POLICY ON

Know Your Customer (KYC) Standards, Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) Measures

Updated as on 31.07.2022

GIC HOUSING FINANCE LTD.
National Insurance Building, 6th Floor
14 Jamshedji Tata Road, Churchgate
Mumbai - 400 020

INDEX

Sl No.	Description	Page No.
1	Introduction	3
2	Policy Objectives	3
3	Definitions	3
4	Key elements of the policy	7
5	Customer Acceptance Policy	7
6	Customer Identification Procedure (CIP)	8
7	CIP in case of Individuals	9
8	List of Officially Valid documents (OVDs)	10
9	CIP in case of non-Individuals	10
10	Customer Due Diligence (CDD) Procedure	13
11	Customer Identification requirements – Indicative guidelines	14
12	Customer accounts opened by professional intermediaries	16
13	Monitoring of Transactions	17
14	Risk management	18
15	Periodic Updation of KYC	19
16	Secrecy obligations and sharing of information	20
17	Customer Education - Employees Hiring – Employee's Training	21
18	Introduction of New Technologies	21
19	Review of Policy	22
20	Designated Director	22
21	Appointment of Principal Officer	23
22	Maintenance of records of transactions	24
23	Maintenance and Preservation of records	24
24	Reporting to Financial Intelligence Unit-India	25
25	Cash and Suspicious Transaction Reports	26
26	Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)	28
27	Illustrative list of Suspicious Transactions pertaining to Individuals	30
28	Illustrative list of suspicious transactions pertaining to Builder/Project/Corporate Clients	32
29	Annex - I Digital KYC Process	33
30	Annex – II Video Customer Identification Process (V-CIP)	35
31	Annex - III: Details of Principal Officer and Designated Director	37

Introduction

As part of the best corporate practices, GIC Housing Finance Limited (GICHFL) ("the Company") has adopted "Policy on Know Your Customer (KYC) guidelines and Anti Money Laundering (AML) Standards" for lending/ credit/ operations/ financial dealings, in line with the extant guidelines framed by Reserve Bank of India ("RBI") with reference to the Prevention of Money-Laundering Act, 2002 (PMLA) and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PMLR), as amended from time to time.

Policy Objectives

The objective of the Policy is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering/ fraudulent/anti-social activities. KYC procedures also enable the Company to identify/ know/ understand their customers and their financial dealings better, which in turn help to manage risks prudently. The provisions of this Policy are applicable to all branches/offices of GICHFL.

Definitions of terms used in this policy

Customer

'Customer' is defined to mean a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person, on whose behalf the person who is engaged in the transaction or activity, is acting.

Transactions

The regulatory norms define transaction as:

Transaction means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and

includes,

a) Opening of an account.

b) Deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means.

c) Entering into any fiduciary relationship.

d) Any payment made or received in whole or in part of any contractual or other legal obligation;

e) Establishing or creating a legal person or legal arrangement.

Officially Valid Documents (OVD)

"Officially Valid Document" (OVD) means the passport, the driving license, proof of possession of Aadhaar number, the Voters Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that, where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India. The customers should be asked to redact or blackout Aadhaar number and the functions responsible should ensure that same.

Central KYC Records Registry (CKYCR)

an entity set up to receive, store, safeguard and retrieve the KYC records in digital form of a customer

Beneficial Owner

A beneficial owner is a natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

Certified Copy

Certified copy means comparing the copy of officially valid document with the original and recording it on the copy by the authorized officer of GIC-HF in a manner prescribed by RBI. In the case of Non Resident Indian (NRI)/Person of Indian Origin (PIO) customers, the following officials also could certify the copy of the OVD

a. Authorized officials of overseas branches of Scheduled Commercial Banks registered in India
b. Branches of overseas banks with whom Indian banks have relationships
c. Notary Public abroad
d. Court Magistrate
e. Judge

f. Indian Embassy/Consulate General in the country where the non-resident customer resides.

For purpose of verifying the original of the OVD and recording it on the copy, GIC-HF might authorize the Direct Selling Agents (DSA), Fintech Partners and their employees. Such authorized officers will sign the declaration of having seen and verified the original (OSV) on the copy of the OVD with their employee code along with the unique code allocated to the DSA/Fintech partner

Politically Exposed Persons (PEP)

(PEPs) are individuals who are or have been entrusted with prominent public functions e.g., Heads of States/ Governments, senior politicians, senior government/judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.

Non-face to face Customer

Non-face-to-face customer means customer who opens accounts without visiting the branch/offices of the

Company or meeting the officials of the Company.

Digital KYC

Capturing live photo of the customer and OVD 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 authorized officer of the Company.

Equivalent e-document

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. This may be obtained for individuals and also from non-individual customers.

Video based Customer Identification Process (V-CIP)

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 Customer Due Diligence (CDD) purpose, and to ascertain the veracity of the information furnished by the customer. This process is to be treated as face-to-face process for the purpose of this Policy

Suspicious transaction

a transaction as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

b. appears to be made in circumstances of unusual or unjustified complexity; or

c. appears to not have economic rationale or bona-fide purpose; or

d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

FATCA

Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

Common Reporting Standards (CRS)

Reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

Key elements of the policy :

As per RBI Directions, KYC policy is hereby incorporated based on the following four key elements:

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

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

i. a person or entity that maintains an account and/or has a business relationship with the GICHFC;
ii. one on whose behalf the account is maintained (i.e. the beneficial owner);
iii. beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc. as permitted under the law, and
iv. any person or entity connected with a financial transaction which can pose significant reputational or other risks, say, a wire transfer or issue of a high value demand draft as a single transaction.
v. The DSA's/ Panel Advocates/ Valuers/ Professionals and other third-party entities engaged in the course of business

Customer Acceptance Policy

The explicit guidelines on the Customer Acceptance Policy are as appended:

i. No account is opened in anonymous or fictitious/benami name.
ii. No account is opened where the company is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
iii. No transaction or account-based relationship is undertaken without following the CDD procedure.
iv. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
v. 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

vi. A Unique Customer Identification Number shall be allotted while entering into new relationships with individual customers as also the existing customers and the company shall apply the CDD procedure at the Unique Customer Identification Number level. Thus, if an existing KYC compliant customer of the company desires to open another account, there shall be no need for a fresh CDD exercise.

vii. CDD Procedure is followed for all the joint account holders, while opening a joint account.

viii. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

ix. Suitable system is put in place 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.

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

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

Customer Identification Procedure (CIP)

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information while establishing a relationship. GICHFL will obtain information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Being satisfied means that GICHFL must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer.

The primary objectives of CIP are;

i. To verify the legal status of the customer/ entity through proper and relevant documents.

ii. To verify that any person purporting to act on behalf of the customer, legal person/entity is so authorized and to verify the identity of such an authorized person.

iii. To understand the ownership and control structure of the customer and to determine who is the natural person who ultimately has control over the management.

The Customer Identification Procedure is to be carried out while establishing a relationship at the following stages:

i. In case of a customer who intends to avail a loan and duly completed application form along with the processing fees is received from the prospective borrower.
ii. In case of a customer who is a business associate (loan agent), when a duly completed application form is received for enrolment.

Also, GICHFL shall undertake identification of customers in the following cases:

i. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

ii. Selling third party products as agents, selling their own products and any other product for more than INR 50,000 (Rupees Fifty Thousand).

The Customer Identification Procedure shall be carried out by verifying Identity of customer and residence proof of customer. GICHFL has drawn the list of documents to be verified and collected for this purpose at the time of establishing a relationship with the customer or while carrying out a financial transaction. Further employees need to carry out KYC verification once again at the time of execution of loan documents in addition to the present process of KYC Verification at the file login time. The KYC verification Procedure should be carried out by the employees of the Company only and should not to be outsourced.

CIP in case of Individuals

While establishing an account-based relationship with an individual or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity, the following documents are mandated to be obtained :

a. the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962 and
b. Recent Photograph; and
c. the Aadhaar number where,
   i. the person 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 person decides to submit Aadhaar number voluntarily for identification purposes and consents to undergo authentication
OR

iii. proof of possession of Aadhaar number or any Officially Valid Document (OVD-shown below) or the equivalent e-document thereof containing the details of his identity and address and

d. any such other documents including in respect of the nature of business and financial status of the customer, or the equivalent edocuments thereof as may be required by the branches, to create customer profile for the purpose of risk categorisation and transaction monitoring.

List of Officially Valid documents (OVDs):

i. Passport,
ii. Driving License,
iii. Proof of possession of Aadhaar Number,
iv. the Voter's Identity Card issued by the Election Commission of India,
v. Job Card issued by NREGA duly signed by an officer of the State Government
vi. Letter issued by the National Population Register containing details of name and address

CIP in case of non-Individuals:

In respect of non-individuals (entities), identification information of individuals, who are Proprietor(s) / Partner(s) / Beneficial Owner(s) /Authorised Signatories shall be obtained, as detailed in para above. Besides prescribed application forms and photographs of persons who will be operating the account, documents as per different Entity Types (i.e., Proprietorship, Partnership, Trust, Companies, Unincorporated association of Individuals etc.) are required for such accounts.

Proprietorship Firms

Documents which could be obtained as proof of business/activity for proprietary firms (any one), in addition to the documents of the proprietor as individual:

a. Registration Certificate

b. Certificate/ license issued by the Municipal authorities under Shop & Establishment Act,

c. Sales and Income tax returns,

d. CST / VAT/GST certificate (Provisional/Final)

e. Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities

f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of Director General of Foreign Trade (DGFT)/License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statue

g. Complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firms income is reflected duly authenticated / acknowledged by the Income Tax Authorities

h. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern

Any one of the above documents in the name of the proprietary concern would suffice

Partnership Firms

Where the customer is a partnership firm, the certified copies of the following documents should be obtained:

a. PAN of the partnership firm

b. Certificate of registration

c. Partnership deed.

d. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf

e. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalf along with any OVD for identity and address proof and one recent photograph of such persons.

Trusts

Where the customer is a trust firm, the certified copies of the following documents should be obtained:

a. PAN/Form No. 60 of the entity

b. Certificate of registration

c. Trust deed.

d. Power of Attorney granted to a member or an employee of the firm to transact business on its behalf

e. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalf and any OVD for identity and address proof and one recent photograph of such persons.

Unincorporated Bodies

Where the customer is an unincorporated association or a body of individuals, the certified copies of the following documents should be obtained:

a. PAN/Form No. 60 of the entity

b. resolution of the managing body of such association or body of individuals;

c. power of attorney granted to him to transact on its behalf

d. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalf and any OVD for identity and address proof and one recent photograph of such persons.

Companies

Where the customer is a Company, the certified copies of the following documents should be obtained:

a. PAN of the Company

b. Certificate of incorporation

c. Memorandum and Articles of Association

d. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf along with their Permanent Account Number or Form 60 and any OVD or Aadhaar card for identity and address proof and one recent photograph of such persons.

For opening accounts of juridical persons not specifically covered above, such as Government or its Departments, societies, universities and local bodies like village panchayats, one certified copy of the following documents should be obtained:

i. Document showing name of the person authorized to act on behalf of the entity;

ii. Officially valid document for proof of identity and address in respect of the person holding an attorney to transact on its behalf and one recent photograph and

iii. Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

Note: Aadhar number along with consent form is required if customer is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhar Act.

Customer Due Diligence (CDD) Procedure

While undertaking CDD, the documents/information as detailed under para above, "Customer Identification Procedure" are obtained from the customer, while establishing an account-based relationship with an 'individual' or dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity.

Obtaining a certified copy mean comparing the copy of OVD so produced by the client with the original and recording the same on the copy by the authorized officer of the Company.

In case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. 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 license agreements with such employers allotting official accommodation;

Provided that in case the OVD submitted by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Provided further that the customer shall submit updated OVD with current address within a period of three months of submitting the above documents.

Customer Identification requirements – Indicative guidelines

Trust/Nominee or Fiduciary Accounts

1. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The company should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, the company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, the company should take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/directors and the beneficiaries, if defined. If the GICHFC decides to accept such accounts in terms of the Customer Acceptance Policy, the company should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

Accounts of companies and firms

2. The company need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the company. The company should verify the legal status of the legal person/ entity through proper and relevant documents. The company should verify that any person purporting to act on behalf of the legal/ juridical person/entity is so authorized and identify and verify the identity of that person. The company should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception, e.g. in the case of a public company it will not be necessary to identify all the shareholders.

Beneficial Ownership

3. Rule 9(3) of the Prevention of Money Laundering Rules, 2005 requires that every financial institution, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "Beneficial Owner" has been defined as the natural person who ultimately owns or controls a client and/or

the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

A juridical person is an Entity, that is not a single natural person (as a human being), authorised by law with duties and rights, recognised as a legal authority having a distinct identity, a legal personality (Also known as artificial person, juridical entity, juridical person or legal person).

The procedure for determination of Beneficial Ownership as per RBI/Government guidelines is as under:

a. Where the customer is a Company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercises control through other means.
   a) Explanation- for the purpose of this sub-clause: -
      i. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company;
      ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.

b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

   Explanation - Term "body of individuals" includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with

15 per cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

Customer accounts opened by professional intermediaries

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

i. 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.

ii. Adequate steps are taken by the Company to satisfy itself 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.

iii. 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.

iv. The third party shall not be based in a country or jurisdiction assessed as high risk.

v. The ultimate responsibility for CDD, including done by a third party and undertaking enhanced due-diligence measures as applicable, shall rest with the GICHFL.

Accounts of Politically Exposed Persons (PEPs)

Company will ensure that:

i. sufficient information including information about the sources of funds, accounts of family members and close relatives is gathered on the PEP;

ii. the identity of the person shall have been verified before accepting the PEP as a customer;

iii. the decision to open an account for a PEP is taken at a senior level in accordance with the Customer Acceptance Policy;

iv. all such accounts are subject to enhanced monitoring on an on-going basis;

v. in the event of in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

vi. The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

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

Central KYC Registry (CKYCR)

The customer KYC information should be shared with the CKYCR in the manner mentioned in the RBI Directions in the RBI's KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be with Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI).

Monitoring of Transactions

Ongoing monitoring of accounts is an essential element of effective KYC procedures. The company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity.

However, the extent of monitoring will depend on the risk sensitivity of the account. We should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The company may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. The extent of monitoring shall be aligned with the risk category of the customer. The company has put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures.

Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the company. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensified monitoring. The company has set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

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, are categorized as low risk.

Customers that are likely to pose a higher-than-average risk to the Company are categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. The Company will 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.

Risk management

GICHFL has established appropriate procedures to ensure effective implementation of KYC programme. The procedures cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibilities are explicitly allocated within the company for ensuring that the policies and procedures are implemented effectively.

GICHFC has devised procedures for creating Risk Profiles of our existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

Internal audit and compliance functions of GICHFC have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function provides an independent evaluation of our policies and procedures, including legal and regulatory requirements. The audit machinery of GICHFL is adequately staffed with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors are mandated to 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 are required to be put up before the Audit Committee of the Board at quarterly intervals. GICHFL has a proper system of fixing accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines.

The Company shall prepare a profile for all the customer based on the risk categorization. The customer profile shall contain information relating to Customer identity, social/financial status, nature of business activity, information about his client business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. The Company shall ensure to classify the customer as low risk, medium risk and high risk, depending on

background, nature and location of the activity. The risk profile should be reviewed at periodical intervals by obtaining the required information. The indicative list of the customers as low risk, medium risk and high risk are as under:

a) Low Risk: Ex Staff of the Company, Govt/Semi Govt Employees, Individuals, pensioners, proprietor ship concerns. Staff Members of public sector Companies, Co-operative Societies, Senior Citizens etc.

b) Medium Risk: Small business enterprises like Pawn Shop, Auctioneers, Cash intensive business as Restaurants, Retail shop, garages, Sole practitioners like law firms, notaries, accountants, bling persons, purthanashin ladies and unregistered bodies.

c) High risk: Customer conducting their business or transactions in unusual circumstances, customer based in high risk countries, politically exposes persons, non-resident customers and foreign nationers, high net worth individuals, firms with sleeping partners, Companies having close family shareholders, shell companies, Trust, Charities, NGO's, NPO's, Customers engaged in business which is associated with higher level of corruption, customers dealing with real estate business, bullion dealers, stock brokers and HUF's.

Periodic Updation of KYC

Periodic KYC 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 as per the following procedure:

a) For 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/ mobile number registered with the Company or any other reliable mode.

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/mobile number registered with the company, branch, digital channels (such as web portal, mobile application of company), letter etc., 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, company, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

b) Customers other than individuals:

i. No change in KYC information: In case of no change in the KYC information of the Legal entity (LE) customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the company, branch, digital channels (such as web portal, mobile application of company), letter from an official authorized by the LE in this regard, board resolution etc.

ii. Change in KYC information: In case of change in KYC information, company shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

The company may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bonafides. Normally, OVD/consent forwarded by the customer through mail/post, etc., shall be acceptable. The company shall ensure to provide acknowledgement with date of having performed KYC updation.

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

In addition to the above, the company shall ensure that,

i. The KYC documents of the customer as per the current Customer Due Diligence (CDD) standards are available with them. This is applicable even if there is no change in customer information but the documents available 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, the company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

Secrecy obligations and sharing of information

(a) Branches shall maintain secrecy regarding the customer information which arises out of the contractual relationship between GICHFL and the customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged without the express permission of the customer.

(c) While considering the requests for data/information from Government and other agencies, GICHFL shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in customer transactions.

(d) The exceptions to the said rule shall be as under:

(i) Where disclosure is under compulsion of law

(ii) Where there is a duty to the public to disclose,

(iii) the interest of GICHFL requires disclosure and

(iv) Where the disclosure is made with the express or implied consent of the customer.

Customer Education - Employees Hiring – Employee's Training

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

Employee Training: The GICHFL shall have an ongoing employee training programme, so that members of the staff are adequately trained in KYC procedures and fully understand the rationale behind the KYC policies and implement them consistently. Mandatory training to be provided to all employees of the Company (including subsidiary company) on KYC Policies and its implementation.

Employees hiring: The KYC norms, AML standards, CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial sector.

It would therefore be necessary that adequate screening mechanism is put in place by GICHFL as an integral part of recruitment/ hiring process of personal.

Introduction of New Technologies

GICHFL should pay special attention to any money laundering threats that may arise from new or developing technologies including on-line transactions that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

(a) Persons authorized by GICHFL, shall be fully compliant with the KYC guidelines applicable to HFCs

(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 GICHFL including brokers/agents etc. who are operating on their behalf.

Review of the Policy

This Policy should be reviewed annually and if there are any amendments in the regulatory guidelines and

the revised policy should be staged for Board's Approval in the subsequent Board Meeting post the

amendments are notified by the regulator.

Designated Director

As per PMLA rules notified by the Govt, on 27/08/13, every HFC shall nominate the Director on their Boards as a designated Director to ensure complaints with the obligations under the Prevention of Money Laundering Act (Amendment Act 2012).

a) A "Designated Director" means a person designated by the GICHFL to ensure overall compliance with the obligations imposed under Chapter IV of the Act and shall be nominated by the Board of the GICHFL;

b) The name, designation and address of the Designated Director including changes from time to time, shall be communicated to the Director, FIU-IND and also to the National Housing Bank; and

c) In no case, the "Principal Officer" shall be nominated as the "Designated Director") Designated Director on the Board of the Company:

GICHFL has nominated the MD as the Designated Director on the Board of the company, as required under the provisions of the PML Rules, 2005 to ensure

compliance with the obligations under the Act and Rules. The Designated Director shall oversee the compliance position of AML norms in the Company.

If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may –

a) Issue a warning in writing; or

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

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

d) By an order, levy a fine on such reporting entity, its Designated Director, officers and employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.

It shall be the duty of every reporting entity, its Designated Director, officers and employees to observe the procedure, manner of furnishing and reporting information on transactions.

Appointment of Principal Officer

The Head of Operations is the "Principal Officer", who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The name of the Principal Officer so designated, his designation and address including changes from time to time, may please be advised to the Director, FIU-IND. Principal Officer shall be located at the Corporate office of GICHFL and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

Role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended from time to time. The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit

organisations of value more than Rupees Ten Lakh or its equivalent in foreign currency to FIU-IND.

With a view to enabling the Principal Officer to discharge his responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information.

Maintenance of records of transactions

GICHFL has introduced a system of maintaining proper record of transactions as required under section 12 of the PMLA read with Rule 3 of the PML Rules, as mentioned below:

all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency; 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 lakh; all transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency; all cash transactions where forged or counterfeit currency notes or HFC notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions; and all suspicious transactions whether or not made in cash and by way of as mentioned in the Rule 3(1) (D).

The branches of GICHFL should ensure that they continue to maintain proper record of all cash transactions (deposits and withdrawals) of Rs.2 lakh and above. The internal monitoring system should have an inbuilt procedure for reporting of such transactions and those of suspicious nature whether made in cash or otherwise, to controlling office on a fortnightly basis.

Records to contain the specified information

Records referred to above in Rule 3 of the PMLA Rules to contain the following information: -

(i) the nature of the transactions;

(ii) the amount of the transaction and, the currency in which it was denominated;

(iii) the date on which the transaction was conducted; and

(iv) the parties to the transaction.

Maintenance and Preservation of records

Section 12 of PMLA requires every housing finance company to maintain records as under:

(a) records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules is required to be maintained for a period of ten years from the date of transactions

(b) records of the identity of all clients of the housing finance company is required to be maintained for a period of ten years from the date of cessation of transactions between the clients and the housing finance company.

GICHFL has set up a system for proper maintenance and preservation of information in a manner (in hard and soft copies) that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities between the clients and the housing finance company.

Reporting to Financial Intelligence Unit-India

Section 12 of PMLA requires every housing finance company to report information of transaction referred to in clause (a) of sub-section (1) of section 12 read with Rule 3 of the PML Rules relating to cash and suspicious transactions etc. to the Director, Financial Intelligence Unit-India (FIU-IND).

The proviso to the said section also provides that where the principal officer of a HFC has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to so to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

a) In terms of the PMLA Rules, HFCs are required to report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat, Chanakyapuri,

Explanation: Government of India Notification dated November 12, 2009- Rule 2 sub-rule (1) clause (ca) defines Non-Profit Organization (NPO). NPO means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under section 25 of the Companies Act, 1956.

b) HFCs should carefully go through all the reporting formats. There are altogether eight reporting formats, as detailed in Annex II, viz. i) Cash Transactions Report (CTR); ii) Summary of CTR iii) Electronic File Structure CTR; iv) Suspicious Transactions Report (STR); v) Electronic File Structure STR; vi) Counterfeit Currency Report (CCR); vii) Summary of CCR and viii) Electronic File Structure-CCR. The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. It would be necessary for MFC's to initiate steps to ensure electronic filing of all types of reports to FIU-IND. The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof are furnished in the instructions part of the concerned formats, c) FIU-IND have placed on their website editable electronic utilities to enable MFC's to file electronic CTR/STR who are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base. It is, therefore, advised that in cases of MFC's, where all the branches are not fully computerized, the Principal Officer of the HFC should cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available FIU-IND in their website http://fiuindia.gov.in.

Cash and Suspicious Transaction Reports

A. Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, HFCs should scrupulously adhere to the following:

i) The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis (not on fortnightly basis) and HFC's should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

ii) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer to FIU-IND in the specified format not later than seven working days from the date of occurrence of such transactions (Counterfeit Currency

Report - CCR). These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

iii) While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.

iv) CTR should contain only the transactions carried out by the HFC on behalf of their clients/customers excluding transactions between the internal accounts of the HFC.

v) A summary of cash transaction report for the HFC as a whole should be compiled by the Principal Officer of the HFC every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India. vi) In case of Cash Transaction Reports (CTR) compiled centrally by HFC's for the branches having Core HFC Solution (CBS) at their central data centre level, HFC's may generate centralised Cash Transaction Reports (CTR) in respect of branches under core HFC solution at one point for onward transmission to FIUIND, provided:

a) The CTR is generated in the prescribed format;

b) A copy of the monthly CTR submitted on its behalf to FIU-India is available at the concerned branch for production to auditors/inspectors, when asked for; and

c) The instruction on 'Maintenance of records of transactions'; 'Information to be preserved' and 'Maintenance and Preservation of records' as contained this Circular.

However, in respect of branches not under CBS, the monthly CTR should continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU-IND.

B. Suspicious Transaction Reports (STR)

i) While determining suspicious transactions, HFC's should be guided by definition of suspicious transaction contained in PMLA Rules as amended from time to time.

ii) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. It is clarified that

HFC's should report ail such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

iii) HFCs should make STRs if they have reasonable ground to believe that the transaction involves proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

iv) 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 report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, HFC's may consider the indicative list of suspicious activities.

vi) HFCs should not put any restrictions on operations in the accounts where an STR has been made. HFCs and their employees should keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It should be ensured that there is no tipping off to the customer at any level.

General

It is mandated that GICHFL ensure that the provisions of PML, Rules framed thereunder and the Foreign Contribution and Regulation Act, 1976, wherever applicable, are adhered to strictly.

Where the GICHFL is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the GICHFL may consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

These guidelines are issued under the National Housing HFC Act and any contravention of or non-compliance with the same may attract penal consequences under the said Act.

Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, HFCs shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

a) Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefilina.Qov.in/Dost login-->My Account--> Register as Reporting Financial Institution

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

Explanation - HFCs shall refer to the spot reference rates published by Dealers' Association of India (FEDAI) on their website at http://www.fedai.ora.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.

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

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

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

f) 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.

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

Illustrative list of Suspicious Transactions pertaining to Individuals :

i. Legal structure of client has been altered numerous times (name changes, transfer of ownership).

ii. Unnecessarily complex client structure.

iii. Individual or classes of transactions that take place outside the established business profile and expected activities/ transaction unclear.

iv. Customer is reluctant to provide information, data, documents;

v. Submission of false documents, data, purpose of loan, details of accounts;

vi. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;

vii. Reluctant to meet in person, represents through a third party/ Power of Attorney holder without sufficient reasons;

viii. Approaches a branch/ office of a HFC, which is away from the customer's residential or business address provided in the loan application, when there is HFC branch/ office nearer to the given address;

ix. Unable to explain or satisfy the numerous transfers in account/ multiple accounts;

x. Initial contribution made through unrelated third party accounts without proper justification;

xi. Availing a top-up loan and/or equity loan, without proper justification of the end use of the loan amount;

xii. Suggesting dubious means for the sanction of loan;

xiii. Where transactions do not make economic sense;

xiv. Unusual financial transactions with unknown source.

xv. Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

xvi. There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;

xvii. Encashment of loan amount by opening a fictitious bank account;

xviii. Applying for a loan knowing fully well that the property/ dwelling unit to be financed has been funded earlier and that the same is outstanding;

xix. Sale consideration stated in the agreement for sale is abnormally higher/ lower than what is prevailing in the area of purchase;

xx. Multiple funding of the same property/ dwelling unit;

xxi. Request for payment made in favour of a third party who has no relation to the transaction;

xxii. Usage of loan amount by the customer in connivance with the vendor/builder/developer/broker/agent etc. and using the same for a purpose other than what has been stipulated.

xxiii. Multiple funding/ financing involving NGO/ Charitable Organization/ Small/ Medium Establishments (SMEs) / Self Help Groups (SHGs) / Micro Finance Groups (MFGs)

xxiv. Frequent requests for change of address;

xxv. Overpayment of instalments with a request to refund the overpaid amount.

xxvi. Investment in real estate at a higher/lower price than expected.

xxvii. Clients incorporated in countries that permit bearer shares

Illustrative list of suspicious transactions pertaining to Builder/Project/Corporate Clients :

i. Builder approaching the HFC for a small loan compared to the total cost of the project;

ii. Builder is unable to explain the sources of funding for the project;

iii. Approvals/ sanctions from various authorities are proved to be fake or if it appears that client does not wish to obtain necessary governmental approvals/ filings, etc.;

iv. Management appears to be acting according to instructions of unknown or inappropriate person(s).

v. Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).

vi. Clients with multijurisdictional operations that do not have adequate centralized corporate oversight.

vii. Advice on the setting up of legal arrangements, which may be used to obscure

viii. Ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or other complex group structures).

ix. Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.

Annex - I Digital KYC Process

A. A Digital KYC Application (KYC App) for digital KYC process is to be made available at customer touch points and is to be undertaken only through this authenticated application of the Company

B. Access of the KYC App to be controlled and be ensured that it is not used by any unauthorized person.

C. KYC App to be accessed only through Login-ID and Password, Live OTP or Time OTP controlled mechanism given to the authorized officials of the Company

D. Customer, for KYC, should visit the location of the authorized official of the Company or vice-versa. The original OVD should be in possession of the customer.

E. Live photograph of the customer should be taken by the authorized officer and the same photograph should be embedded in Customer Application Form (CAF).

F. KYC App should add a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

G. KYC App should have a feature such that only live photograph of the customer is captured and not printed or video-graphed photograph.

H. Background behind the customer should be white and no other person should come into frame

I. Live photograph of original OVD or proof of possession of Aadhaar (if offline verification is not being done) placed horizontally, should be captured vertically from above and water - marking as stated above should be done. No skew or tilt in the mobile device should be there while capturing the live photograph of the original documents.

J. Live photograph of customer and original documents should be captured in proper light so that they are clearly readable and identifiable.

K. All the entries in the CAF should be made 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.

L. 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' is to be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF.

M. In case, the customer does not have his/her own mobile number, mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF.

N. In any case, the mobile number of authorized officer registered with the Company should not be used for customer signature.

O. It must be verified that mobile number used in customer signature is not mobile number of authorized officer.

P. Authorized officer should provide a declaration about capturing live photograph of customer and original document. For this purpose, authorized official should be verified with OTP sent to the mobile number registered with the Company. This OTP validation is to be treated as authorized officer's signature on the declaration. Live photograph of authorized official should also be captured in the authorized officer's declaration.

Q. Subsequent to all these activities, the KYC App should give information about the completion of the process and submission of activation request to an activation officer of the Company, and also generate transaction-ID/reference-ID number of the process. Authorized officer should intimate the details regarding transaction-ID/reference-ID number to customer for future reference.

R. Authorized officer of the Company should verify that

i. information available in picture of document is matching with information entered in CAF

ii. live photograph of the customer matches with the photo available in the document

iii. all the necessary details in CAF including mandatory fields are filled properly

S. On Successful verification, the CAF should be digitally signed by authorized officer of the Company and the a print of CAF, should be bear signatures/thumb-impression of customer at appropriate place

T. The signed document should be scanned and uploaded in system and the original hard copy should be returned to the customer.

Annex – II Video Customer Identification Process (V-CIP)

A. Live V-CIP should be carried out by an official of the Company after obtaining customer's informed consent

B. Video of the customer should be recorded along with photograph

C. For identification of the customer, offline verification of Aadhaar should be conducted

D. Clear image of PAN card displayed by customer should be captured, except in cases where e-PAN is provided. PAN details should be verified from Income Tax department.

E. Live location of customer (Geotagging) should be captured to ensure that customer is physically present in India

F. Photograph in Aadhaar/PAN details should match with the customer and the identification details in Aadhaar/PAN should match with details provided by customer.

G. Sequence and/or type of questions during video interactions should be varied in order to establish that interactions are real-time and not pre-recorded.

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

I. Accounts opened through V-CIP should be operational only after being subjected to concurrent audit

J. Process should be seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt.

K. Liveliness check should be carried out in order to guard against spoofing and such other fraudulent manipulations.

L. To ensure security, robustness and end to end encryption, software and security audit and validation of the V-CIP application should be carried out before rolling it out.

M. Interaction should be triggered from the domain of the Company, and not from third party service provider

N. Process should be operated by officials specifically trained for this purpose and activity log along with the credentials of the official performing the V-CIP should be preserved.

O. Video recording should be stored in a safe and secure manner and bear the date and time stamp

P. Assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies may be taken, to ensure the integrity of the process as well as the information furnished by the customer.

Annexure III: Details of Principal Officer and Designated Director

Document Title	Details of Principal Officer and Designated Director
Type of Document	Annexure to the KYC and AML Policy

Nomination details mentioned below:

Designation	Name
Designated Director	Managing Director of GIC-HF
Principal Officer	Compliance Head of GIC-HF