



## **PREVENTION OF MONEY LAUNDERING - PMLA POLICY AND KYC POLICY**

(Approved by the Board of Directors on May 15, 2007, and further amended on January 30, 2017, and August 2, 2019, July 31, 2020, November 06, 2020, February 12, 2022 and May 21, 2022)

---

**CAPRI GLOBAL CAPITAL LIMITED**

**CIN:** L65921MH1994PLC173469

**Regd. & Corporate Off:** 502, Tower A, Peninsula Business Park, Senapati Bapat Marg, Lower Parel,  
Mumbai – 400013, Maharashtra, (India).

**Tel:** +91-22-40888100; **Fax:** +91-22-40888160

**Email:** [compliance.officer@capriglobal.in](mailto:compliance.officer@capriglobal.in)

---

## **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 framework 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. RBI has issued Master Direction-"Know Your Customer (KYC) Directions, 2016" having reference Number DBR.AML.BC.No.81/14.01.001/2015 -16 dated February 25, 2016 ("**RBI Master Directions on KYC**") and is updated till April 20, 2020.

Reserve Bank of India has made amendments in RBI Master Directions on KYC vide its Circular No. RBI/2019-20/138 DOR.AML.BC.No.27/14.01.001/2019-20 dated January 9, 2020 with a view to leveraging the digital channels for Customer Identification Process (CIP) by Regulated Entities (REs), the Reserve Bank of India has decided to permit Video based Customer Identification Process (V-CIP) as a consent based alternate method of establishing the customer's identity, for customer onboarding. Further, Reserve Bank of India has issued Internal Money Laundering (ML) and Terrorist Financing (TF) risk assessment by REs - Amendment to Master Direction (MD) on KYC vide its Circular No. RBI/2019-20/221 DOR.AML.BC.No.66/14.01.001/2019-20 dated April 20, 2020 with a view to mitigate and manage the identified Risk. Further, Reserve Bank of India has issued amendments Restriction on Account Operations for Non- Compliance to carry out periodic updation of KYC of existing customers. Keeping in view the current COVID-19 related restrictions vide its Circular No. RBI/2021-22/29 DOR. AML.REC 13/14.01.001/2021-22 dated May 5, 2021.

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India, Regulated Entities (REs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. REs shall take steps to implement the provisions of the aforementioned Act and Rules, including operational instructions issued in pursuance of such amendment(s). to Master Direction (MD) on KYC vide its Circular No. DBR AML.BC.No.81/14.01.001/2015-16 dated May 10, 2021. Further, Reserve Bank of India has issued amendments Restriction on Account Operations for Non- Compliance to carry out periodic updation of KYC of existing customers. Keeping in view the current COVID-19 related restrictions is updated vide its Circular No. RBI/2021-22/44 DOR. AML.REC 74/14.01.001/2021-22 dated December 30, 2021.

This Policy document is prepared in line with the RBI Master Directions on KYC and amendments thereto 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 ("**CGCL**") from being used, intentionally or unintentionally, by criminal elements for money laundering activities.

### **2) Definition of Money Laundering**

Section 3 of PMLA Act 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 Policy, 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 categorization 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. A detailed search to be carried out to find that the Client is not in defaulters / negative list of regulators. (Search should invariably be carried out from reports generated from any of CIC (CIBIL, CRIF, EXPERIAN or EQUIFAX) and Ministry of Corporate Affairs sponsored website [www.watchoutinvestors.com](http://www.watchoutinvestors.com)
- n. 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.
- o. Where Permanent Account Number (PAN) is obtained the same shall be verified from the verification facility of the issuing authority
- p. Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

## 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 Annexure-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 Annexure-II. The prior approval of Head- Compliance shall be necessary for accepting any document other than the one listed in Annexure-III

#### Video based Customer Identification Process (V – CIP)

V-CIP is a method of customer identification by an official of the Company by undertaking seamless, secure real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this Master Direction.

The Company may undertake live V-CIP, to be carried out by an official of the Company, for establishment of an account based relationship with an individual customer,

CGCL may undertake V-CIP to carry out:

i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

Provided that in case of CDD of a proprietorship firm, CGCL shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28 of PML Act apart from undertaking CDD of the proprietor.

ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17 of PML Act

iii) Updation/Periodic updation of KYC for eligible customers.

CGCL opting to undertake V-CIP, shall adhere to the following minimum standards:

#### **(a) V-CIP Infrastructure**

i) CGCL should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of CGCL, and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

ii) CGCL shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with CGCL. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

#### (b) V-CIP Procedure

i) CGCL shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of CGCL specially trained for this purpose. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

ii) If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

iv) Any prompting, observed at end of customer shall lead to rejection of the account opening process.

v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.

vi) The authorised official of CGCL performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

- a. OTP based Aadhaar e-KYC authentication
- b. Offline Verification of Aadhaar for identification
- c. KYC records downloaded from CKYCR, in accordance with Section 56 of PML Act, using the KYC identifier provided by the customer
- d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

CGCL shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of PML Act

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

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, REs shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, CGCL shall ensure that no incremental risk is added due to this.

vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial

profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

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

ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

x) The authorised official of CGCL shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

xi) Assisted V-CIP shall be permissible when banks take help of Banking Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.

xii) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by CGCL.

**(c) V-CIP Records and Data Management**

i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. REs shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.

ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, CGCL shall at their option, rely on CDD done internally and not outsourced. However optionally CDD by a third party can be considered, subject to the following conditions:

1. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
2. Adequate steps are taken by CGCL to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
3. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the Prevention of Money-Laundering Act.
4. The third party shall not be based in a country or jurisdiction assessed as high risk.
5. The ultimate responsibility for CDD, including done by a third party and undertaking enhanced due diligence measures, as applicable, shall rest with the CGCL

**Unique Customer Identification Code for Customers (UCIC)**

CGCL shall introduce Unique Customer Identification code to 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.

#### **12 A) Money Laundering and Terrorist Financing Risk Assessment by the Company :**

- a. The Company shall carry out Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.
- b. The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board of the Company in alignment with the outcome of the risk assessment exercise & it should be reviewed annually by the company.
- c. The outcome of the exercise shall be put up to the Board or any Committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. The Company shall monitor the implementation of the controls and enhance them if necessary.

#### **13) Customer Due Diligence (CDD) /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 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 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.

CGCL shall categorize risk profile of its customers into 3 (three) basic categories in order with the profile. The category along with the illustrative example are as below:

**(i) Low Risk:**

Low Risk customers are those i (other than high net worth) whose identities and sources of income and net worth can be easily identified and the transactions in whose accounts by and large conform to known profile. Low-risk customers shall include

- ✓ Salaried employees whose salary structures are well defined and can be ascertained from Bank credits or documents provided for verification.
- ✓ .

Self-Employed customers

**(ii) Medium Risk:**

The medium risk customers are those who are covered under caution / negative list as defined in Credit Operation Manual but onboarded after proper credit due diligence process. Profiles defined under the negative list are considered as medium risk customers other than customer profiles as defined in 13 (iii) of this policy. I

**(iii ) High Risk**

The high risk customers shall be categorized on the basis of the customer's background, nature and location of the activity, country of origin, sources of funds and client profile.

High risk customer shall typically include

- ✓ non-resident customers
- ✓ high net-worth individuals
- ✓ trusts, charities, NGOs and organizations receiving donations,

- ✓ companies having close family shareholding or beneficial ownership,
- ✓ firms with sleeping partners
- ✓ politically exposed persons (PEPs) of foreign origin
- ✓ non face to face to customers and
- ✓ Persons with dubious reputation as per public information available.
- ✓ Persons whose sources of income are not clear

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

CGCL shall adopt a risk-based approach for periodic updation of KYC. However, 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 from the date of opening of the account / last KYC updation.

The annual review would be carried out to access which account is nearing the timelines as above and Re- KYC to be initiated

#### **a) Individual Customers:**

- i. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id and mobile number registered with the Company, / letter.
- ii. **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id and mobile number registered with the Company / letter. and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

Further, CGCL, at their option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii) of PML Act, for the purpose of proof of address, declared by the customer at the time of periodic updation. Such requirement, however, shall be clearly specified by the CGCL in their internal KYC policy duly approved by the Board of Directors of CGCL or any committee of the Board to which power has been delegated.

#### **b) Customers other than individuals:**

- i. **No change in KYC information:** In case of no change in the KYC information of the LE customer, a self- declaration in this regard shall be obtained from the LE customer through its email id registered with the Company. ,letter from an official authorized by the LE in this regard, board resolution etc. Further, CGCL shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.
- ii. **Change in KYC information:** In case of change in KYC information, CGCL shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

#### **c) Additional measures :** In addition to the above, CGCL shall ensure that,

- i. The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, CGCL shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- ii. Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC.

- iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
- iv. In order to ensure customer convenience, Company may consider making available the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of the Company or any committee of the Board to which power has been delegated.
- v. CGCL shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measure, which otherwise are not mandated under the above instructions, adopted by the Company such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Company where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of the Company or any committee of the Board to which power has been delegated.
- vi. CGCL shall ensure that their internal KYC policy and processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

In case of existing customers, CGCL shall obtain the Permanent Account Number or equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing which CGCL shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-document thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the CGCL shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, CGCL shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

Explanation – For the purpose of this Section, “temporary ceasing of operations” in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the CGCL till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

“Certified Copy ” - Obtaining a certified copy by CGCL shall mean comparing the copy of the proof of possession of Aadhar number where offline verification cant not be carries out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the CGCL as per the provisions contained in the Act

#### **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 or the equivalent e-documents there off as mentioned in **Annexure III** containing details of identity and address;
- b. the Aadhar number where.
  - i. The customer is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
  - ii. The customer decides to submit his Aadhar number voluntarily the company shall notify under first proviso to sub-section (1) of section 11A of the PML Act;

or

- (aa) the proof of possession of Aadhaar number where offline verification can be carried out , or
- (ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and
- c. the Permanent Account Number or the equivalent e-document thereof or Form No 60 as defined in Income – tax Rules ,1962, and
- d. such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the company

Provided that where customer has submitted

- i. Aadhaar number under clause (a) above CGCL should notified under first proviso to sub-section (1) of section 11A of the PML Act CGCL shall carry out authentication of the customers Aadhar Number using e- KYC authentication facility provided by the Unique Identification Authority of India. Further in such case, if customer wants to provide a current address different from the address as per the identify information available in the Central Identities Datta Repository he may gave a self – declaration to that effect to the company
- ii. Proof of possession of Aadhar under clause (aa) above where offline verification can be carried out CGCL Shall carry out offline verification
- iii. An equivalent e- document of any OVD CGCL shall verify the digital signature as per the provisions of the Information Technology Act 2000(21 of 2000) and any rules issues thereunder and take a live photo as specified under **Annexure-I**
- iv. Any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out CGCL shall carry out verification through digital KYC as specified under **Annexure- I**

Provided that for a period not beyond such date as may be notified by the Government for class of CGCL, instead of carrying out digital KYC , CGCL pertaining to such class may obtain a certified copy of the proof of possession of Aadhar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Explanation – For the purpose of this Section, the definitions as per RBI Master Directions on KYC are as under:

- i. **“Digital KYC “** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Company as per the provisions contained in the Act.
- ii. **“Digital Signature”** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- iii. **“Equivalent e – document “** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.
- iv. **“ Know Your Client (KYC) Identifier”** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- v. **“Central KYC Records Registry” (CKYCR)** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer
- vi. **“Designated Director”** means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML and the Rules and shall include:
  - a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the Regular Entity is a Company,
  - b. the Managing Partner, if the Regular Entity is a Partnership Firm,
  - c. the Proprietor, if the Regular Entity is a Proprietorship Concern,
  - d. the Managing Trustee, if the Regular Entity is a trust,

- e. a person or individual, as the case may be, who controls and manages the affairs of the Regular Entity, if the Regular Entity is an unincorporated association or a body of individuals,

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 CGCL 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.

Offline verification shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

CGCL Shall carry out offline verification of a customer if he is desirous of undergoing Aadhaar offline verification for identification purpose.

In cases where successful authentication has been carried out, other OVD and photograph need not be submitted by the customer.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of PML Act the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 of PML Act owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, CGCL shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e- document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the CGCL and such exception handling shall also be a part of the concurrent audit as mandated in Section 8 of PML Act. CGCL shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the CGCL and shall be available for supervisory review

Explanation 1: CGCL shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above

Explanation 2: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder

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 III** containing details of identity and address of the individual (proprietor) shall be obtained.

In addition to the above, any two of the documents or the equivalent e - documents there of 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**

- a. For opening an account of a company, one certified copy of each of the documents or the equivalent e - documents as per Annexure II shall be obtained:
- b. For opening an account of a partnership firm, one certified copy of each of the documents or the equivalent e - documents as per Annexure III shall be obtained:
- c. For opening an account of a trust, one certified copy of each of the documents or the equivalent e - documents as per Annexure III shall be obtained:
- d. For opening an account of an unincorporated association or a body of individuals, one certified copy of each of the documents as per Annexure III 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. Any cases in 60+ DPD to be revisited to check customers business continuity, source of fund to repay the loan EMI, status of any property mortgaged etc.

## **Enhanced Due Diligence Procedure**

Accounts of non-face-to-face customers (Other than Aadhaar OTP based on – boarding) : 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) Appointment of Designated Director :**

CGCL has appointed Mr. Rajesh Sharma, Managing Director (email: rajesh.sharma@capriglobal.in) as the 'Designated Director' who will be responsible for overall compliance with the obligation imposed under Chapter IV of the Act

#### **18) Principal Officer [Money Laundering Reporting Officer]**

The 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.

CGCL has appointed Mr. Ashok Agrawal - Associate Director as the 'Principal Officer' designate who will be responsible for reporting all transactions and sharing of information. He will also be responsible to ensure that proper steps are taken to fix accountability for serious lapses and intentional contraventions of the KYC guidelines.

- Name of the 'Principal Officer' – Mr. Ashok Agrawal
- Designation - Associate Director
- Telephone: **022-43548200 / 022-66518011** Fax: **022-22019051**
- Website - [www.capriglobal.in](http://www.capriglobal.in)
- E- Mail - [ashok.agarwal@capriglobal.in](mailto:ashok.agarwal@capriglobal.in)

#### **19) Reporting Requirements to Financial Intelligence Unit - India**

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

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. The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established through the production of an OVD and Permanent Account Number or Form No 60 as the case may be

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;
- d. the parties to the transaction.

Maintenance & Preservation of Records: CGCL shall preserve account information related documents for at least five 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 five 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 15<sup>th</sup> 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.

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.

**20) Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS) Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements: -**

1 Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions at the link <https://incometaxindiaefiling.gov.in/> post login --> My Account --> Register as Reporting Financial Institution

2 Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61 B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation - HFCs shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H of Income Tax Rules

3. Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H of Income Tax Rules

4 Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

5 Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

6, Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time

ii) In addition to the above, other United Nations Security Council Resolutions (UNSCRs) circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of  
OTHER RESPECTIVE MEASURES

**21) 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 the following link :

<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.

**22) Other Instructions**

Company shall maintain the confidentiality of information as provided in Section 45NB of RBI Act 1934. [CDD](#)

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

(a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

(b) In terms of provision of Rule 9(1A) of PML Rules, the CGCL shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

(c) Operational Guidelines for uploading the KYC data have been released by CERSAI.

(d) CGCL shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

(e) The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, Company required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules *ibid*.

(f) CGCL shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules *ibid*. The KYC records have to be uploaded as per the LE Template released by CERSAI.

(g) Once KYC Identifier is generated by CKYCR, CGCL shall ensure that the same is communicated to the individual / LE as the case may be.

(h) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, CGCL shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per (e) and (f) respectively at the time of periodic updation as specified in Section 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

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

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

(i) there is a change in the information of the customer as existing in the records of CKYCR;

(ii) the current address of the customer is required to be verified;

(iii) the Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client

**23) Review & Amendment to the Policy**

This Policy shall be reviewed by the Risk Management Committee and Board. Any changes or modification on the Policy would be presented for approval of the Board on recommendation of the Risk Management Committee. The changes required due to business exigencies or due to regulatory /audit requirements can be approved by the Managing Director/Executive Director of the Company and such changes made to be brought to the attention of the Risk Management Committee and Board of the first meeting following amendment.

**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.

**Annex I**  
**Digital KYC Process**

- A. CGCL shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of CGCL.
- B. The access of the Application shall be controlled by CGCL & it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by CGCL to its authorized officials.
- C. The customer, for the purpose of KYC, shall visit the location of the authorized official of CGCL or vice-versa. The original OVD shall be in possession of the customer.
- D. CGCL must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of CGCL shall put a water- mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by CGCL) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
- E. The Application of CGCL shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
- F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
- G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
- H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e- Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
- I. Once the above-mentioned process is completed a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with CGCL shall not be used for customer signature. CGCL must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer
- J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with CGCL. . Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.
- K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of CGCL and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-

id/reference-id number to customer for future reference.

- L. The authorized officer of CGCL shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.
- M. On Successful verification, the CAF shall be digitally signed by authorized officer of CGCL who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.



**Annexure III Customer Identification Procedure (Indicative List of Documents To Be obtained from different Types of Customers or the equivalent e-documents thereof shall be obtained:)**

<b><u>Type of Customers</u></b>	<b><u>Documents to be Obtained</u></b>
Individual  For Identification & Address	<ol style="list-style-type: none"> <li>1) Passport</li> <li>2) PAN Card / Form No 60</li> <li>3) Voter's identity Card issued by Election Commission of India</li> <li>4) Driving License with photograph</li> <li>5) Aadhaar Card</li> <li>6) Job Card Issued by NREGA duly signed by an officer of the State Government <b>and letter issued by the National Population Register containing details of names and address.</b></li> </ol> <p>where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-</p> <ol style="list-style-type: none"> <li>7) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); property or Municipal tax receipt;</li> <li>8) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;</li> <li>9) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation</li> </ol> <p>Provided further that the customer shall submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents.</p>
Non-Resident Indians- Individuals	<ol style="list-style-type: none"> <li>1) Copies of Passport and Residence Visa,</li> <li>2) a valid document indicating foreign residential address and passport size photographs of the applicant.</li> <li>3) The applicant is to be duly introduced by Banker/ Notary Public/ Indian Embassy/ Local customer who has been subjected to full KYC Procedure.</li> </ol> <p>In case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 (FEMA 5(R)), alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained:</p> <ol style="list-style-type: none"> <li>1) Authorised officials of overseas branches of Scheduled Commercial Banks registered in India.</li> <li>2) branches of overseas banks with whom Indian banks have relationships</li> <li>3) Notary Public abroad</li> <li>4) Court Magistrate</li> <li>5) Judge,</li> <li>6) Indian Embassy/Consulate General in the country where the non-resident</li> </ol>

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"> <li>1) Certification of Incorporation</li> <li>2) Memorandum and Articles of Association</li> <li>3) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.</li> <li>4) Permanent Account Number of the company</li> <li>5) Documents, as specified in Section 16, relating to the beneficial owner the managers, officers, or employees, as the case may be, holding an attorney to transact on the company's behalf</li> </ol> <p>Any of the documents for the identity of each of the directors/ authorized officials (as given above for individuals) and their addresses, Recent passport size Photographs of directors/authorized officials.</p>
Accounts of registered 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"> <li>1) Registration certificate,</li> <li>2) Partnership deed</li> <li>3) Permanent Account Number of the Partnership Firm</li> <li>4) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees as the case may be holding an attorney to transact on its behalf</li> </ol>
Accounts of trusts & foundations	<ol style="list-style-type: none"> <li>1) Certificate of registration, if registered</li> <li>2) Trust deed</li> <li>3) Permanent Account Number of the Trust</li> <li>4) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees as the case may be holding an attorney to transact on its behalf</li> </ol>
An unincorporated association (Includes Unregistered trusts/partnership firms) or a body of individuals ((includes societies)	<ol style="list-style-type: none"> <li>1) Resolution of the managing body of such association or body of individuals</li> <li>2) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals.</li> <li>3) Power of attorney granted to transact on its behalf</li> <li>4) Documents, as specified in Section 16, relating to beneficial owner, managers officers or employees, as the case may be, holding an attorney to transact on its behalf</li> <li>5) Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals</li> </ol>

Accounts of Proprietary Concerns	Any two of the following documents in the name of the proprietary concern shall be required.
Name, Address and Activity of the Proprietary Concern.	<ol style="list-style-type: none"> <li>1) Registration certificate (in the case of a registered concern),</li> <li>2) Certificate/licence issued by the Municipal authorities under Shop &amp; Establishment Act,</li> <li>3) Sales and income tax returns,</li> <li>4) CST / VAT certificate, certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities,</li> <li>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.</li> <li>6) Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department.</li> <li>7) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT</li> <li>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.</li> <li>9) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.</li> </ol> <p>In cases where CGCL is satisfied that it is not possible to furnish two such documents, CGCL may, at their discretion, accept only one of those documents as proof of business/activity</p>
Juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats	<ol style="list-style-type: none"> <li>1) Document showing name of the person authorised to act on behalf of the entity</li> <li>2) Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf</li> <li>3) Such documents as may be required by the Company to establish the legal existence of such an of such an entity or juridical person</li> </ol>

#### Annexure IV: 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.