भारतीय बीमा विनियामक और विकास प्राधिकरण
INSURANCE REGULATORY AND
DEVELOPMENT AUTHORITY OF INDIA

MASTER GUIDELINES

ON

ANTI MONEY LAUNDERING/COUNTER FINANCING OF TERRORISM (AML/CFT)

Contents

...., 2022

To,

The Chairperson/ CEOs of all the Insurers

1. Introduction

In terms of the provisions of Prevention of Money- Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of records) Rules, 2005 (as amended from time to time), insurers are 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 transaction. Insurers shall take steps to implement provisions of Prevention of Money-Laundering Act, 2002 ("PMLA") and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, ("PML Rules") as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

2. Short Title, Applicability and Commencement

2.1 These guidelines shall be called as Master Guidelines on Anti-Money laundering/Counter Financing of Terrorism (AML/CFT) for all the insurers. These guidelines are issued by exercising the power enshrined under Section 34 of Insurance Act, 1938, Section 14(1) of Insurance Regulatory and Development Authority Act 1999 and provisions 4,5,7,9, 9A & 10 of the PML Rules.

2.2 These Guidelines would be applicable for all class of Life, General or Health Insurance business carried out by the 'Insurers' except Re-insurance business carried out by the 'Indian Insurance company' or 'foreign company' in India.

2.3 These guidelines would come into force after three months from the date of notification.

3. Definitions

In these guidelines, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them as below:

3.1 "Aadhaar number", shall have the meaning assigned to it under clause(a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, hereinafter referred to as 'The Aadhaar Act',

3.2 "Act" and "Rules" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

3.3 "Authentication", means the process as defined under clause (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 as amended from time to time.

3.4 "Beneficial owner" shall have the meaning assigned to it under sub clause (fa) of clause (1) of Section 2 of the PML Act.

3.5 "Central KYC Records Registry" (CKYCR) means an entity defined under clause (ac) of sub rule (1) of Rule 2 of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

3.6 "Client" shall have the meaning assigned to it under sub clause (ha) of clause (1) of Section 2 of the PML Act

Explanation: For the purpose of this 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.

3.7 "Client Due Diligence" shall have the meaning assigned to it under sub clause (b) of clause (1) of Rule 2 of the PML Rules.

3.8 "Designated Director" shall have the meaning assigned to it under sub clause (ba) of clause (1) of Rule 2 of the PML Rules

3.9 “Digital KYC” shall have the meaning assigned to it under sub clause (bba) of clause (1) of Rule 2 of the PML Rules

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

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

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

3.13 "Officially valid document" shall have the meaning assigned to it under sub clause (d) of clause (1) of Rule 2 of the PML Rules.

3.14 “Politically Exposed Persons (PEPs)” means the 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.

3.15 “Principal Officer” shall have the meaning assigned to it under sub clause (f) of clause (1) of Rule 2 of the PML Rules.

3.16 “Specified Transaction” means any transaction or class of transactions, as prescribed by the Government, were there is a high money-laundering or terrorist financing risk.

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

3.18 “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.

3.19 Words and expressions used and not defined in these guidelines but defined in the Insurance Act, 1938 (4 of 1938), Insurance Regulatory and Development Authority Act, 1999 (41 of 1999),the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005,the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016shall have the meanings respectively assigned to them in those Acts, Rules, Regulations, Guidelines issued under those Acts, as the case may be.

4. Background:

4.1 The Prevention of Money Laundering Act, 2002 came into force with effect from 1st July 2005.

The Central Government by exercising the power under section 73 of the PMLA has issued PML (Maintenance of Records) Rules 2005 and has amended the same from time to time to carry out the provisions of the PML Act.

4.2 Insurers offer a variety of products aimed at transferring certain financial risks from the insured to insurers. These products include Life, General and Health insurance contracts. These products are offered to the public through trained agents and also through a number of alternate distribution channels.

4.3 The obligation to establish an anti-money laundering program applies to insurers as per provisions of Rule 9(14) (ii)& (iii) of the PML Rules. They have the responsibility for guarding against insurance products and services being used to launder unlawfully derived funds or to finance terrorist acts.

5. What is Money Laundering?

5.1 Money Laundering is a process or activity of moving illegally acquired money through financial systems so that it appears to be legally acquired. Section 3 of PMLA specifies the Offence of Money Laundering.

5.2 There are three common stages of money laundering as detailed below which are resorted to by the launderers. Insurers may unwittingly get exposed to a potential criminal activity while undertaking normal business transactions: -

5.2.1 **Placement** - the physical disposal of cash proceeds derived from illegal activity;

5.2.2 **Layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and

5.2.3 **Integration** - creating the impression of apparent legitimacy to criminally derived wealth.

If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds. Insurers are therefore placed with a statutory duty to make a disclosure to Financial Intelligence Unit-India (FIU-IND) when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of drug trafficking or of a predicated offence, or was or is intended to be used in that connection is passing through the insurers. Such disclosures are protected by law, enabling the person with information to be able to disclose the same without any fear.

6. Internal policies, procedures, and controls:

6.1 Every Insurer has to establish and implement policies, procedures, and internal controls that effectively serve to prevent and impede Money Laundering (ML) and Terrorist Financing (TF).

6.2 To be in compliance with these obligations, the senior management of insurers shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The insurers shall:

6.2.1 Develop an AML/CFT program comprising of policies and procedures, for dealing with Money- laundering (ML) and Terrorist Financing (TF) reflecting the current statutory and regulatory requirements

6.2.2 Ensure that the content of these guidelines are understood by all staff members/agents.

6.2.3 Review the AML/CFT program atleast once in a year on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures and to avoid conflict of interest, the person doing such a review shall be different from one who has framed such policies and procedures

6.2.4 Adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF

6.2.5 Undertake client due diligence ("CDD") measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction

6.2.6 Have in place a system for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities (if so required); and

6.2.7 Develop staff members'/agents' awareness and vigilance to guard against ML and TF

6.3 Policies and procedures set under AML/CFT program shall cover:

6.3.1 Communication of policies relating to prevention of ML and TF to all management and relevant staff that handle policyholder's

information, (whether in branches or departments) in all the offices of the insurer;

6.3.2 Client due diligence measures, including requirements for proper identification;

6.3.3 Maintenance of records;

6.3.4 Compliance with relevant statutory and regulatory requirements;

6.3.5 Co-operation with the relevant law enforcement authorities, including the timely disclosure of information;

6.3.6 Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff, of their responsibilities in this regard. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

6.3.7 AML/CFT program should be reviewed from time to time to conform with the extant PMLA and PML Rules.

7. Appointment of a Designated Director and a Principal Officer:

7.1. A "Designated Director" has to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules shall be appointed or designated by the insurers.

7.2. A Principal Officer (PO) at a senior level and preferably not below the level of Head (Audit/Compliance)/Chief Risk Officer shall be appointed to ensure compliance with the obligations imposed under chapter IV of the Act and the Rules.

7.3. The contact details with mobile no. and email id of the Designated Director and the Principal Officer or any changes thereon shall be communicated to IRDAI and FIU-IND within 7 days of its effect.

7.4. In terms of Section 13(2) of the PMLA, the Director, FIU-IND can take appropriate action, including imposing a monetary penalty on insurers or its Designated Director or any of its employees for failure to comply with any of its AML/CFT obligations.

8. Recruitment and Training:

Periodic risk management reviews should be conducted at least once in a year to ensure Insurer's strict adherence to laid down process and strong ethical and control environment. The concept of AML/CFT should be part of in-house training curriculum for employees/ agents.

8.1 Insurers should have adequate screening procedures while engaging employees/ agents/ Director/ Key Management Personnel (KMPs).

8.2 They should identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

8.3 Instruction manuals on the procedures for selling insurance products, customer identification, record-keeping, acceptance and processing of insurance proposals, issue of insurance policies should be set out.

8.4 The following training requirements are considered essential based on the class of employees/Agents:

8.4.1 *New employees:* A general appreciation of the background to money laundering, and the subsequent need for identifying and reporting of any suspicious transactions to the appropriate designated point should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority.

8.4.2 *Front-line staff/Agents*: Members of staff who are dealing directly with the public (whether as member of staff or agents) are the first

point of contact with potential money launderers and their efforts are therefore vital to the strategy in the fight against money laundering. It is vital that "front-line" staff is made aware of the Insurer's policy for dealing with non-regular customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

8.4.3 *Processing staff:* Those members of staff who receive completed proposals and cheques for payment of the premium contribution must receive appropriate training in the processing and verification procedures.

8.4.4 *Administration/Operations Supervisors and Managers*: A high level of awareness program on money-laundering instances and suitable instructions covering all aspects of anti-money laundering procedures should be provided to those responsible persons for supervising or managing front-line staff.

8.4.5 *Ongoing training*: It will also be necessary to make arrangements for refresher training at regular intervals to ensure that employees/ agents are duly updated on their responsibilities. Timing and content of training packages for various levels of employees/ agents will need to be adapted by individual insurers for their own needs.

8.4.6 Records of training imparted to employees/ agents in the various categories detailed above shall be maintained.

9. Internal Control/Audit:

Internal audit/inspection department of insurers shall verify compliance with the extant policies, procedures and controls related to money laundering activities at least on an annual basis. Insurers shall also upgrade its questionnaire and system from time-to-time in accordance with the extant 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.

10. Know Your Customer (KYC) Norms

10.1 What are KYC Norms?

10.1.1 Considering the potential threat of usage of the financial services by a money launderer, insurers should make reasonable efforts to determine the true identity of customer(s).

10.1.2 Effective procedures should be put in place to obtain requisite details for proper identification of new/ existing customer(s). Special care has to be exercised to ensure that the contracts are not under anonymous or fictitious names.

10.1.3 Where a client is a juridical person, insurers shall take steps to identify the client and its beneficial owner(s) and take all reasonable measures to verify his/her identity to their satisfaction so as to establish the beneficial ownership. Procedures for determination of Beneficial Ownership shall be as prescribed in sub rule (3) of Rule 9 of PML Rules.

10.1.4 While implementing the KYC norms on juridical persons, insurers will have to identify and verify their legal status through various documents (indicated, but not limited to, at **Annexure I** of this guidelines), to be collected in support of

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

No reporting entity shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

10.1.5 While implementing the KYC norms on juridical person other than those mentioned in **Annexure I**, insurers shall verify that any person purporting to act on behalf of such client is so authorised and verify the identity of that person.

10.1.6 Where a client is an individual person, insurers shall verify the identity, address and recent photograph in order to comply with provision as specified in Rule 9 (4) of the PML Rules.

A list of documents is to be verified and collected under KYC norms for individuals is given in **Annexure II.**

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

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 insurer.

10.1.7 Insurers may perform KYC process by any of the following methods:

10.1.7.1 Aadhaar based KYC through Online Authentication subject to notification by the Government under section 11A of PMLA

OR

10.1.7.2 Aadhaar based KYC through offline verification

OR

10.1.7.3 Digital KYC as per PML Rules

OR

10.1.7.4 Video Based Identification Process (VBIP) as consent based alternate method of establishing the customer's identity, for customer. The process of VBIP has been specified in **Annexure III**.

OR

10.1.7.5 By using 'KYC identifier' allotted to the client by the CKYCR

OR

10.1.7.6 by using Officially Valid documents

AND

10.1.7.7 PAN/Form 60 (if the premium amount aggregating to more than fifty thousand rupees in a financial year) and any other documents as may be required by the insurer

10.1.8 Customer information should be collected from all relevant sources, including from agents/intermediaries.

10.1.9 Care has to be exercised to avoid unwitting involvement in insuring assets bought out of illegal funds.

10.1.10 It is imperative to ensure that the insurance premium should not be disproportionate to income/ asset.

10.1.11 At any point of time, where insurers are no longer satisfied about the true identity and the transaction made by the customer, a Suspicious Transaction Report (STR) should be filed with Financial Intelligence Unit-India (FIU-IND).

10.2 Client Due Diligence (CDD)

Insurers shall undertake client due diligence (CDD) as per the provisions of Rule 9 of PML Rules. Accordingly, the insurer shall undertake CDD as follows:

10.2.1 Knowing New Customer/ Client

In case of every new contract, necessary Client due diligence with valid KYC documents of the customer/ client shall be done at the time of commencement of account based relationship.

10.2.2 Knowing Existing Customer/Client

The AML/ CFT requirements are applicable for all the existing customers/ clients. Hence, necessary Client due diligence with KYC (as per extant PML Rules) shall be done for the existing customers from time to time basis the adequacy of the data previously obtained or as may be specified by the Authority from time to time.

10.2.3 Ongoing Due Diligence

Besides verification of identity of the customer at the time of initial issuance of contract, Risk Assessment and ongoing due diligence should also be carried out (if so required) at times when additional/ subsequent remittances are made.

Any change which is inconsistent with the normal and expected activity of the customer should attract the attention of the insurers for further ongoing due diligence processes and action as considered necessary.

10.2.4 Verification at the time of payout/claim stage (redemption/ surrender/ partial withdrawal/ maturity/ death etc.)

10.2.4.1 In insurance business, no payments should be allowed to third parties except as provided in the contract or in cases like superannuation/ gratuity accumulations and payments to beneficiaries/ legal heirs/assignees in case of death benefits.

10.2.4.2 Necessary due diligence should be carried out of the policyholders / beneficiaries/ legal heirs/ assignees before making the pay-outs.

10.2.4.3 Free look cancellations need particular attention of the Insurer especially in cases of client indulging in

free look cancellation on more than one occasion at short intervals frequently.

10.2.4.4 Necessary due diligence become more important in case the policy has been assigned by the policyholder to a third party not related to him (except where insurance policy is assigned to Banks/ FIs/ Capital market intermediaries regulated by IRDAI/RBI/ SEBI). Notwithstanding the above, insurers are required to ensure that no vulnerable cases go undetected, especially, where there is suspicion of money- laundering or terrorist financing, or where there are factors to indicate a higher risk, necessary due diligence will have to be carried out on such assignments and STR should be filed with FIU-IND, if necessary.

11. Simplified Due Diligence (SDD):

11.1 Simplified measures as provided under sub clause (d) of clause (1) of Rule 2 of PML Rules are to be applied by the insurer in case of individual policies, where the aggregate insurance premium is not more than Rs 10000/ - per annum.

However, simplified Client Due Diligence measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific higher-risk scenarios apply, based on the Risk Assessment/categorization policy of the insurers.

Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

11.2 The list of simplified due diligence documents are listed in Annexure II.

12. Enhanced Due Diligence (EDD):

12.1 Insurers shall, prior to the commencement of each specified transaction:

12.1.1 Verify the identity of the clients preferably using Aadhaar subject to the consent of customer or;

12.1.2 Verify the client through other modes/ methods of KYC as mentioned above.

12.2 Insurer shall examine the ownership and financial position, including client's source of funds commensurate with the assessed risk of customer and product profile which may include:

12.2.1 Conducting independent enquiries on the details collected on/provided by the customer wherever required,

12.2.2 Consulting a credible database, public or other, etc.,

12.3 Insurers should examine, as far as reasonably possible, the background and purpose of all complex, unusually large specified transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, insurers should be required to conduct enhanced due diligence measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

12.4 Insurer shall not allow the specified transaction to be carried out where the client fails to submit the required details / documents, as required by the Insurers.

12.5 Conducting enhanced due diligence should not be limited to merely documenting income proofs. It would mean having measures and procedures which are more rigorous and robust than that of normal KYC. These measures should be commensurate to the risk. While it is not exhaustive, the following are some of the reasonable measures in carrying out enhanced due diligence:

12.5.1 More frequent review of the customers' profile/transactions

12.5.2 Application of additional measures like gathering information from publicly available sources or otherwise

12.5.3 Review of the proposal/contract by a senior official of the insurers.

12.6 Measures so laid down should be such that it would satisfy competent authorities (regulatory/enforcement authorities), if need be at a future date, that due diligence was in fact observed by the insurers in compliance with the guidelines and the PML Act, based on the assessed risk involved in a transaction/contract.

12.7 Insurers shall increase the future monitoring of the business relationship with the client, including greater scrutiny or transactions where any specified transaction or series of specified transactions undertaken by a client is considered suspicious or likely to involve proceeds of crime.

13. Sharing KYC information with Central KYC Registry(CKYCR)

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

13.2 Where a customer submits a "KYC identifier" for KYC, the Insurers 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 Insurers as per Rule 9(1C) of PML Rules.

However, for the purpose of proper due diligence, Insurers may seek the other necessary documents.

13.3 If KYC is done relying on "KYC identifier" submitted by third party and the Insurer is satisfied with KYC as per Rule 9 of PML Rules, no KYC records requires to be uploaded by the Insurers, unless there is any change in KYC information, provided by the customer.

13.4 If the KYC identifier is not submitted by the client / customer, insurers shall search (with certain credentials) for the same on CKYCR portal and record the KYC identifier of the client/ customer, if available.

13.5 If the KYC identifier is not submitted by the client/customer or not available in the CKYCR portal, insurer shall capture the KYC information in the prescribed KYC Template meant for 'Individuals' or 'Legal Entities', as the case may be.

13.6 Insurers 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.

13.7 Once "KYC Identifier" is generated/ allotted by CKYCR, the Insurers 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.

13.8 The following details need to be uploaded on CKYCR if Verification/Authentication is being done using Aadhaar:

13.8.1 **For online Authentication,**

a. The redacted Aadhar Number (Last four digits)
b. Demographic details
c. The fact that Authentication was done

13.8.2 **For offline Verification**

a. KYC data
b. Redacted Aadhaar number (Last four digits)

13.9 At the time of periodic updation, it is to be ensured that all existing KYC records of individual customers are incrementally uploaded as per the extant CDD standards, by /before the next transaction on to CKYCR. Insurers shall upload the updated KYC data pertaining

to inforce/ paid-up individual policies against which "KYC identifier" are yet to be allotted/ generated by the CKYCR.

13.10 Insurer shall not use the KYC records of the client obtained from Central KYC Records registry for purposes other than verifying the identity or address of the client and should not transfer KYC records or any information contained therein to any third party unless authorised to do so by the client or Insurance Regulatory and Development Authority of India(IRDAI) or by the Director(FIU-IND).

13.11 Insurers shall upload the KYC data pertaining to accounts of legal entities opened on or after April 1, 2021, on to CKYCR in terms of Rule 9 (1A) of the PML Rules.

13.12 Insurers shall also ensure that in case of accounts of legal entities opened prior to April 1, 2021, the KYC records are uploaded on to CKYCR during the process of periodic updation by/ before the next transaction. Insurers shall ensure that during periodic updation, the customers' KYC details are migrated to current Customer Due Diligence (CDD) standards.

14. Reliance on third party KYC:

For the purposes of KYC norms under clause 10, while insurers are ultimately responsible for customer due diligence and undertaking enhanced due diligence measures, as applicable, insurers may rely on a KYC done by a third party subject to the conditions that-

14.1 the Insurer, within two days from the commencement of the account based relationship, obtains valid KYC documents from the third party or the information of the client due diligence carried out by the third party.

However, where the insurer relies on a third party that is part of the same financial group, they should obtain the KYC documents

within fifteen days from the commencement of the account based relationship.

14.2 the Insurer is satisfied that such 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 Act.

14.3 the third party is not based in a country or jurisdiction assessed as high risk.

14.4 the Insurer is ultimately responsible for client due diligence and undertaking enhanced due diligence (if required).

15. Risk Assessment/ Categorization

15.1 Insurers has to carry out "Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise as provided in sub rule (13) of Rule 9 of PML Rules periodically at least once in a year to identify, assess, document and take effective measures to mitigate its money laundering and terrorist financing risk for clients, customers or geographic areas, products, services, services, nature, volume of transactions or delivery channels etc. While assessing the ML/TF risk, the insurers are required to take cognizance of the overall sector specific and country specific vulnerabilities, if any, that the Government of India / IRDAI may share with insurers from time to time. Further, the internal risk assessment carried out by insurer should be commensurate to its size, geographical presence, complexity or activities/ structure etc.

15.2 In the context of the very large base of insurance customers and the significant differences in the extent of risk posed by them, as part of the risk assessment, the insurers shall at a minimum, classify the customer into high risk and low risk, based on the individual's profile and product profile, to decide upon the extent of due diligence.

15.3 The documented risk assessment shall be updated from time to time. The insurers shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be

applied. It shall be made available to competent authorities and law-enforcement agencies, as and when required.

15.4 Risk Categorization

15.4.1 For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and source of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society, government departments and government owned companies, regulators and statutory bodies.

In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Notwithstanding the above, in case of continuing policies, if the situation warrants, as for examples if the customer profile is inconsistent with this investment through top-ups, a re-look on customer profile is to be carried out.

15.4.2 For the high risk profiles, like for customers who are non-residents, high net worth individuals, trusts, charities, NGO's and organizations receiving donations, companies having close family shareholding or beneficial ownership, firms with sleeping partners, politically exposed persons (PEPs), and those with dubious reputation as per available public information who need higher due diligence, KYC and underwriting procedures should ensure higher verification and counter checks.

16. Contracts with Politically Exposed Persons (PEPs)

16.1 Insurers shall devise procedure to ensure that proposals for contracts with high risk customers are concluded only after approval of senior management officials. It is however emphasized that proposals of Politically Exposed Persons (PEPs) (as specified in the AML/CFT Master Circular issued by Reserve Bank of India from time to time) in particular

requires examination by senior management, not below the level of Head (underwriting) /Chief Risk Officer.

16.2 Insurers are directed to lay down appropriate on-going risk management procedures for identifying and applying enhanced due diligence measures on an on-going basis to PEPs and customers who are close relatives of PEPs. These measures are also to be applied to insurance contracts of which a PEP is the ultimate beneficial owner (s).

16.3 If the on-going risk management procedures indicate that the customer or beneficial owner(s) is found to be PEP, or subsequently becomes a PEP, the senior management should be informed on this business relationship and apply enhanced due diligence measures on such relationship.

17. New Business Practices/Developments:

17.1 Insurers shall pay special attention to money laundering threats that may arise from

17.1.1 Development of new products

17.1.2 New business practices including new delivery mechanisms

17.1.3 Use of new or developing technologies for both new and pre-existing products.

17.2 Special attention should especially, be paid to the 'non-face-to-face' business relationships brought into effect through these methods.

17.3 Insurers should lay down systems to prevent the misuse of money laundering framework. Safeguards will have to be built to manage typical risks associated in these methods like the following:

17.3.1 Ease of access to the facility;

17.3.2 Speed of electronic transactions;

17.2.3 Ease of making multiple fictitious applications without incurring extra cost or the risk of detection;

17.4 The extent of verification in respect of such 'non face-to-face' customers will depend on the risk profile of the product and that of the customer.

17.5 Insurers shall have in place procedures to manage specific increased risks associated with such relationships e.g. verification of details of the customer through on-site visits.

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

18.1 Section 51A of the Unlawful Activities (Prevention) Act, 1967(UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated August 27, 2009 detailing the procedure for the implementation of Section 51A of the UAPA

18.2 The insurers should 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.

18.3 Insurers shall periodically check MHA website for updated list of banned entities.

18.4 A list of individuals and entities subject to UN sanction measures under UNSC Resolutions (hereinafter referred to as 'designated individuals/ entities') would be circulated to the insurers through Life/ General Insurance Council, on receipt of the same from the Ministry of External Affairs (MEA). This is in addition to the list of banned entities compiled by Ministry of Home Affairs (MHA) that have been circulated to the insurers till date.

18.5 Insurers shall maintain an updated list of designated individuals/entities in electronic form and run a check on the given parameters on a regular basis to verify whether designated individuals/entities are holding any insurance policies with the insurers. An updated list of individuals and entities which are subject to various sanction measures as approved by Security Council Committee established pursuant to UNSC 1267 can be accessed regularly from the United Nations website at https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_listand

UNSC 1988 can be accessed regularly from the United Nations website at https://www.un.org/securitycouncil/sanctions/1988/materials

18.6 By virtue of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), the Central Government is empowered to freeze, seize or attach funds of and/or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism. [The list is accessible at website http://www.mha.nic.in/BO]. To implement the said section an order reference F. No. 17015/10/2002-IS-VI dated 27th August, 2009 has been issued by the Government of India. The salient aspects of the order with particular reference to insurance sector are provided at **Annexure IV**.

18.7 Shri Prabhat Kumar Maiti, Sectoral Development Department, Insurance Regulatory and Development Authority of India, Sy. No- 115/1, Financial District, Nanakramguda, Gachibowli, Hyderabad-500032; E-mail: prabhat@irdai.gov.in; Telephone: 040 - 20204866; is the UAPA Nodal Officer for the purposes of implementation in the insurance sector.

19. Contracts emanating from countries identified as deficient in AML/CFT regime:

Insurers are required to:

19.1 Conduct enhanced due diligence while taking insurance risk exposure to individuals/entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime.

19.2 Pay Special attention to business relationships and transactions, especially those which do not have apparent economic or visible lawful purpose. In all such cases, the background and purpose of such transactions will as far as possible, have to be examined and written findings have to be maintained for assisting competent authorities.

19.3 Alert Agents/Brokers/ employees appropriately to ensure compliance with this stipulation.

19.4 Go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations while using the FATF Public

Statements, being circulated through the Life/ General Insurance Council.

19.5 Take similar measures on countries considered as high risk from terrorist financing or money laundering perspective based on prior experiences, transaction history or other factors (e.g., legal considerations, or allegations of official corruption).

20. Reporting Obligations:

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

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the Insurers for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

20.2 The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist insurers in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) **(Annexure V)** which FIU-IND has placed on its website shall be made use of by Insurers which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of those insurers, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

20.3 While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule

shall be constituted as a separate violation. Insurers shall not put any restriction on operations in the accounts where an STR has been filed. Insurers shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

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

21. Record Keeping

21.1 In view of Rule 5 of the PML rules, the insurers, its designated director, Principal Officer, employees are required to maintain the information/records of types of all transactions [as mentioned under Rules 3 and 4 of PML Rules 2005] as well as those relating to the verification of identity of clients for a period of five years. The records referred to in the said Rule 3 shall be maintained for a period of five years from the date of transaction. Records pertaining to all other transactions, (for which insurers are obliged to maintain records under other applicable Legislations/Regulations/Rules) insurers are directed to retain records as provided in the said Legislation/Regulations/Rules but not less than for a period of five years from the date of end of the business relationship with the customer.

21.2 Records can be maintained in electronic form and/or physical form. In cases where services offered by a third party service providers are utilized,

21.2.1 Insurers shall be satisfied about the organizational capabilities, and that technology, systems and measures are in place to safeguard the privacy of the data maintained and to prevent unauthorized access, alteration, destruction, disclosure or dissemination of records and data.

21.2.2 The physical or electronic access to the premises, facilities, automatic data processing systems, data storage sites and facilities including back-up sites and facilities and to the

electronic data communication network of the service provider is controlled, monitored and recorded.

21.2.3 The service provider has established standard transmission and encryption formats and non-repudiation safeguards for electronic communication of data.

21.2.4 It should also be ensured that the provisions under the relevant and extant data protection statutes are duly complied with.

21.3 Insurers should implement specific procedures for retaining internal records of transactions both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity. Insurers should retain the records of those contracts, which have been settled by claim or cancelled, for a period of at least five years after that settlement.

21.4 In situations, where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed. Wherever practicable, insurers are required to seek and retain relevant identification documents for all such transactions and report such transactions of suspicious funds.

21.5 In case of customer identification data obtained through the customer due diligence process, account files and business correspondence should be retained (physically or electronically) for at least five years after the business relationship is ended.

21.6 In case of non- availability of KYC of the existing clients as per the extant PML Rules or if the records of the existing client are to be updated to comply with the extant PML Rules, the insurers shall obtain the records by / before the next transaction.

22. Information to be maintained

Insurers are required to maintain and preserve the information as prescribed in Rule 4 of PML Rules in respect of transactions referred in Rule 3 of PML Rules.

23. Sharing of Information:

Insurers shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the insurer and customer. Sharing of information on customers may be permitted amongst organizations such as Income tax authorities, Law Enforcement authorities and such other authorities as required under law or by the order of court.

24. Monitoring of Transactions

24.1 Regular monitoring of transactions is vital for ensuring effectiveness of the AML/CFT procedures. This is possible only if the insurers has an understanding of the normal activity of the client so that it can identify deviations in transactions/ activities.

24.2 Insurers shall pay special attention to all complex large transactions/ patterns which appear to have no economic purpose. The insurers may specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. The background including all documents/ office records/ memorandums/ clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to IRDAI/ FIU-IND/ other relevant Authorities, during audit, inspection or as and when required. These records are required to be maintained and preserved for a period of five years from the date of transaction between the client and insurers.

24.3 The higher authorities of the insurers shall monitor and ensure that Suspicious transactions shall be regularly reported to the Director, FIU-IND.

24.4 Further, the compliance cell of insurers shall randomly examine a sample of transactions undertaken by clients to comment on their nature i.e. whether they are in nature of suspicious transactions or not.

25. Compliance Arrangements:

25.1 AML/CFT Program

25.1.1 In order to discharge the statutory responsibility and to detect possible attempts of money laundering or financing of terrorism, every Insurer need to have a robust AML/CFT program which shall include a Client Due Diligence Program covering all the above aspects.

25.1.2 The Client Due Diligence Program shall include policies, controls and procedures, approved by the senior management, to enable the insurers to manage and mitigate the risk that have been identified either by the insurers or through national risk assessment

25.1.3 The program should have the approval of the board and should be reviewed on a periodic basis and suitable changes (if any) be effected based on experience and to comply with the extant Act / Rules / Regulations.

25.2 Responsibility of insurers:

The guidelines place the responsibility of a robust AML/CFT program on the insurers. Nonetheless, it is necessary that the following steps are taken to strengthen the level of control on the intermediaries/representative of insurer engaged by the insurers:

25.2.1 The list of rules and regulations covering performance of intermediaries /representative of insurer must be put in place. A clause should be added making KYC norms mandatory and specific process document can be included as part of the contracts.

25.2.2 Services of defaulting intermediaries /representative of insurer who expose the insurers to AML/CFT related risks on multiple occasions should be terminated/ blacklisted and the details be reported to IRDAI.

25.2.3 As most part of the insurance business is through intermediaries /representative of insurer,s the selection process of intermediaries /representative of insurer should be monitored religiously in view of set AML/CFT measures.

25.3 Certificate of Compliance:

The insurer shall submit an annual certificate of compliance as prescribed in Annexure VI

26. Exemptions/ Relaxation:

Notwithstanding the standards mentioned for Simplified Due Diligence in Clause 11 of these guidelines, the insurers may exercise different Exemptions/ Relaxations from the stipulated KYC norms in certain conditions, as mentioned below:

26.1 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.

26.2 For continued operation of accounts of existing customers having insurance policy of not more than aggregate premium of Rs. 50,000/- in a financial year, exemption from PAN/Form 60 may be granted till such date as may be notified by the central government.

26.3 Under an Individual Travel Insurance**,** for the 'Policyholder / Insured', KYC may be exempted at the time of commencement of Account based relationship as well as at the time of claim pay out for a value less than Rs. 1,00,000/-.

26.4 Under an Individual Health policies, for the 'Policyholder / Insured' , KYC may be exempted at the time of claim pay out for a value less than Rs. 1,00,000/-.

26.5 Under All kinds of Group Insurance (Life /General/Health) except Group Credit insurance and Government Schemes, for the member beneficiary

/certificate of Insurance (COI) Holders KYC may be exempted at the time of commencement of Account based relationship as well as at the time of claim pay out for a value less than Rs. 1,00,000/-, provided the KYC of Master Policyholders / Juridical Person / Legal Entity and the respective Beneficial Owners (BO) are completed.

However, the above exemptions/relaxations are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific higher-risk scenarios apply, basis the Risk Assessment/categorization policy of the insurers.

27. Repeal Provisions

From the date of coming into force of these guidelines, the instructions / guidelines contained in the circulars mentioned in the Appendix, issued by IRDAI shall stand repealed.

28. Notwithstanding anything contained in this guideline, in case of any issue with respect to interpretation of any provision of this guidelines, the provisions/ directives of the FIU India, the PML Act/Aadhaar Act/Income Tax Act and their rules as amended from time to time, will prevail.

The insurers are also advised to refer to the extant relevant directives, rules, laws and provisions mentioned therein on a regular basis to broadly understand, apply, update their AML /CFT program and implement the provisions of this guideline.

(_____)

Member

Annexure I

List of Documents for KYC purposes

Where the Client is other than individual

Features	Documents
Insurance Contracts with companies	i. Certificate of incorporation ii. Memorandum & Articles of Association iii. Permanent Account Number of the company iv. A resolution of 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 under sub-rule (4) of Rule 9 of extant PML Rules 2005 relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
Insurance Contracts with partnership firms	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) of Rule 9 of extant PML Rules 2005 relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
Insurance Contracts with trusts & foundations	i. Registration Certificate ii. Trust Deed iii. Permanent Account Number or form 60 of the Trust; and iv. Such documents as are required for an individual under sub-rule (4) of Rule 9 of extant PML Rules 2005 relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
Insurance Contracts with Unincorporated association or a body of individuals	i. Resolution of the managing body of such association or body of individuals; ii. Permanent Account Number or Form 60 of the unincorporated

	associations or a body of individuals; iii. Power of attorney granted to him to transact on its behalf; iv. Such documents as are required for an individual under sub-rule (4) of Rule 9 of extant PML Rules 2005 relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf; v. Such information as may be required by the insurers to collectively establish the legal existence of such an association or body of individuals.

Any other Documents that shall be notified by the Central Government, in consultation with the Regulator from time to time.

Annexure II

List of Documents for KYC purposes

Where the Client is an individual

i. Passport

ii. Permanent Account Number or the equivalent e-document thereof or Form No. 60 (mandatory if the premium amount aggregating to more than fifty thousand rupees in a financial year)

iii. Voter's Identity Card issued by Election Commission of India

iv. Driving License

v. Aadhaar number* (**s**ubject to notification under section 11A of PMLA allowing insurers to perform online authentication)/ Proof of possession of Aadhaar (if offline)

vi. Job card issued by NREGA duly signed by an officer of the State Government

vii. Letter issued by the Unique Identification Authority of India or National Population Register containing details of name, address and Aadhaar number.

viii. Any other documents approved by the government from time to time

1. Where simplified measures for due diligence are applied for verifying the identity of the clients the following documents shall 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;

2. In case of officially valid document furnished by the client does not contain updated address, the following documents 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) bank account or Post Office savings account statement;

d) pension or family pension payment orders (PPOs) issued to retired employees by Government Department or Public Sector Undertakings, if they contain the address;
e) letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and licence agreements with such employers allotting official accommodation; and
f) documents issued by Government departments of foreign jurisdiction and letter issued by Foreign Embassy or Mission in India.

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.

*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 insurer.

Annexure III

Video Based Identification Process(VBIP)

Insurers 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 Insurer/authorised person 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 eSign mechanism.

b) The insurer/authorised person 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.

c) 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.

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

e) The authorised person/ Insurer 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.

f) 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.

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

h) Insurers 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. Insurers shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

i) To ensure security, robustness and end to end encryption, the insurers 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.

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

k) Insurers 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 Insurer shall exercise extra caution and the additional necessary details viz. IP address etc. shall be preserved by the insurer to substantiate the evidence at the time of need.

l) Insurers are encouraged 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 insurer.

m) Authorized person of the insurer 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 insurer.

n) Insurer shall maintain the details of the concerned Authorised person, who is facilitating the VBIP.

o) Insurers shall ensure to redact or blackout the Aadhaar number as per extant PML Rules.

p) Insurer will 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 an 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 an 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 IV

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 paras:

i. **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 insurers 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 insurers 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, insurers would 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. Insurers 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 IS-I Division of MHA (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 insurers are the ones listed as designated individuals/entities and the insurance policies, reported by insurers 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 within 24 hours of such verification and conveyed electronically by the Central [designated] Nodal Officer for the UAPA to the concerned office of insurers under intimation to IRDAI and FIU-IND.

f. 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.

ii. 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 insurers.

b. Insurers 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 Nodal Officer of IS-I Division of MHA within two working days.

c. The Additional Secretary (IS-I), MHA, the Nodal Officer for IS-I Division of MHA 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 insurers. However, if it is not possible for any reason to pass an Order unfreezing the assets within 5 working days, the Nodal Officer of IS-I Division shall inform the applicant.

iii. <u>Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001</u>

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 UAPA Nodal Officer for IS-I Division for freezing of funds or other assets.

c. The UAPA Nodal Officer of IS-I Division of MHA, shall cause the request to be examined, within 5 working days, 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 UAPA Nodal Officer of IS-I Division, the request would be forwarded to insurers 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.

iv. <u>Communication of orders under section 51A of UAPA</u>

IRDAI would communicate all Orders under section 51A of UAPA relating to insurance policies, to all the insurers after receipt of the same from IS-I Division of MHA.

v. <u>Exemption in accordance with UNSCR 1452</u>

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 V

Illustrative list of Suspicious Transactions:

1. Customer insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information
2. Frequent free look cancellation by customers;
3. Assignments to unrelated parties without valid consideration;
4. Request for purchase of a policy in amount considered beyond apparent need;
5. Policy from a place where he does not reside or is not employed;
6. Frequent request for change in addresses;
7. 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
8. Overpayment of premiums with a request for a refund of the amount overpaid.
9. Refund of proposal deposit by cancelling the proposal on request of the customer;
10. Media reports about a customer;
11. Information sought by Enforcement agencies;
12. Unusual termination of policies;
13. Borrowing the maximum loan amount against a policy soon after buying it

Note: The list is only illustrative and not exhaustive. Red Flag Indicators issued by FIU-IND also be taken in account for Suspicious Transaction wherever necessary. For more examples on Suspicious Transactions please visit http://fiuindia.gov.in.

Annexure VI

Certificate of compliance (Master Guidelines AML/CFT)

Name of Insurer: _____

Period of Report (FY): _____

We do hereby certify that our company …….. (name)

1)has fully complied with all the norms laid down under Master AML / CFT guidelines 2022, and the company has set up a robust mechanism to comply with the extant PML Rules / Acts.

or

2) has observed the following deviation as per the norms laid down under Master AML / CFT guidelines 2022

[Note: Deviation observed, if any, may be highlighted in the following format]

Sl. No.	**Particulars / Clause of Principles of AML/CFT**	**Nature of Non- compliance (in brief)**	**Reason for non – compliance**	**Corrective Action taken (if any)**

Principal Officer/Chief Compliance Officer
(Name and Signature)

Chief Executive Officer
(Name and Signature)

[**Note**: The insurer should fill up Sl. No. 1 or 2]

Appendix

List of Circulars* (repealed)

Sl. No.	Circular Ref	Date	Contents
1.	IRDA/SDD/GDL/CIR/020/02/ 2013	7th February 2013	AML/CFT (Guidelines for General Insurers)
2.	IRDAI/SDD/GDL/CIR/175/09/ 2015	28th September 2015	Master circular on AML/CFT (Guidelines for Life Insurers)
3.	IRDAI/SDD/MISC/CIR/135/07 /2016	12th July 2016	Operationalisation of Central KYC Record Registry (CKYCR)
4.	IRDAI/SDD/MISC/CIR/248/11 /2017	8th November 2017	The prevention of Money-Laundering (Maintenance of Records) Second Amendment Rules, 2017
5.	IRDAI/SDD/CIR/ MISC/ 267/12/2017	18thDecember 2017	The prevention of Money-Laundering (Maintenance of Records) Seventh Amendment Rules, 2017
6.	IRDAI/SDD /CIR/MISC/047 03/2018	20th March 2018	The prevention of Money-Laundering (Maintenance of Records) Second and Seventh Amendment Rules, 2017
7.	IRDA/SDD/CIR/ MISC/020/01/2019	29th January 2019	Allowing Aadhaar Card as one of the acceptable documents for KYC under certain conditions

8.	IRDA/ SDD / CIR / MISC/245/09/2020	18thSeptember 2020	Video Based Identification Process
9.	IRDAI/SDD/CIR/MISC/016/01 /2021	22nd January 2021	Centralized KYC Registry – Roll out of Legal Entity Template & other changes

* The above circulars have been repealed by this Master Guidelines.