided by CGCL may be verified to ensure that funds are utilized for the purpose for which it is given. The decision to accept PEP as customer shall be approved by VP and above. Such customers shall be subject to enhanced monitoring on an ongoing basis. The above norms shall be applicable in the case of family members or close relatives of PEPs.

5) Accounts of non-face to face customers:

In the case of non face to face customers, apart from applying the usual customer identification procedures, certification of all documents presented shall be insisted upon and if necessary, additional documents shall be called for.

Annexure II Customer Identification Procedure (Indicative List of Documents To Be obtained from different Types of Customers)

<u>Type of Customers</u>	<u>Documents to be Obtained</u>
Individual For Identification & Address	<ol style="list-style-type: none"> 1) Passport 2) PAN Card 3) Voter's identity Card issued by Election Commission of India 4) Driving License with photograph 5) Aadhaar Card 6) Job Card Issued by NREGA duly signed by an officer of the State Government
Non Resident Indians-Individuals	<ol style="list-style-type: none"> 1) Copies of Passport and Residence Visa, 2) a valid document indicating foreign residential address and passport size photographs of the applicant. 3) The applicant is to be duly introduced by Banker/ Notary Public/ Indian Embassy/ Local customer who has been subjected to full KYC Procedure.
Accounts of Companies Name of the company Principal place of business Mailing address of the company, Telephone/Fax Number	<ol style="list-style-type: none"> 1) Certification of Incorporation 2) Memorandum and Articles of Association 3) Current list of directors 4) Resolution of the Board of Directors or Power of Attorney issued for opening of the account and delegating powers to operate the account(s) of the company/corporation <p>Any of the documents for identity of each the directors/ authorized officials (as given above for individuals) and their addresses Recent passport size Photographs of directors/authorized officials.</p>
Accounts of partnership firms Legal name Address Names of all partners and their addresses Telephone numbers of the firm and partners	<ol style="list-style-type: none"> 1) Registration certificate, if registered 2) Partnership deed 3) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf 4) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses
Accounts of trusts & foundations	<ol style="list-style-type: none"> 1) Certificate of registration, if registered
Names of trustees, settlers, beneficiaries and signatories Names and addresses of the founder, the managers/directors and the beneficiaries Telephone/fax numbers	<ol style="list-style-type: none"> 1) Power of Attorney granted to transact business on its behalf 2) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses 3) Resolution of the managing body of the foundation/association 4) Trust Deed

<p>Accounts of Proprietary Concerns</p> <p>Name, Address and Activity of the Proprietary Concern.</p>	<p>Any two of the following documents in the name of the proprietary concern shall be required.</p> <ol style="list-style-type: none"> 1) Registration certificate (in the case of a registered concern), 2) Certificate/licence issued by the Municipal authorities under Shop & Establishment Act, 3) Sales and income tax returns, 4) CST / VAT certificate, certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, 5) Licence issued by the professional body incorporated under a statute like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc. 6) Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. 7) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT 8) The complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities. 9) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.
<p>Hindu Undivided family</p> <p>For Identity of the HUF, its activities, address and authority for opening and operation of its account(s)</p> <p>For identity of the Karta and major co-parceners of the HUF who are authorized to operate the account(s) and their addresses.</p>	<ol style="list-style-type: none"> 1) Prescribed Joint Hindu Family Letter signed by all the major Co-parceners. 2) Declaration Form from the Karta. 3) Any of the Officially Valid documents for identity of each of the Karta and each of the major coparceners (as given above for individuals) and their addresses 4) Recent Passport size Photographs of all such persons.
<p>Societies, Associations NGOs, Clubs, and other organizations</p> <p>For Identity of the organization, its</p>	<ol style="list-style-type: none"> 1) Certificate of Registration, if registered, 2) Bye laws 3) Telephone/Utility Bill in the name of the organization 4) List of Managing Committee Members 5) Resolution of the Managing Committee of the Organization for opening of the account and delegating powers to operate the accounts of the

<p>activities, address and authority delegated for opening and operation of its account(s). For identity of the Managing Committee Members who are authorized to operate the accounts of the organization and their addresses.</p>	<p>organization. 6) Any of the documents for identity of each the authorized Managing committee Members (as given above for individuals) and their addresses</p>
<p>Local Bodies/Government Departments etc. For Identity of the applicant, its activities, address and authority delegated for opening and operation of its account(s).</p>	<p>Notification/Resolution/Letter of Permission for opening and delegation of authority to operate the account</p>

Annexure III: An Indicative List of Suspicious Activities

1) Transactions Involving Large Amounts of Cash

Company transactions that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the company, e.g. cheques,

2) Transactions that do not make Economic Sense

Transactions in which assets are withdrawn immediately after being deposited unless the business activities of the customer's furnishes a plausible reason for immediate withdrawal.

3) Activities not consistent with the Customer's Business

Accounts with large volume of credits whereas the nature of business does not justify such credits.

4) Attempts to avoid Reporting/Record-keeping Requirements

A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

Any individual or group that coerces/induces or attempts to coerce/induce a CGCL employee not to file any reports or any other forms.

An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

5) Unusual Activities

Funds coming from the countries/centers which are known for money laundering.

6) Customer who provides Insufficient or Suspicious Information

A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.

A customer/company who is reluctant to reveal details about its activities or to provide financial statements.

A customer who has no record of past or present employment but makes frequent large

transactions.

7) **Certain actions of Employees arousing Suspicion**

An employee whose lavish lifestyle cannot be supported by his or her salary. Negligence of employees/willful blindness is reported repeatedly.