The Oriental Insurance Co. Ltd.

Regd. Office "Oriental House"

A-25/27, Asaf Ali Road

New Delhi – 110 002

AML/CFT Policy 2023

(Based on IRDA's
Master Guidelines on Anti-Money Laundering/ Counter Financing of Terrorism (AML/CFT), 2022 dated 1st August 2022)

(Reference No. IRDAI/IID/GDL/MISC/160/8/2022)

(APPROVED BY THE BOARD OF THE COMPANY IN THE MEETING HELD ON 29TH MAY 2023 VIDE NOTE NO. II-10)

Index

Glossary

Company	The Oriental Insurance Company Ltd
PML Act	Prevention of Money Laundering Act, 2002
PML Rules	Prevention of Money- Laundering (Maintenance of records) Rules, 2005
Guidelines	Master Guidelines on Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT), 2022
CAP	Customer Acceptance Policy
CDD	Client Due Diligence
CIP	Customer Identification Procedures
OVD	Officially Valid Document
V-CIP	Video Based Customer Identification Process
PEP	Politically Exposed Person
KYC	Know Your Customer
CKYCR	Central KYC Registry
AML	Anti-Money Laundering
CFT	Counter Financing of Terrorism
CTR	Cash Transaction Report
CCR	Counterfeit Currency Report
NTR	Non-Profit Organisation Transaction Report
STR	Suspicious Transaction Report
IRDAI	Insurance and Regulatory Development Authority of India
FIU – IND	Financial Intelligence Unit – India
UIDAI	Unique Identification Authority of India
CERSAI	Central Registry of Securitisation Asset Reconstruction and Security Interest of India

1. Introduction:

In terms of the provisions of PML Act and the PML Rules made there under (as amended from time to time), the Company is required to follow Customer Identification Procedures while undertaking a transaction at the time of establishing an account based relationship/ client based relationship and monitor their transactions on an on-going basis. This document is intended to lay down the procedures to facilitate identification of customer and suspicious transactions, control money laundering, combating financing of terrorism and careful scrutiny/ monitoring of large value of cash transactions.

2. Objectives:

The AML/CFT Policy, hereinafter referred to as the Policy, is intended to establish effective measures to enable the Company to achieve the objectives prescribed in the Guidelines, which are as follows:

a. Preventing the abuse of the resources of the Company for money laundering ("ML") and/or financing of terrorism ("FT");
b. Carrying out a business-wide assessment of the risks of ML and FT to which the Company may be subject to and designing and implementing appropriate controls to effectively mitigate and manage the identified risks;
c. Establish and implement policies, procedures and internal controls, which outline the actions to be undertaken by relevant employees/agents/intermediaries to prevent ML and FT while discharging their functional responsibilities;
d. Meeting applicable legal requirements;
e. Mitigating any reputational risk;
f. Safeguarding against establishing any relations or undertaking any transaction that may relate to or may facilitate ML and/or FT or any other illicit activity;
g. Exercising due diligence while dealing with customers, persons appointed to act on behalf of customers, and beneficial owners; and
h. Continuously reviewing and updating the AML/CFT Policy and its corresponding Standards, as threats and standards evolve, to detect and prevent ML and/or FT.

The Policy provides operating guidance to the Company on how to manage risks related to money laundering and the financing of terrorism. The provisions of this Policy shall be applied coherently and in accordance with the scope of the AML/CFT Policy, across all relevant procedures and methodologies.

3. Scope:

This Policy shall be applicable to all the functions of the Company dealing with clients/customers/policyholders. All the relevant functions shall adhere to the guidelines mentioned in this Policy and also incorporate them while designing other internal policies, procedures, products etc.

This Policy shall be read in conjunction with related internal operational guidelines issued by the Company from time to time. The present Policy envisages the following key aspects for adherence and implementation of AML/CFT in the Company:

a) Client Acceptance Policy (CAP)
b) Customer Identification Procedures (CIP)
c) Client Due Diligence measures
d) Risk assessment and categorisation
e) Contracts with PEP
f) Sharing KYC information with Central KYC Registry (CKYCR):
g) Implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA)
h) Monitoring and reporting of suspicious transactions
i) Record Keeping
j) Training to employees, agents and intermediaries

4. Customer Acceptance Policy (CAP)

a) No policy shall be issued in anonymous or fictitious/ benami name(s) and customers shall be accepted only after verifying their identity and address, as laid down in Customer Identification Procedures. No transaction or account-based relationship shall be undertaken without following CDD procedure.

b) Parameters of risk perception shall be defined to classify customers as low and high risk keeping in view customer's identity, the nature of asset insured and mode of premium payment.

c) The Company shall not issue any policy or renew an existing policy when the Company is unable to apply appropriate CDD measures due to non-cooperation of the customer or non-reliability of the data/information furnished.

d) Suitable system shall be put in place to ensure that insurance coverages are not extended to any person or entity, whose name appears in the sanctions lists issued by UN Security Council (UNSC) and/or Ministry of Home Affairs (MHA).

5. Customer Identification Procedure (CIP)

The Company shall verify the customers' identity by using reliable and authentic sources of documents, data or information to ensure that the insurance contracts are not under anonymous or fictitious names.

The Company shall determine the beneficial ownership and controlling interest in case of applicants who are not individuals and the KYC of the beneficial owners shall be completed.

To know the identity and address of customer and to verify the same, the Company shall refer to related documents as detailed in **Annexure-A.**

A. When shall KYC and CDD be done?

I. New Customers:

In case of new customer, KYC along with CDD shall be done at the time of commencement of account-based relationship. At the time of booking a policy, the identity and address of the customer needs to be verified while conducting KYC through any of the modes as permitted by the relevant regulatory and/or statutory authorities in the following manner:

(a) **Customers who are natural persons**:

i. Address/location details
ii. Identity Proof and recent photograph

(b) **Customers that are legal/juridical persons**:

i. Legal status of the legal person/entity through proper and relevant documents.
ii. Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person is established and verified.
iii. Understand the ownership and control structure of the customer and determine who are the natural persons and ultimately control the legal person.

List of documents required for conducting KYC is attached as **Annexure –A.**

In case the customer falls within the high risk category, an additional due diligence in the form of 'Customer Evaluation Sheet' (attached herewith as **Schedule II**) capturing the customer profiling details needs to be undertaken by representatives of sales function/agent/intermediary at the point of sale.

II. Existing Customer

Necessary customer due diligence with KYC shall be done for the existing customers from time-to-time basis the adequacy of the data previously obtained.

In case of non- availability of KYC of the existing customers/policyholders, the same shall be collected within 2 years from the effective date of the Guidelines for low-risk customers and within 1 year for other customers (including high risk customers).

For continuity of operations, in case where aggregate premium is not more than Rs. 50,000/- in the financial year, PAN details/Form 60 may be obtained from the customers/policyholders.

III. Ongoing due diligence:

The risk assessment and ongoing due diligence shall also be carried out in the following cases:

i. In case of any endorsement for change in name or address more than 3 times in a financial year
ii. Where there is remittance of additional premium of more than 50% of the base premium during the subsistence of the specific insurance policy
iii. Where there is request for enhancement of sum insured of more than 50% of the original sum insured during the subsistence of the specific insurance policy
iv. Assignment to third parties not related to customer/policyholder except where insurance policy is assigned to Banks/ FIs/ Capital market intermediaries regulated by IRDAI/RBI/ SEBI or Marine cargo insurance policies

IV. Verification at the time of pay out (Claim/ refund/ reimbursement)

i. No payments shall be allowed to third parties except as provided in the insurance contract and/or payments to beneficiaries/ legal heirs/assignees in case of death benefits.
ii. Necessary due diligence shall be carried out before making any payment to the Policyholder/ Beneficiaries/ Legal heirs/ assignee, as the case may be.
iii. Frequent free look cancellations, 3 or more cancellations by the same customer during the calendar month where the total amount refunded is in excess of one lakh.

B. How shall KYC and CDD be done

I. Where the client is a natural or Individual person:

The Company shall conduct KYC to verify the identity and address of the customer through any of the modes as permitted by the relevant regulatory and/or statutory authorities at the time of commencement of account-based relationship.

A list of documents to be verified and / or collected, as the case may be, under KYC norms of individuals is given in **Annexure-A**

II. Where a client is a juridical person:

While implementing the KYC norms on juridical persons, the Company will identify and verify their legal status through various documents (Refer Annexure-A) to be collected or procured through digital modes, in support of

- The name, legal form, proof of existence,
- Powers that regulate and bind the juridical persons,
- Address of the registered office/ main place of business,
- Authorized individual person(s), who is/ are purporting to act on behalf of such client, and
- Ascertaining Beneficial Owner(s)

The determination of beneficial ownership shall be ascertained during the solicitation stage. However, verification of the beneficial owner will be undertaken at the claim stage. Necessary information with respect to identification and KYC of the beneficial owner(s) is attached as **Annexure B**

III. Where client is a group Policyholder:

Under all kinds of Group Insurance, KYC of Master Policyholders / Juridical Person / Legal Entity and the respective Beneficial Owners (BO) shall be collected. However, the details of all the individual members covered under the group insurance needs to be maintained by Master Policyholders. The concerned business function needs to ensure that the details of beneficiaries are made available to the Company as and when required.

C. Modes of conducting KYC

The KYC can be conducted through any of the following method:

- Aadhaar based KYC through online Authentication
- Aadhaar based KYC through offline verification
- Digilocker KYC
- Digital KYC
- Video Based Identification Process

- By using KYC identifier allotted by CKYCR
- By using officially valid documents and
- PAN/ Form 60 (if PAN not available)
- Any other documents required to verify the identity and address of customer

Keeping in view the high volume of insurance policies underwritten by the Company and in order to facilitate seamless customer service, e-KYC and/or CKYC shall be the preferred modes for conducting KYC of the customers. However, other modes may be adopted in case the circumstances so warrants.

For modes of conducting KYC, please refer **Annexure C** for reference.

The Company shall endeavour to conduct KYC of the customers on its own; however there may be circumstances where the Company may have to rely on KYC conducted by third parties. Under such circumstances, following conditions needs to be complied:

(a) Necessary information of such CDD carried out by the third party shall be obtained immediately;

(b) Necessary steps shall be taken by the Company to ensure that copies of identification data and other relevant documentation relating to the CDD requirements are made available by the third party upon request without delay;

(c) Such third party shall be regulated, supervised or monitored, and has measures in place for compliance with CDD and record-keeping in line with the requirements and obligations under the PMLA;

(d) The third party is not based in a country or jurisdiction assessed as high risk;

(e) The ultimate responsibility for CDD and undertaking enhanced due diligence measures shall lie with the Company

(f) Where the Company relies upon third party that is part of the same financial group, it shall obtain KYC documents or the information of the client due diligence within 15 days.

6. Risk Assessment/ Categorization:

The Company will classify the customer into high risk and low risk based on individual‘s profile and product profile. The Guidelines further require identifying, assessing, documenting and taking effective measures to mitigate ML and TF risk for customers or geographic areas, products, services, nature and volume of transactions or delivery channels etc. The Guidelines also specify illustrative category of customers for classification purposes.

The majority of general insurance business is based on indemnity, wherein there is no investment component in the insurance contracts offered by general/health insurance companies and the payment is made at the time of claim(s) which not only is based on occurrence of the insured contingent event but also to the extent of actual loss suffered. Further, motor and health insurance constitutes more than 50% of general insurance business and majority of claims are settled on cashless basis whereby the claim payment is directly made to the network hospital providers and/or garages, as the case may be. All the claims are examined with respect to admissibility as per the terms of insurance policy and entitlement of the intended beneficiary.

The susceptibility of general insurance business to money laundering is minimal and the premium is highly disproportionate to the sum insured. Further, vulnerability of customers on the basis of occupancy may not be relevant and suitable for general insurance business.

Keeping in view the above, general insurance business is classified as low risk from an AML point of view, it will be appropriate to undertake risk categorization on the basis of underlying asset, quantum of sum insured and mode of premium payment apart from specified category of customers which may pose higher risk.

Basis of categorization:

I. Underlying asset

- Type of asset (hypothecated or non-hypothecated)
- When was the asset purchased and
- Overall quantum of premium paid by the customer

II. Mode of Payment

- Mode or multiple modes of payment of premium

III. **Type of Customer**

- Net worth/Constitution
- PEP
- Residential status

Particulars	Low Risk	High Risk
How to Identify the risk	All risks other than those defined as High risk	**I. Underlying asset** • Non-hypothecated asset bought by an individual/ proprietor/partnership firm/LLP/LLC • Policy issuance in the 1st year of purchase and • SI exceeds Rs. 2 crore for motor and Rs. 50 crore for non- motor insurance

		II. Mode of Payment • Where multiple modes of premium payment used for payment of premium for single policy, including DD and / or cash. • Where value of DD(s) is more than Rs. 50,000. • Aggregate value of such payments exceeds Rs. 2,00,000 a month or Rs. 10,00,000 on annual basis. III. **Type of Customer** • HNI customer - individual customer paying premium of Rs. 5 lakh on all policies purchased in a year (excluding motor products) • PEP/close relative of PEP/PEP is beneficial owner • NRI/Foreign resident and who is also HNI • Trust/NGO where premium payment exceeds Rs. 10 lakh in a year • Customers emanating from countries identified as deficient in AML/CFT regime
KYC and Due Diligence requirement	Basic requirements of verifying the identity and location of the customer are to be met	Need enhanced due diligence, KYC and underwriting procedures, wherever appropriate, shall ensure higher verification and counter checks.

The Company shall also carry out ML and TF risk assessment on entity basis taking cognizance of the sector and country specific vulnerabilities, commensurate to its size, geographical presence, complexities and activities/structure etc. The risk assessment may be reviewed every alternate year.

7. Contracts with Politically Exposed Persons (PEP)

All proposals of PEPs shall be examined by the Head of Office. Further, appropriate on-going risk management procedures needs to be implemented by the underwriting function for conducting due diligence on on-going basis to PEPs (individually as well as being the beneficial owner) and their close relatives.

Keeping in view the fact that the information relating to PEPs is neither available in public domain nor any data base is in existence, the Company may take necessary declarations from the customers besides trying to procure information from other available resources.

8. Sharing KYC information with Central KYC Registry (CKYCR):

The Customers information shall be shared with CKYCR in the prescribed KYC templates prepared for Individual or Legal entities as the case may be. The scenario-based actions required by the Company is detailed as under:

Scenario	**Actions required**
Where a customer submits a "KYC identifier" for KYC	The Company shall retrieve the KYC records from CKYCR. In such case, the customer shall not submit the KYC records unless there is a change in the KYC information required by Company as per Rule 9(1C) of PML Rules.
KYC identifier is not submitted by customer	The Company shall search (with certain credentials) for the same on CKYCR portal and record the KYC identifier of the client/ customer, if available.
If the KYC identifier is not submitted by the client/customer or not available in the CKYCR portal	The Company shall capture the KYC information in the prescribed KYC Template meant for Individuals or Legal Entities, as the case may be.

Note:

(i) The Company shall file the electronic copy of the client's KYC records with CKYCR within 10 days after the commencement of account-based relationship with a client/customer (both Individual/ legal entities).

(ii) Once "KYC Identifier" is generated/ allotted by CKYCR, the Company shall ensure that the same is communicated immediately to the respective policyholder in a confidential manner, mentioning its advantage/use to the individual/legal entity, as the case may be.

9. Implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA)

.

The Company will not enter into a contract with a customer whose identity matches with any person in the UN sanction list or with banned entities and those reported to have links with terrorists or terrorist organizations.

Processing Steps

i. On weekly basis, the Company shall check the United Nations Security Council portal https://www.un.org/securitycouncil/sanctions/1267/press-releases as well as the MHA website for any updates on banned entities/individuals or keep a track on receipt of any communication from IRDAI or General Insurance Council for any updates pertaining to banned entities/individuals.

ii. Maintain a list of these entities and keep it updated as and when any change occurs

iii. The positive matches, if any will be shared with the compliance function for further evaluation.

iv. Evaluate the data received and check whether the match is found on more than one parameter i.e. name, date of birth, passport number etc. If yes, the same has to be reported to FIU within 7 days of identification by filing a Suspicious Transaction Report (STR).

v. The process as specified in Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) is detailed in **Annexure D**

The Company may also undertake screening services from suitable service provider for compliance with above stated requirement, if required.

10. Monitoring and Reporting of Transactions:

i. Appropriate 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.

ii. The Company shall monitor the transactions of the customers on an ongoing basis, as specified in clause 5 A III, and identify transactions that fall outside the regular pattern of activity keeping in view the risk of ML. Special attention shall be paid to complex, unusually large transactions and all unusual patterns having no apparent economic or visible lawful purpose.

iii. High risk customer shall be subjected to enhanced due diligence.

iv. All transactions including those of suspicious nature shall be reported to the Principal Officer on an immediate basis and the Principal Officer shall monitor and ensure that suspicious transactions shall be regularly reported to the Director,

Financial Intelligence Unit-India. An illustrative list of suspicious transactions is attached herewith as **Annexure E.**

v. Reporting to Financial Intelligence Unit-India

- In terms of the PML Rules, reporting entities are required to report information relating to cash and suspicious transactions 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.
  Website: http://fiuindia.gov.in

- The Company shall carefully go through all the reporting requirements and formats that are available on the website of FIU –IND

- These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIU-IND. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, Company shall adhere to the following:

  a) The Cash Transaction Report (CTR) (wherever applicable) i.e., all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency, for each month shall be submitted to FIU-IND by 15th of the succeeding month.

  b) All series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency. The Suspicious Transaction Report (STR) shall be submitted 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 shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.

c) The Non-Profit Organization Transaction Reports (NTRs) i.e., all transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency for each month shall be submitted to FIU-IND by 15th of the succeeding month.

d) Counterfeit Currency Reporting (CCRs): 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

- The Principal Officer will be responsible for timely submission of CTR, CCR, STR and NTR to FIU-IND.

- Utmost confidentiality shall be maintained in filing of CTR, STR, CCR and NTR to FIU-IND.

- No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/ non–profit organization transactions to be reported.

- The Company shall not put any restrictions on operations in the accounts where an STR has been made. The Company and its directors, officers, and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the policyholder at any level

- The Company shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

- The Company shall submit the report(s) to FIU-IND in such manner and in such format as may be prescribed from time to time.

11. Record Keeping

The records prepared and maintained by the Company must be such that

- the requirements of the law and expectations of the Authority are fully met;
- auditors and authorities are able to assess the effectiveness of Company's AML/CFT policies and procedures;
- any transaction or instruction conducted through the Company on behalf of any individual customer can be reconstructed;
- any customer or underlying beneficial owner can be properly identified;

- all suspicious transaction reports received internally, and those submitted to FIU, can be identified; and
- the Company can meet, within the required time frame, any inquiries or court orders from the appropriate law enforcement agencies.

How long shall the records, be retained

The minimum periods for which records must be maintained to comply with the requirements of the law are outlined in the following table

S. No	Record Description	Records to be maintained for
1	All cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;	At least for 5 years from the date of transaction
2	All series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency:	At least for 5 years from the date of transaction
3	All transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency;	At least for 5 years from the date of transaction
4	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;	At least for 5 years from the date of transaction
5	Records relating to the verification of identity of clients	Not less than for a period of five years from the date of end of the business relationship with the customer.
6	The Company shall retain the records of those contracts, which have been settled by claim or cancelled.	For a period of at least 5 Years after settlement of claim.
7	In situations, where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure. Wherever practicable, Company is required to seek and retain relevant identification documents for all such transactions and report such transactions of suspicious funds.	Shall be retained until it is confirmed that the case has been closed and 5 years thereafter.

8	In case of customer identification data obtained through the customer due diligence process, account files and business correspondence shall be retained.	At least for 5 Years after the business relationship has ended

How the records shall be maintained

The records shall contain all necessary information specified by the Authority to permit reconstruction of individual transaction, including the following information: -

(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.

12. Training to Employees, Agents and Intermediaries

The Company shall impart training on Guidelines to its employees, agents and intermediaries on an ongoing basis. The focus of the training may be different for frontline staff, compliance staff, staff dealing with new customers and claims.

The Company shall endeavor to train its agents and intermediaries at regular intervals. The training material shall be reviewed on periodical basis or earlier if there is any change in the relevant regulatory and/or statutory prescriptions.

13. Internal Control/Audit

Internal audit/inspection department of the Company shall periodically verify compliance with the extant policies, procedures and controls related to money laundering activities on the basis of overall risk assessment. The Company shall also upgrade its questionnaire and system from time-to-time in accordance with the existing PMLA and PML Rules. The reports should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects. The Company shall submit audit notes and compliance to the Audit Committee.

Schedule I

Definitions:

"Aadhaar number", means an identification number issued to an individual under sub-section (3) of Section 3 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services)Act,2016 (Aadhaar Act), and includes any alternative virtual identity generated under sub-section (4) of that section;

Subsection (3) of Section 3 of Aadhaar Act:
On receipt of the demographic information and biometric information under sub-section (1), the Authority shall, after verifying the information, in such manner as may be specified by regulations, issue an Aadhaar number to such individual.

Subsection (4) of Section 3 of Aadhaar Act:
The Aadhaar number issued to an individual under sub-section (3) shall be a twelve-digit identification number and any alternative virtual identity as an alternative to the actual Aadhaar number of an individual that shall be generated by the Authority in such manner as may be specified by regulations.

"Authentication" means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

"Beneficial owner" means an individual who ultimately owns or controls a client of a reporting entity or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person

For identification and determination of beneficial owner, please refer Annexure B

"Central KYC Records Registry" (CKYCR) means a reporting entity, substantially owned and controlled by the Central Government, and authorised by that Government through a notification in the Official Gazette to receive, store, safeguard and retrieve the KYC records in digital form of a client as referred to in clause (ha) in such manner and to perform such other functions as may be required under these rules

"Client" means a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who engaged in the transaction or activity, is acting

Explanation: For the purpose of AML guideline, the term client includes a customer/ person (Natural or Juridical) who may be a proposer or policyholder, or master policyholder or life assured or beneficiaries or assignees, as the case may be.

“Client Due Diligence” (CDD) means due diligence carried out on a client

“Designated Director" means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes

(i) the Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,

(ii) the managing partner if the reporting entity is a partnership firm,

(iii) the proprietor if the reporting entity is a proprietorship concern,

(iv) the managing trustee if the reporting entity is a trust,

(v) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a [body of individuals;]

[(va) a person who is heading the reporting entity in India, if the reporting entity is located in an International Financial Services Centre; and]

(vi) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

Explanation. - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 1956 (1 of 1956);]

“Digital KYC” means the capturing live photo of the client 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 reporting entity as per the provisions contained in the Act;

“KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

“KYC Records” means the records, including the electronic records, relied upon by a reporting entity in carrying out client due diligence as referred to in rule 9 of these rules.

“Offline verification” means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations

“On-going Due Diligence” means regular monitoring of transactions to ensure that they are consistent with the customers‟ profile and source of funds.

"Officially Valid Document" shall have the meaning assigned to it under sub clause (d) of clause (1) of Rule 2 of the PML Rules 2005.

List of documents covered are as under:

a. Passport
b. Driving licence
c. Proof of possession of Aadhaar number
d. Voter's Identity Card issued by Election Commission of India,
e. Job card issued by NREGA duly signed by an officer of the State Government
f. Letter issued by the National Population Register containing details of name, address and Aadhaar or any other document as notified by the Central Government in consultation with the Regulator

Provided that where simplified measures are applied for verifying the identity of the clients the following documents shall also be deemed to be 'officially valid documents:

(a) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions.
(b) letter issued by a gazetted officer, with a duly attested photograph of the person

Provided further that where simplified measures are applied for verifying the limited purpose of proof of address of the clients, where a prospective customer is unable to produce any proof of address, the following documents shall be deemed to be 'officially valid document':

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

(b) property or Municipal tax receipt;

(c) bank account or Post Office savings bank account statement [or if the reporting entity is located in an International Financial Services Centre, statement of foreign bank];

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

(e) letter of allotment of accommodation from employer issued by State or Central Government Departments or Public Sector Undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and licence agreements with such employers allotting official accommodation; and

[Provided also that in case the officially valid document presented 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 also that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the

photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document

"Provided also that where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as are issued by the Unique Identification Authority of India

[Explanation - For the purpose of this clause, a document shall be deemed to be an "officially valid document" even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.]"

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

"Principal Officer" means an officer designated as such by the Company.

"Suspicious Transaction" shall have the meaning assigned to it under sub clause (g) of clause (1) of Rule 2 of the PML Rules

Rule 2 (1) (g) of the PML Rules

"Suspicious Transaction" means a transaction referred to in *clause (h),* 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 have no 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 organisation or those who finance or are attempting to finance terrorism.]

Rule 2 (1) (h) of the PML Rules

"transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes –

(i) opening of an account;

(ii) 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;

(iii) the use of a safety deposit box or any other form of safe deposit;

(iv) entering into any fiduciary relationship;

(v) any payment made or received in whole or in part of any contractual or other legal obligation;

(vi) any payment made in respect of playing games of chance for cash or kind including such activities associated with casino; and

(vii) establishing or creating a legal person or legal arrangement.]

"Video Based Identification Process (VBIP)" means an alternative (optional) electronic process of Identification/ KYC in paperless form, carried out by the insurer/authorised person (person authorised by the insurer and specifically trained for face-to-face VBIP) by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer/beneficiary to obtain identification information including the necessary KYC documents required for the purpose of client due diligence and to ascertain the veracity of the information furnished by the customer/ beneficiary.

Words and expressions used and not defined in this Policy but defined in the Insurance Act, 1938 (4 of 1938), Insurance Regulatory and Development Authority Act, 1999 (41 of 1999), the PML Act, the PML Rules, the Aadhaar Act, Unlawful Activities (Prevention) Act, 1967 shall have the meanings respectively assigned to them in those Acts, Rules, Regulations, Guidelines issued under those Acts, as the case may be.

Schedule II

Customer Evaluation sheet

1. Name of the Proposer: _____
2. Occupation(Tick as applicable) ☐ Salaried ☐ Self Employed/Business

3. Present Address : _____

_____

4. Mobile :_____
5. Phone (with STD/ISD Code _____
6. Email ID :_____
7. Annual Income (Tick as applicable)

☐ . 5 Lakh ☐ Lakh to 10 Lakh; ☐ 0 Lakh to 25 Lakh;

☐ 25 Lakh

8. If the proposer is salaried:

Name of Employer :_____

Address of the Office :_____

_____

9. If the proposer is a Self-employed/Business:

Nature (Tick as applicable): ☐ Sole Propriter ☐ Partnership

Name of the entity: _____

Address of the entity: _____

_____

10. Insurance Product Applied for: _____

11. Category of Business (Tick as applicable): ☐ First Time ☐ Renewal

---

To be filled and signed by either employee or Agent

Signature:_____ Signature:_____

Name of the Employee:_____ Name of Agent:_____

Employee ID:_____ Agent Code: _____

Annexure A – List of Officially Valid Documents	
Type of customer	**Documents**
Individual • ***Proof of Identity***	Any of the below '*Officially valid document'* namely; i. Passport ii. Permanent Account Number (PAN) Card iii. Proof of possession of Aadhaar number iv. Driving license v. Voter's Identity Card issued by Election Commission of India vi. Job card issued by NREGA duly signed by an officer of the State Government vii. Letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government in consultation with the Regulator An individual can also submit the following: • Aadhaar number where, (i) he 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) he decides to submit his Aadhaar number voluntarily to a banking company or any reporting entity notified under first proviso to sub-section (1) of section 11A of the Act; or • Proof of possession of Aadhaar number where offline verification can be carried out; or • the proof of possession of Aadhaar number where offline verification cannot be carried out or any officially valid document or the equivalent e-document thereof containing the details of his identity and address; and • the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and • such other documents including in respect of the

	nature of business and financial status of the client, or the equivalent e-documents thereof as may be required by the reporting entity:] Provided that if the client does not submit the Permanent Account Number, he shall submit one certified copy of an 'officially valid document' containing details of his identity and address, one recent photograph and such other documents including in respect of the nature or business and financial status of the client as may be required by the reporting entity. [Explanation. - Obtaining a certified copy by reporting entity shall mean comparing the copy of officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the reporting entity in a manner prescribed by the regulator.] **Provided that where simplified measures are applied for verifying the identity of the clients the following documents shall [also] be deemed to be *'officially valid documents'*:** (a) identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions; (b) letter issued by a gazetted officer, with a duly attested photograph of the person;]
• ***Proof of Address***	In case of officially valid document furnished by the client does not contain updated address, the following documents [or their equivalent e-documents thereof] shall be deemed to be officially valid documents for the limited purpose of proof of address:- (a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); (b) property or Municipal tax receipt; (c) pension or family pension payment orders (PPOs) issued to retired employees by Government

	Departments or Public Sector Undertakings, if they contain the address; (d) 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 the client shall submit updated officially valid document [or their equivalent e-documents thereof] with current address within a period of three months of submitting the above documents. **Provided further that where simplified measures are applied for verifying the limited purpose of proof of address of the clients, where a prospective customer is unable to produce any proof of address, the following documents shall [also] be deemed to be *'officially valid document'*:** (a) bank account or Post Office savings bank account statement [or if the reporting entity is located in an International Financial Services Centre, statement of foreign bank]; Provided also that in case the officially valid document presented 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 also that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document: Provided also that where the client submits his proof of possession of Aadhaar number as an officially valid

	document, he may submit it in such form as are issued by the Unique Identification Authority of India; [Explanation. - For the purpose of this clause, a document shall be deemed to an "*officially valid document*" even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.]
Companies • ***The name, legal form, proof of existence*** • ***Powers that regulate and bind the juridical persons,*** • ***Address of the registered office/ main place of business,*** • ***Authorized individual person(s), who is/ are purporting to act on behalf of such client, and*** • ***Ascertaining Beneficial Ownership***	The certified copies of the following documents [or the equivalent e-documents thereof], namely; (i) Certificate of Incorporation; (ii) Memorandum and Articles of Association; (iii) Permanent Account Number of the company; (iv) Resolution from the Board of Directors and power of attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf; [and] (v) such documents as are required for an individual relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
Partnership Firms • ***The name, legal form, proof of existence*** • ***Powers that regulate and bind the juridical persons,*** • ***Address of the registered office/ main place of business,*** • ***Authorized individual***	The certified copies of the following documents [or the equivalent e-documents thereof], namely: - (i) registration certificate; (ii) partnership deed; (iii) Permanent Account Number of the partnership firm; and (iv) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

person(s), who is/ are purporting to act on behalf of such client, and • ***Ascertaining Beneficial Ownership***	
Trusts and Foundations	The certified copies of the following documents [or the equivalent e-documents thereof], namely:- (i) registration certificate; (ii) trust deed; (iii) Permanent Account Number or Form No.60 of the trust; and (iv) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
Unincorporated association or a body of individuals	The certified copies of the following documents [or the equivalent e-documents thereof], namely:- (i) resolution of the managing body of such association or body of individuals; (ii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals; (iii) power of attorney granted to him to transact on its behalf; [and] (iv) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf; (v) such information as may be required by the reporting entity to collectively establish the existence of such association or body of individuals.

Note-:

(i)No further documentation is necessary for proof of residence where the document of identity submitted also includes the proof of residence/address.

(ii) Where a customer submits Aadhaar for identification and wants to provide current address different from the address available in the Central Identities Data Repository, the customer may give a self- declaration to that effect to the Company.
(iii) Under Individual Policies, those individuals who are not able to undergo Aadhaar Authentication due to any injury, illness or old age or otherwise, or they do not wish to go for Aadhaar Authentication, they may submit their Officially Valid Documents (OVDs) at the time of commencement of Account based relationship.
(iv) In case of low risk customers and cases where aggregate premium per annum is less than or equal to Rs. 10,000/- , simplified due diligence needs to be undertaken. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.
(v) In case of high risk customers, KYC and underwriting procedures should ensure higher verification and counter checks. An enhanced due diligence in the form of 'Customer evaluation sheet' capturing the customer profiling details needs to be undertaken by the sales staff/agent/intermediary at the point of sale.

Annexure-B

Identification and KYC of beneficial owner

S. No	Applicable for	Beneficial owner		KYC Documents required for
I	Where the client 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 a controlling ownership interest or who exercises control through other means	a) Ownership of more than 25 % of shares or capital or profits of company b) Control shall include the right to appoint majority of the directors or to control	KYC to be taken for beneficial owners if they fall in the category as defined under the Guidelines. List of Document to be checked is attached as **Annexure-A**
Ii	Where the client is a partnership firm or a company	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person	Ownership of/entitlement to more than 15% of the capital or profits of the partnership	KYC to be taken for beneficial persons if they fall in the category as defined under the Guidelines. List of Document to be checked is attached as **Annexure-A**
iii	Where the client 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	Ownership of/entitlement to more than 15% of the property or capital or profits of such association or body of individuals	KYC to be done for beneficial owners. List of Document to be checked is attached as **Annexure-A**
iv	Where no natural person is identified under	The beneficial owner is the relevant natural person who holds the position of senior managing official		KYC to be done for the specified natural person.

	(i), (ii) or (iii) above		List of Document to be checked is attached as **Annexure-A**
V	Where the client is a trust	The identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% percent 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	KYC for the settler of the trust, the trustee, the protector and the beneficiaries with 15% or more interest needs to be conducted.
vi	Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company	Not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.	

Annexure C

Modes of conducting KYC

I. Officially valid documents

Customers may submit any of the officially valid document as detailed in ***Annexure A*** along with the copy of PAN Card/Form 60 as applicable

II. Aadhaar based e-KYC

Aadhaar based e-KYC is a paperless authentication process of an individual's identity, carried out with his/her consent. This involves ID verification via biometric and demographic details available in the UIDAI database, collected during the Aadhaar registration process.

In this process, the Reporting Entity can directly access all the personal information of individuals like name, address, gender, date of birth, etc., from the UIDAI database and verify it themselves to help you establish your identity.

You can complete the verification process for Aadhaar e-KYC online or offline. The procedures for both type of mode is defined as under:

1. Online procedure for Aadhaar e-KYC

(i) Via biometrics authentication:

Customers need to go through the following procedure when opting for Aadhaar e-KYC verification via biometrics.

Step 1: Provide your Aadhaar card to your Reporting Entity. They will note your Aadhaar number or Unique Identification number (UID).
Step 2: Next, they will use a biometric scanner to capture and read your fingerprint or retinal image.
Step 3: This value is then communicated to the UIDAI, which matches this input value with the already existing value present against your Aadhaar in its database.
Step 4: Your identity will be successfully established once both the values match.
Once this verification procedure is completed, the UIDAI will give the Reporting Entity access to all your details like date of birth, address, photograph, etc.
The UIDAI also lets the Reporting Entity to keep a soft copy of such details in their servers, thus, allowing them to access such data as and when required.

(ii) Via mobile OTP authentication

You can also opt for the OTP-based authentication method, which can be carried out in the following manner.
Step 1: Produce your Aadhaar card before the Reporting Entity.
Step 2: UIDAI will send an OTP on your registered mobile number.

Step 3: Now, enter this OTP in the device provided by your Reporting Entity.

After this, the UIDAI will provide your details to the agent that is similar to the biometric authentication procedure.

2. Offline procedure for Aadhaar e-KYC

If none of the online methods is feasible, Reporting Entity can use your Aadhaar for offline KYC verification via any of the following methods.

(i) By scanning QR code:

Reporting Entity can use a mobile scanner to scan the QR code present on the Aadhaar card to extract all demographic information and complete the offline UIDAI KYC verification. Extracting information via this method does not require Reporting Entity to access the UIDAI's database.

(ii) Paperless method of offline e-KYC:

Following method can be opted to get your Aadhaar e-KYC done offline.
Step 1: Go to the official portal of the UIDAI.
Step 2: Enter your 12 digit Aadhaar number or 16-digit Virtual identification Number (VID) and enter captcha code. Click on "Send OTP."
Step 3: Enter the OTP received on your registered mobile number and download the Aadhaar XML. It contains your details like name, gender, date of birth, address, and hashed email and mobile number, among other information. It is also digitally signed by UIDAI and is protected with a 4-character Share Code.
Step 4: You can then provide this XML file to your Reporting Entity along with Share Code, who will then verify your identity using the machine-readable details in the file.

III. KYC through CKYC Portal

Central KYC Registry is a centralized repository of KYC records. Once the KYC documents are submitted by a customer, they are registered in the repository with a unique CKYC number. The CKYC number can be quoted instead of submitting physical KYC documents for any financial transaction. The CKYC repository can be accessed by all financial institutions for verifying the KYC details of their customers.

A. **Where a client submits a KYC Identifier to a reporting entity**, then such reporting entity shall retrieve the KYC records online from the Central KYC Records Registry by using the KYC Identifier and shall not require a client to submit the same KYC records or information or any other additional identification documents or details, unless -

- there is a change in the information of the client as existing in the records of Central KYC Records Registry;

- the current address of the client is required to be verified;
- the reporting entity considers it necessary in order to verify the identity or address of the client, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

Process to retrieve information is as under:

- Reporting entity can search for the record by entering CKYC identifier or by entering a valid ID type and number.
- Reporting entity can download single / bulk records by entering CKYC identifier and an authentication factor (viz. date of birth / date of incorporation).

Step 1- Visit the web portal of any KRA agency (www.karvykra.com or www.cvlkra.com). (Currently only Karvy and Central Depository Services Limited provide for the CKYC Check Facility.)
Step 2- Enter your PAN.
Step 3- Enter the security/CAPTCHA code.
Step 3- Your CKYC status along with details will be displayed.

B. **In case customer doesn't have CKYC identifier**, the customer needs to submit following documents to reporting entity(RE) and RE shall upload these details on CKYC portal

- The data captured as per the common KYC template is to be uploaded on the Central KYC portal along with the scanned copy of the supporting documents. For an individual record, the signature and photograph is to be cropped separately and uploaded.
  The specifications for scanning the supporting documents and photograph are stated below:
  (i). Document should be scanned in grey-scale with a scanning resolution of 150-200 DPI.
    a. Photograph must be a recent passport size, preferably in colour. However, scanning has to be in colour mode.
    b. Dimensions 200 x 230 pixels
    c. Size of photograph should be between 20kb-50kb
  (ii). Acceptable file format : '.tif', '.tiff', '.pdf', '.jpeg', '.jpg'
  (iii). File Size (Maximum Limit): 350 kb for individual KYC record.
- The reporting entity can bulk upload the KYC details and scanned images. Images for each record will be required to be zipped separately. The master zip file will be digitally signed by the reporting entity.
- Bulk files can be uploaded either at the branch, region or institution level.
- The entity should ensure adequate internet bandwidth for bulk upload. Bulk upload is provided via SFTP. For bulk upload of size less than 20 MB the Central KYC front-end application may also be used. Based on validations, a response file will be generated. This file will contain the success records, error records and download records. The response file is available for download from the Central KYC application.

Upon successful upload, customer will be provided with a 14 digit KYC Identifier Number (KIN). An SMS/email will be sent by CERSAI to your registered mobile number once the KIN is generated. Customer can quote this KIN for any kind of financial transaction and customer doesn't have to submit KYC documents again unless there is a change in your KYC details.

C. **If customer provides CKYC identifier number but details are not updated**, In case of change of existing information of a customer (including minor turning major) in the records of Central KYC Registry, a reporting entity will initiate an update request.

- The updated data along with the scanned copy of the supporting document, where required, will be uploaded on the Central KYC Registry portal.
- In order to initiate an updation request, the reporting entity will need to have the latest KYC record of the customer.
- On updation of a KYC record at the Central KYC Registry, all linked entities (institutions that have either uploaded or downloaded the KYC record for that particular KYC record), will receive an electronic update notification of KYC record. The entities can download the last updated record of the customer.

IV. Digital KYC Process

1. "**Digital KYC**" means capturing live photo of the client 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 reporting entity as per the provisions contained in the Act;

Process:

A. The reporting entities 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 the Reporting Entities.

B. The access of the Application shall be controlled by the Reporting Entities and 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 Reporting Entities to its authorized officials.

C. The client, for the purpose of KYC, shall visit the location of the authorized official of the Reporting Entity or vice-versa. The original Officially Valid Document (OVD) shall be in possession of the client.

D. The Reporting Entity must ensure that the Live photograph of the client is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Reporting Entity

shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Reporting Entities) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the client.

E. The Application of the Reporting Entities shall have the feature that only live photograph of the client is captured and no printed or video-graphed photograph of the client is captured. The background behind the client 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 client.

F. Similarly, the live photograph of the original officially valid document 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 client 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 client. 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 client's own mobile number. Upon successful validation of the OTP, it will be treated as client signature on CAF. However, if the client 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 the Reporting Entity shall not be used for client signature. The Reporting Entity must check that the mobile number used in client 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 client 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 the Reporting Entity. 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 the Reporting Entity, 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 client for future reference.

L. The authorized officer of the Reporting Entity 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 client 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 representative of the Reporting Entity 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.

V. Video Based Identification Process (VBIP)

The Company may undertake live VBIP by developing an application which facilitates KYC process either online or face-to-face in-person verification through video. This may be used for establishment/continuation/ verification of an account based relationship or for any other services with an individual customer/beneficiary, as the case may be, after obtaining his/her informed consent and shall adhere to the following stipulations:

a) The authorised person of the Company while performing the VBIP for KYC shall record clear live video of the customer/beneficiary present for identification and obtain the identification information in the form as below:

i) Aadhaar Authentication if voluntarily submitted by the Customer/ beneficiary, subject to notification by the government under Section 11 A of PMLA or

ii) Offline Verification of Aadhaar for identification, if voluntarily submitted by the Customer/beneficiary or

iii) Officially Valid Documents (As defined in rule 2(d) under PML Rules 2005) provided in the following manner –

1) As digitally signed document of the Officially Valid Documents, issued to the Digilocker by the issuing authority

or

2) As a clear photograph or scanned copy of the original Officially Valid Documents, through the e-Sign mechanism.

b) The Company may also utilize this facility to verify PAN (wherever applicable). The authorised person of the Company 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. Use of printed copy of e-PAN is not valid for VBIP.

c) The authorised person of the Company shall ensure that the online video is clear and the customer/beneficiary along with the authorised person in the video shall be easily recognisable and shall not be covering their face in any manner.

d) Live location of the customer/beneficiary (Geotagging) shall be captured (both for online/ face-to-face VBIP) to ensure that customer/beneficiary is physically present in India.

e) The authorised person of the Company shall ensure that the photograph and other necessary details of the customer/beneficiary in the Aadhaar/ Officially Valid Documents/ PAN matches with the customer/beneficiary present for the VBIP.

f) The authorised person of the Company shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

g) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, if voluntarily submitted by the Customer/ beneficiary, it shall be ensured that the generation of XML file or QR code is recent and not older than 3 days from the date of carrying out VBIP.

h) All accounts opened or any service provided based on VBIP shall be activated only after being subject to proper verification by the Company to ensure that the integrity of process is maintained and is beyond doubt.

i) The Company shall ensure that the process is a seamless, real-time, secured end- to-end encrypted audio-visual interaction with the customer/beneficiary and the quality of the communication is adequate to allow identification of the customer/ beneficiary beyond doubt. The Company shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

j) To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the VBIP application as per extant norms before rolling it out and thereafter from time to time.

k) The audio-visual interaction shall be triggered from the domain of the Company itself, and not from third party service provider. The VBIP process shall be operated by the Company/authorized persons. The activity log along with the credentials of the official performing the VBIP shall be preserved.

l) The Company shall ensure that the video recording bears the GPS coordinates, date (DD/MM/YY) and time stamp (HH.MM.SS) along with other necessary details, which shall be stored in a safe and secure manner as per PML Rules.

While exercising Online VBIP, the Company shall exercise extra caution and the additional necessary details viz. IP address etc. shall be preserved by the Company to substantiate the evidence at the time of need.

m) The Company shall endeavour to take assistance of the latest available technology (including Artificial Intelligence (AI) and face matching technologies etc.) to strengthen and ensure the integrity of the process as well as the confidentiality of the information furnished by the customer/beneficiary. However, the responsibility of identification shall rest with the Company.

n) Authorized person of the Company shall facilitate face to face VBIP process only at the customer/beneficiary end.

However, the ultimate responsibility for client due diligence will be with the Company.

o) The Company shall maintain the details of the concerned Authorised person, who is facilitating the VBIP.

p) The Company shall ensure to redact or blackout the Aadhaar number as per extant PML Rules.

q) The Company shall adhere to the IRDAI Cyber security guidelines as amended from time-to-time along with the necessary security features and standard as mentioned below:

- The Video KYC application and related APIs/Web Services shall undergo application security testing (both gray box and white box) through a CERT-In empanelled vendor and all reported vulnerabilities shall be mitigated before moving into production.

- The infrastructure components used for hosting Video KYC application shall undergo vulnerability assessment and secure configuration review through a CERT-In empanelled vendor and all reported vulnerabilities shall be mitigated before moving into production.

- There shall be an end-to-end encryption from the customer/beneficiary to the hosting point of the Video KYC

application. The minimum encryption standards and key lengths like AES 256 for encryption should be used.

- If the Video KYC application and video recordings are located at a third party location and/or in Cloud then the third party location and/or cloud hosting location shall be in India.

Annexure D

Implementation of Section 51A of UAPA

To implement the said section an order reference F. No. 14014/01/2019/CFT dated 2nd February, 2021, has been issued by the Government of India. The salient aspects of the order with particular reference to insurance sector are detailed in the following paragraphs:

1. **Procedure for reporting/freezing of insurance policies of 'designated individuals/entities'**

   In case any matching records are identified, the procedure required to be adopted is as follows:

a) To maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in the Schedule to the Order, hereinafter, referred to as designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of insurance policies with them.

b) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the Company shall immediately inform full particulars of the funds, financial assets or economic resources or related services in the form of insurance policies, held by such a customer on their books to the Central [designated] Nodal Officer for the UAPA, at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

c) The Company shall also send a copy of the communication mentioned in 1(b) above to the UAPA Nodal Officer of the State/UT (where the account is held) and to IRDAI and FIU-IND without delay.

d) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, Company shall prevent such designated individuals/entities from conducting any transactions, under intimation to the Central [designated] Nodal Officer for the UAPA at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in, without delay.

e) The Company shall file a Suspicious Transaction Report (STR) with FIU-IND in respect of the insurance policies covered by paragraph (1) (a) above, carried through or attempted, in the prescribed format.

f) On receipt of the particulars (held in the form of Insurance Policies) of suspected designated individual/entities the Central [designated] Nodal Officer for the UAPA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the Company

are the ones listed as designated individuals/entities and the insurance policies, reported by Company are held by the designated individuals/entities.

g) In case, the results of the verification indicate that the insurance policies are owned by or are held for the benefit of the designated individuals/entities, an order to freeze these insurance policies under section 51A of the UAPA would be issued without delay and conveyed electronically by the Central [designated] Nodal Officer for the UAPA to the concerned office of Company under intimation to IRDAI and FIU-IND.

h) The said order shall take place without prior notice to the designated individuals/entities.

"Freezing of insurance contracts" would require not-permitting any transaction (financial or otherwise), against the specific contract in question.

2. Procedure for unfreezing of insurance policies of individuals/entities inadvertently affected by the freezing mechanism, upon verification that the individual/ entity is not a designated individual/entity

a) Any individual or entity, if they have evidence to prove that the insurance policies, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the concerned Company.

b) Company shall inform and forward a copy of the application together with full details of the insurance policies inadvertently frozen as given by any individual or entity, to the Central [designated] Nodal Officer of MHA within two working days.

c) The Central [designated] Nodal Officer for the UAPA shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, without delay, unfreezing the insurance policies owned/held by such applicant, under intimation to the concerned Company. However, if it is not possible for any reason to pass an Order unfreezing the assets within 5 working days, the Nodal Officer shall inform the applicant. The insurer shall act basis the feedback received from the Nodal Officer and proceed for unfreezing of the insurance policy.

3. Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001

a) U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets, derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.

b) To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the Central [designated] Nodal Officer for freezing of funds or other assets.

c) The Central [designated] Nodal Officer of MHA, shall cause the request to be examined without delay, so as to satisfy that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officer in IRDAI. The proposed designee, as mentioned above would be treated as designated individuals/entities.
d) Upon receipt of the request by Nodal Officer in IRDAI from the Central [designated] Nodal Officer, the request would be forwarded to Company and the procedure as enumerated at paragraphs (i) above on freezing of insurance policies shall be followed.
e) The freezing orders shall take place without prior notice to the designated persons involved.

4. Communication of orders under section 51A of UAPA

IRDAI would communicate all Orders under section 51A of UAPA relating to insurance policies, to all the Company after receipt of the same from MHA.

5. Exemption in accordance with UNSCR 1452

The above provisions of freezing shall not apply to funds and other financial assets or economic resources that are necessary for paying insurance premiums or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, after notification by the MEA of the intention to authorize, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification.

Annexure E

Illustrative list of Suspicious Transactions

I. Customer insisting on anonymity, reluctant to provide identifying information, or providing minimal, seemingly fictitious information;
II. Frequent free look cancellation by customers;
III. Assignments to unrelated parties without valid consideration;
IV. Request for purchase of a policy for an amount considered beyond apparent need;
V. Policy from a place where he does not reside or is not employed;
VI. Frequent request for change in addresses;
VII. Inflated or totally fraudulent claims e.g. by arson or other means causing a fraudulent claim to be made to recover part of the invested illegitimate funds;
VIII. Overpayment of premiums with a request for a refund of the amount overpaid;
IX. Refund of proposal deposit by cancelling the proposal on request of the customer;
X. Media reports about a customer;
XI. Information sought by enforcement agencies;
XII. Unusual termination of policies;
XIII. Borrowing the maximum loan amount against a policy soon after buying it