Bajaj Allianz General Insurance Company Limited

Anti-money Laundering & Counter Financing of Terrorism (AML/CFT) Policy

Table of Contents

1. Preamble

Bajaj Allianz General Insurance Company Limited (hereinafter referred to as 'BAGIC' or 'the Company') does not wish to be exploited for money laundering purposes or any kind of financing of terrorist activities. The successful business of Bajaj Allianz General Insurance Company Limited is based on good reputation and integrity. These assets are guided by high standards of customer identification / verification and customer management (jointly "know your customer principle"). BAGIC standards in money laundering prevention are outlined in this Policy.

2. Scope

This Policy applies to the activities of all employees, agents, intermediaries and other contracting parties/vendors of BAGIC.

3. Money Laundering

This Policy is amended and updated in line with the Insurance Regulatory and Development Authority of India (IRDAI) Master Guidelines on Anti-Money Laundering/ Counter Financing of Terrorism (AML/CFT), 2022 vide Master Circular No. IRDAI/IID/GDL/MISC/160/8/2022 dated 1 August 2022 (AML Guidelines).

3.1 What is Money Laundering?

As defined by IRDAI, money laundering is moving illegally acquired cash through financial systems, so that it appears to be legally acquired.

There are perceived to be three common stages of money laundering as detailed below, which are resorted to by the launderers and insurance institutions may unwittingly get exposed to a potential criminal activity while undertaking normal business transactions:

- Placement - the physical disposal of cash proceeds derived from illegal activity,
- 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
- Integration - creating the impression of apparent legitimacy to criminally derived wealth.

If the layering process succeeds, 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. Financial institutions such as BAGIC are therefore placed with a statutory duty to make a disclosure to the authorized officer 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. Such disclosures are protected by law, enabling the person with information to be able to disclose the same without any fear and BAGIC likewise need not fear breaching their duty of confidentiality owed to customers.

3.2 Money Laundering Prevention in BAGIC

BAGIC wishes to comply with high standards of ethics and integrity in relation to its business in addition to complying with the relevant legislation pertaining to prevention of

money laundering activities and counter-financing of terrorist activities. Appropriate measures will be taken when there are reasonable grounds for suspecting money-laundering or terrorism activities.

It is BAGIC's policy to conduct business only with clients and associates who are involved in legitimate activities and to fully comply with all applicable money laundering prevention laws and regulations, including identification, verification, record-keeping and reporting requirements.

4. Principal Officer and Designated Director

In terms of AML Guidelines, a Designated Director and the Principal Officer (PO) are required to be appointed by BAGIC to ensure compliance with the applicable provisions of the said guidelines. For the purpose of this policy, the Designated Director shall be Chief Executive Officer and Managing Director of the Company and Principal Officer shall be Chief Compliance Officer of the Company.

5. Products to be covered

The AML requirements focus on the vulnerability of all the products to any of the process of money laundering as suggested by IRDAI. Reinsurance and Retrocession contracts where the treaties are between insurance companies for reallocation of risks within the insurance industry and do not involve transactions with customers and hence are exempted from the purview of AML requirements. In respect of Group Insurance Policies, KYC requirements apply to the Master Policyholder (MPH) and not at a member level. However, personal details such as Name, Mobile No., Email ID of the group members are required to be maintained by the MPH and made available to BAGIC as and when required.

6. Policies, Procedures and Controls

It is the aim of BAGIC to be prevented from being misused for any kind money laundering purposes. Following procedures are in place to ensure the same:

6.1. Know Your Customer (KYC)

6.1.1 Considering the potential threat of usage of financial services by a money launderer, BAGIC and its employees, agents etc., would exercise special care to determine the true identity of all customers while (at the time of or before) issuing the policies, on an ongoing basis and also at the time of claim settlement through effective procedures for obtaining proof of identification and residence/address, to ensure that the contracts are not anonymous or under fictitious names.

6.1.2 KYC process is initially to be done at the time of establishing an account-based relationship/ client-based relationship and monitor their transactions on-going basis as per the AML Guidelines. Any change in the customers' recorded profile that comes to the notice of the insurer, and which is inconsistent with the normal and expected activity of the customer should attract the attention of the employees, agents etc., for further ongoing KYC processes and action as considered necessary.

6.1.3 BAGIC will take the necessary 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.

6.1.4 Where a client is an individual person, BAGIC will verify the identity, address and recent photograph in order to comply with provision as specified in sub rule (4) of Rule 9 of the PML Rules, including by using end to end Digital KYC mode as allowed under the applicable regulations.

6.1.5 The person who funds / pays for an insurance contract, either as the beneficial owner or otherwise, becomes relevant for the purpose of determining the identity of the "customer" and the term also refers to the proposer / policyholder, beneficiaries and assignees as may be applicable for the purposes of the AML guidelines.

6.1.6 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 Master Policyholders under the group insurance shall maintain the details of all the individual members covered, which shall also be made available to the BAGIC as and when required.

6.1.7 At any point of time, where Principal Officer 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) if it is satisfied that the transaction meets the criteria specified in sub clause (g) of clause (1) of Rule 2 of the PML Rules and any guidelines / indicators issued by IRDAII or FIU-IND.

6.1.8 Methods by which the Company may carry out the KYC verification:

i. Aadhaar based KYC through Online Authentication subject to notification by the Government under section 11A of PMLA, Or
ii. Aadhaar based KYC through offline verification, Or
iii. Digital KYC as per PML Rules, Or
iv. 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 I,** Or
v. By using "KYC identifier" allotted to the client by the CKYCR, Or
vi. By using Officially Valid documents AND PAN/Form 60 (wherever applicable) and any other documents as may be required by the insurer.

6.2. Client Due Diligence/ KYC

6.2.1. Client due diligence with valid KYC documents of the customer/ client shall be done at the time of commencement of account-based relationship subject to clause 6.1.6 above.

6.2.2. 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. In case of non-availability of KYC of the existing clients as per the extant PML Rules, the same

shall be collected within two years for low-risk customers and within one year for high-risk customers. For the purpose of this clause, existing customer shall mean all the customers of the Company having active policy with the Company as on 31 December 2022. However, BAGIC will make all endeavors to educate its customers and complete the customer due diligence for the existing customers in an expeditious manner.

6.2.3. Ongoing Due Diligence: Any change which is inconsistent with the normal and expected activity of the customer shall be reviewed by the Company for further ongoing due diligence processes/ action if deemed necessary.

6.3 KYC at the Claims/Refund stage:

6.3.1. KYC verification also needs to be carried out at the time of claim/refund stage (death/ refunds/reimbursement etc.).

6.3.2. No payments shall be made to third parties except as provided in the contract of insurance or in death cases where the payments are required to be made to beneficiaries/ legal heirs/assignees. Necessary due diligence shall be carried out by BAGIC with respect to such policyholders / beneficiaries/ legal heirs/ assignees before making the payments.

6.3.3. The Company shall take necessary due diligence steps for free look cancellations cases where the client frequently indulges in seeking multiple cancelation requests.

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

6.4.1. The Company shall not enter a contract with a customer whose identity matches with any person in the UN sanction list or with banned entities/designated individuals or entities and those reported to have links with terrorists or terrorist organizations. Designated individuals/ entities shall mean such individuals/entities who are subject to UN sanction measures under UNSC Resolutions.

6.4.2. The Company shall periodically check MHA website for updated list of banned entities.

The alternate procedures for identification of customers and his/her income are detailed in **Annexure II and III.**

7. Risk Assessment/ Categorization

It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction, etc. As such, the Company would apply due diligence measures on each of the customer on a risk sensitive basis. The basic principle enshrined in this approach is that the Company should adopt an enhanced customer due diligence process for higher risk categories of customers.

In the context of our very large base of customers and the significant differences in the extent of risk posed by them, the Company classifies the customers into high risk and low risk. The basis for such a classification is as follows:

7.1 Low risk customers:

Low risk customers would be those individuals and entities whose identities can be easily identified and transactions in whose accounts by and large conform to the known profile. Illustrative examples of low-risk customers are:

- Salaried employees (Private & Public Sector),
- People belonging to lower economic strata of the society (Contract employees, daily wage, factory workers, self-employed persons etc.),
- Corporate Customers (Company registered under the Companies Act, 1956/2013, which includes private, public, one-person company),
- Limited Liability Partnership registered under The Limited Liability Partnership Act, 2008.

For low-risk customers, only the basic requirements of verifying the identity and address proof of the customer shall be required to be met. This will not be acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific high-risk scenarios apply.

7.2 High risk customers:

High risk profile customers are predominantly those types of customers wherein the details required to carry out the due diligence / KYC is not centrally available and / or are not available in the public domain defined as those who are:

- Non-residents, including such individuals/entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime,
- Trusts, charities, NGO's, Societies and organizations receiving donations,
- Foreign Companies originating from Sanction countries having close family shareholding or beneficial ownership,
- Partnership Firms,
- Politically Exposed Persons and
- Those with dubious/negative reputation as per public information available.

For high-risk customer, BAGIC employee shall take necessary steps to examine one or more of the following to carry out the customer's due diligence:

- Background and purpose of the transaction especially those which do not have apparent economic or visible lawful purpose. The Company shall examine and maintain written findings in highly suspicious cases for the purpose of assisting competent authorities,
- Insurable interest,
- Source of premium payment,
- KYC documents as may be available.

7.3 The above-mentioned lists are only illustrative and the person responsible for underwriting / sales should exercise independent judgment to ascertain whether new client should be classified as high-risk customer. In all such cases, higher due diligence will be carried out. Underwriting procedures shall ensure higher

verification and counter checks. BAGIC shall revamp its underwriting system to ensure such due diligence being carried out properly.

7.4 The approval of the senior management officials (i.e. Head of Underwriting / Chief Technical Officer etc) shall be taken to before concluding proposals for contracts with high risk customers.

8. Contracts with Politically Exposed Persons (PEPs)

8.1 The proposals of Politically Exposed Persons (PEPs) in particular require examination by Chief Technical Officer.

8.2 The Company shall 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 where such information is available. These measures are also to be applied to insurance contracts of which a PEP is the ultimate beneficial owner (s).

9. Monitoring and Reporting of Cash Transactions

9.1. Premium / proposal deposit exceeding Rs. 50,000/- should be remitted through cheques, demand drafts, credit card or any other banking channels. Collection of premiums / proposals deposits in cash beyond Rs. 50,000/- per transaction is permitted only subject to the customer quoting the PAN. The Company shall verify the authenticity of PAN of the person or entity funding the premium / proposal deposit on an insurance policy. In case of possible attempts to circumvent the requirements of disclosure of PAN, the same shall be reviewed from the angle to suspicious activities and shall be reported to FIU-India, if required.

9.2. As per the Sec 269ST of the Income Tax 1961, incorporated by the Finance Act 2017, the Company should not accept an amount of Rs. 2 Lacs or more in Cash:

(a) in aggregate from a person in a day; or
(b) in respect of a single transaction; or
(c) in respect of transactions relating to one event or occasion from a person.

9.3. BAGIC has to report integrally connected cash transactions above Rs. 10 Lacs per month to Financial Intelligence Unit-India (FIU-IND) by 15th of next succeeding month. The report will be generated from the system. The format for the report would be as prescribed by IRDAI / FIU–IND from time to time.

10. Monitoring and Reporting of Suspicious Transactions

Suspicious transaction means a transaction whether made in cash which, to a person acting in good faith -

Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or appears to be made in circumstances of unusual or unjustified complexity; or appears to have no economic rationale or bonafide purpose;

All suspicious transactions for AML must be monitored. The Company shall report all suspicious transactions as defined under clause 3.16 of the AML Guidelines irrespective of the monetary value involved in such transactions.

An illustrative list of such transactions as suggested by IRDAI is given below:

- Customer insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information,
- Cash based suspicious transactions for payment of premium over and above Rs. 5,00,000/- (Rupees Five Lakhs only). It should also consider multiple DDs each denominated for less than Rs. 50,000/-,
- Assignments to unrelated parties without valid consideration,
- Request for a purchase of policy in amount considered beyond his apparent need,
- Policy from a place where he does not reside or is employed,
- Unusual terminating of policies and refunds,
- Frequent request for change in addresses,
- 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,
- Overpayment of premiums with a request for a refund of the amount overpaid.

BAGIC has to report the suspicious transactions immediately on identification. When such transactions are identified post facto the contract, it must be reported to FIU-IND within 7 working days of identification in the prescribed formats. The format for the report would be as prescribed by IRDAI / FIU–IND from time to time.

11. Submission of Data on AML/CFT Guidelines

As per revised Master Guidelines on Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT), 2022 dated August 1, 2022, the Company shall submit annual compliance certificate in the prescribe format within 45 days of end of Financial Year.

12. Record Keeping

12.1. As per Rule 5 of the PML rules, BAGIC, its Designated Director, Principal Officer, employees are required to maintain the information/records of types of all transactions as well as those relating to the verification of identity of customer for a period of five years from the date of transaction. Records pertaining to all other transactions, for which BAGIC are obliged to maintain records under other applicable Legislations/Regulations/Rules 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.

12.2. BAGIC will maintain the record in electronic form and/or physical form. In cases where services offered by a third-party service providers are utilized, BAGIC 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, 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.

12.3. Specific procedures for retaining internal records of transactions both domestic and international shall be maintained to comply swiftly with information requests from the competent authorities. Such records shall be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) to provide, if necessary, evidence for prosecution of criminal activity. In the case of long-term insurance, full documentary evidence is usually retained based on material completed at the initiation of the proposal of the contract, together with evidence of processing of the contract up to the point of maturity, for a period of at least five years after that settlement.

12.4. The 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.

12.5. BAGIC shall ensure maintenance of records for the said period as per the prescribed formats and shall furnish the same to the Principal Officer as and when called for by him. BAGIC shall ensure that systems and resources are in place at all times to ensure the same.

12.6. The background including all documents /office records /memorandums pertaining to such transactions, as far as possible, shall be examined by the Principal officer for recording his findings. These records are required to be preserved for ten years (as against the requirement of five years mentioned under the PML guidelines). Directors, officers, and employees (permanent and temporary) are prohibited from disclosing the fact that a Suspicious Transactions Report or related information of a policy holder/prospect is being reported or provided to the FIU-IND.

13. Responsibilities

13.1. Management

13.1.i. BAGIC shall put in place appropriate safeguards suited to its respective business and customers against money laundering and against fraudulent activities to the detriment of the Company. In the event of dubious or unusual practices in the light of past experience or knowledge of money laundering methods, the company shall investigate these in the context of the current business relationship and individual transactions.

13.1.ii. The Management of BAGIC shall make all necessary arrangements to ensure that the organization has a sound and proper money laundering prevention safeguard. The ultimate responsibility for the implementation as well as the functioning and effectiveness of the money laundering prevention safeguards remains with the management even if individual managers have been assigned specific areas of responsibility.

13.1.iii. The Branch Managers/Area Managers/Zonal Managers and Regional Managers are also responsible for and required to ensure that the Board approved AML program is being implemented effectively, including monitoring compliance by the company's insurance agents with their obligations under the program.

13.2. Employees / Agents / Corporate Agents / Contracting Parties/Vendors

13.2.i. It is mandatory for all employees / agents / corporate agents / contracting parties/vendors to follow AML policy and must report violations of this policy / guidelines by another employee / agent / corporate agent / contracting parties/vendors to the Principal Officer. The PO will review such cases. If it is determined that the reported activity involves known or suspected money laundering, other criminal activity, or that the transaction is otherwise suspicious, it will be reported by the PO to the Financial Intelligence Unit-India (FIU-IND) set up by the Government of India for further investigation and action in the form of Suspicious Transaction Reports (STR).

13.2.ii. Initiate appropriate actions against defaulting intermediaries /representative of insurer, who expose the insurers to AML/CFT related risks on multiple occasions and the details would be reported to IRDAI for further action.

13.2.iii. 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.

13.2.iv. Necessary steps will be taken to secure compliance to secure compliance, including when appropriate, terminating the business relationship with such an agent/corporate agent.

14. Recruitment and Training of Employees/Agents/Intermediaries

14.1. The agents / other intermediaries, etc. would be monitored for sales practices followed by Sales Distribution Channels and if any unfair practice is being reported then action would be taken after due investigation.

14.2. Periodic risk management reviews would be conducted to ensure adherence to laid down process and ethical and control environment.

14.3. Adequate screening mechanism as an integral part of BAGIC personnel recruitment/hiring process.

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

14.5. The concept of AML would be part of in-house training curriculum for agents / others.

14.6. The specific document with respect to KYC norms will be included as part of the contracts with agents.

14.7. BAGIC has on-going AML/CFT training programme for all new employee frontline staff, processing staff, administration/operation supervisor and managers, staff dealing with new customers and claims conducted by inhouse training team. The frontline staff is specially trained to handle issues arising from lack of customer education.

14.8. Records of training imparted to staff in the various categories should be maintained by the respective training team.

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

15.1. 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.

15.2. Where a customer submits a “KYC identifier” for KYC, BAGIC 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.

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

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

15.5. Operation team 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) only in case of physical or scanned copy of the documents being submitted and upon duly filled CKYC form received from the customers.

15.6. Once “KYC Identifier” is generated/ allotted by CKYCR, the operation team 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.

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

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

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

15.8. At the time of periodic updation, it is to be ensured that all existing KYC records of individual/legal entity customers are incrementally uploaded as per the extant CDD standards. BAGIC shall upload the updated KYC data pertaining all policies against which “KYC identifier” are yet to be allotted/generated by the CKYCR.

15.9. BAGIC will 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 will

not transfer KYC records or any information contained therein to any third party unless authorised to do so by the client or IRDAII or by the Director (FIU-IND).

16. Internal Control / Audit

Internal Audit Department would verify on a regular basis, compliance with policies, procedures and controls relating 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 extant PMLA and PML Rules. The reports will 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. Exception reporting under AML policy should be done to Audit Committee of the Board.

17. Applicability

The various parts of this policy become applicable as per dates mentioned in various IRDAI Circulars. This policy is as per the extant provisions of applicable laws, rules and regulations. Any changes therein, to the extent applicable, shall be incorporated into this policy.

The said policy is available for the employees ready reference on <<<<<LiNK>>>>

(End of the Policy)

Annexure- I

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 Company official 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 Company may also utilize this facility to verify PAN (wherever applicable). The Company official 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 Company official 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 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 Company official 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 insurer 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 official. 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 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.

m) The Company 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 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 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 - II
Customer Identification Procedure
Any one document to be obtained from Customers

Features	Documents
Insurance Contracts with individuals a) Legal name and any other names used	i. PAN / Form 60 ii. Aadhaar number; iii. Where PAN is not submitted, one certified copy of an Officially Valid Document (OVD) should be submitted iv. Any other document as may be notified by the Central Government in consultation with the Reserve Bank of India v. Any other document as may be required by the banking company or financial institution or intermediary vi. Letter from a recognized public authority or public servant verifying the identity and residence of the customer
b) Proof of Residence	(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; (e) Aadhaar Provided no further documentation is necessary for proof of residence where the document of identity submitted also includes the proof of residence/address.
c) Proof of Identity & Residence both	Other than the above, following could also be treated as valid proofs of identity and residence: i. Written confirmation from the banks where the prospect is a customer, regarding identification and proof of residence. ii. Personal identification and certification of the employees of the insurer for identity of the prospective policyholder. iii. Valid lease agreement along with rent receipt, which is not more than 3 months old as a residence proof. iv. Employer's certificate as a proof of residence. (Certificates of employers who have in place systematic procedures for recruitment along with maintenance of mandatory records of its employees are generally reliable). v. Current Passbook with details of permanent / present residence address (updated up to the previous month) or Current Statement of bank account with details of permanent / present residence address (as downloaded, updated up to the date of submission)

Features	Documents
Insurance Contracts with companies a) Name of the company b) Principal place of business c) Mailing address of the company d) Telephone / Fax Number	i. Certificate of incorporation and Memorandum & Articles of Association ii. Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account iii. Power of Attorney granted to its managers, officers or employees to transact business on its behalf iv. Copy of PAN allotment letter v. and PAN / Form 60 issued to managers, officers or employees holding an attorney to transact on the company's behalf or where an Aadhaar number has not been assigned, proof of application towards enrolment for Aadhaar and in case PAN is not submitted an OVD should be submitted.
Insurance Contracts with partnership firms a) Legal name b) Address c) Names of all partners and their addresses d) Telephone numbers of the firm and partners	i. Registration certificate, if registered ii. Partnership deed iii. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf iv. and PAN / Form 60 issued to the person holding an attorney to transact on its behalf or where Aadhaar number has not been assigned, proof of application towards enrolment for Aadhaar and in case PAN is not submitted an OVD should be submitted.
Insurance Contracts with trusts & foundations a) Names of trustees, settlers beneficiaries and signatories b) Names and addresses of the founder, the managers / directors and the beneficiaries c) Telephone / fax numbers	i. Certificate of registration, if registered ii. Trust Deed iii. Power of Attorney granted to transact business on its behalf iv. Any OVD to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/directors and their addresses v. Resolution of the managing body of the foundation / association vi. and PAN Number or Form 60 issued to the person holding an attorney to transact on its behalf or where Aadhaar number has not been assigned, proof of application towards enrolment for Aadhaar and in case Permanent Account Number is not submitted an OVD

Officially Valid Document (OVD) means Passport, Driving Licence, PAN Card, Voter's Identity Card issued by Election Commission of India, Job Card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number or any other document as notified by the Central Government in consultation with the Regulator, Letter from a recognized public authority or public servant verifying the identity and residence of the customer;

Annexure II of the guidelines for establishment of identity and residence proof may be deemed as illustrative. Documents which are easily obtained in any name like birth certificates, an identity card issued by the employer of the applicant even if bearing a photograph, credit cards, business cards, driving licenses (not bearing a photograph), provisional driving licenses and student union card should not be accepted mechanically, and adequate safeguards should be in place to satisfy its acceptance. In other words, any other document that is accepted by the insurer to establish the identity and proof of residence as required under Rule 9 of the PMLA rules 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 insurer in compliance with the guidelines and the Act.

Annexure - III

Income Proofs

Standard Income proofs:

- Income tax assessment orders/Income Tax Returns
- Employer's Certificate
- Audited Company accounts
- Audited firm accounts and Partnership Deed

Non-standard Income Proofs:

- Chartered Accountant's Certificate
- Agricultural Income Certificate
- Agricultural-land details & Income assessments
- Bank Cash-flows statements, Pass-book

Note: The list is only illustrative and not exhaustive

***

Version 1 approved by the Board of Directors on 5 May 2006
Version 2 approved by the Board of Directors on 27 November 2006
Version 3 approved by the Board of Directors on 25 September 2009
Version 4 approved by the Board of Directors on 12 February 2010
Version 5 approved by the Board of Directors on 31 January 2012
Version 6 approved by the Board of Directors on 10 May 2013
Version 7 approved by the Board of Directors on 16 January 2018
Version 8 approved by the Board of Directors on 16 January 2019
Version 9 approved by the Board of Directors on 14 January 2022
Version 10 approved by the CEO and CFO on 30 December 2022