Bajaj Allianz General Insurance Company Limited

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

Policy and Guideline

Table of Contents

1. Preamble 3
2. Scope 3
3. Money Laundering 3
3.1 What is Money Laundering? 3
3.2 Money Laundering Prevention in BJAZ 3
4. Principal Compliance Officer: 4
5. Products to be covered: 4
6. Policies, Procedures and Controls 4
6.1 Know Your Customer (KYC) 4
6.2 When to KYC 5
6.3 Customer Risk Profile 5
6.4 What to Know and When to Know: 6
6.5 Monitoring and Reporting of Cash Transactions: 7
6.6 Monitoring and Reporting of Suspicious Transactions: 7
7. Record Keeping: 9
8. Responsibilities 9
9 Recruitment, Monitoring and Training of Employees/Agents/Corporate Agents 11
10. Internal Control / Audit: 11
11. Applicability: 12
Annexure I 13
Annexure - II 15
Annexure - III 15

1. Preamble

Bajaj Allianz General Insurance Company Limited (hereinafter referred to as 'BJAZ') does not wish to be abused for money laundering purposes or the 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"). BJAZ standards in money laundering prevention are outlined in the following Policies and Guidelines.

2. Scope

This Policy applies to the activities of all employees, agents, brokers and other independent contractors of BJAZ.

3. Money Laundering

This Policy is introduced considering Insurance Regulatory and Development Authority (IRDA hereinafter) guideline on Anti-Money Laundering issued to all insurance companies vide Master Circular No. 022/IRDA/MasterAML/Nov-08 dated 24th November 2008 [Updated upto 31st July 2010] and the subsequent clarifications / circulars issued.

3.1 What is Money Laundering?

As defined by IRDA, 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 which 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 BJAZ 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 BJAZ likewise need not fear breaching their duty of confidentiality owed to customers.

3.2 **Money Laundering Prevention in BJAZ**

BJAZ 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 BJAZ'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 Compliance Officer:

In terms of IRDA guidelines/rules, the Company Secretary of the Company shall be the Principal Compliance Officer (PCO) for Bajaj Allianz General Insurance Company Limited for compliance of all AML guidelines and for prevention of money laundering and counter-financing terrorist activities. The PCO shall report to the Chief Executive Officer.

5. Products to be covered:

The AML requirements focus on the vulnerability of the products to any of the process of money laundering as suggested by IRDA.

5.1 **Examples of vulnerable products from the angle of AML are as follows:**

5.1.1 Motor policies initiated directly through customers or agents.
5.1.2 Standalone Medical / Health Insurance Products
5.1.3 Fire policies, because it is relatively easy to claim total loss on fictitious assets and convert money showing it as insurance proceeds;
5.1.4 Marine policies, because it is relatively easy to claim total loss on fictitious assets and convert money showing it as insurance proceeds;
5.1.5 Personal accident policies can be misused the same way as life insurance contracts. Non existent persons can be insured and death faked as if caused by an insured event and proceeds can be misappropriated. Similarly, persons can be insured without insurable interest and proceeds of insurance misappropriated either by causing death or faking death;

5.2 As per IRDA guideline for AML, following categories of products / business lines are exempted from the purview of AML requirements:

5.2.1 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;
5.2.2 Group insurance businesses, which are typically issued to a company, financial institution, or association and generally restrict the ability of an individual insured or participant to manipulate its investment.

6. Policies, Procedures and Controls

It is the aim of BJAZ to be prevented from being misused for money laundering purposes.

6.1. Know Your Customer (KYC)

6.1.1 Considering every potential threat of usage of the financial services by a money launderer, BJAZ and its employees, agents etc., would exercise special care to determine the true identity of all customers requesting its services at the time of settlement of their claims through effective procedures for obtaining identification and ensure that the contracts are not anonymous or under fictitious names.

6.1.2 KYC process is initially to be done as per the extant 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 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 for the purposes of the AML guidelines.

6.2. When to KYC

Subject to clause 6.4.2, KYC should be carried out in respect of all policies at the settlement stage and where claims payout / premium refund cross a threshold of Rs.1,00,000/- per claim / premium refund. Special care should also be exercised to ensure that the contracts are not anonymous or under fictitious names.

6.3. Customer Risk Profile

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:

6.3.1 Low risk customers:

Low risk customers would be those individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile. Illustrative examples of low risk customers are:

- 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 etc.

In such cases, only the basic requirements of verifying the identity and location of the customer will be met.

6.3.2 High risk customers:

High risk profile customers are defined as those 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,
-
- Non- face to face customers which includes Tele calling, Internet Marketing, Logging in of business or payment of premiums/lump sums at branches, and
- Those with dubious reputation as per public information available

6.3.3 The above-mentioned list is only illustrative and the person responsible to 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 here higher verification and counter checks. BJAZ shall revamp its underwriting system to ensure such due diligence being carried out properly.

6.3.4 The approval of the senior management officials shall be taken to before concluding proposals for contracts with high risk customers.

6.4. What to Know and When to Know:

6.4.1 Subject to clause 6.4.2 herein below, a mandatory list of documents to be verified in respect of all policies at the settlement stage where claims payout / premium refund cross a threshold of Rs.1,00,000/- is given in **Annexure I and II .** It is mandatory to obtain any one of the documents to clearly establish the customer identity, address and income, consistent with the risk profile.

6.4.2 Provided however it is imperative to ensure that the insurance being purchased is reasonable. Accordingly, customer's source of funds, his estimated net worth etc., should be documented properly and the advisor and/or employee shall obtain income proofs as in Annexure III, to establish his need for insurance cover. Proposal form may also have questionnaires/declarations on sources of fund, and details of bank accounts. Large single premiums should be backed by documentation, to establish source of funds. Therefore, before underwriting, Collection of PAN and Income Proof as per Annexure III are mandatory from all persons purchasing insurance products where the contracted annual premium payable on the insurance policies, per policy basis, is equal to or exceeds Rs. 1.00 lakh. Accordingly clause 6.4.1 shall be read with this clause. Provided further in case of non face to face business which includes Tele calling, Internet Marketing, Logging in of business or payment of premiums/lump sums at branches, collection of documentation be completed for premiums is equal to or exceeds Rs. 1.00 Lakh per person per annum within 15 days of issue of policy. Steps have to be taken to identity the beneficial owner and take all reasonable measures, to verify his/her identity of the beneficial owner. "Beneficial owner" for this purpose means "the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

6.4.3 Document the identity and address of the customer, duly certified by an authorized person as identified by the insurer.

6.4.4 Where a client is a juridical person, verification of identity is required to be carried out on persons purporting to act and is authorized to act on behalf of a client.

6.4.5 In cases detailed KYC needs to be done, customer information will be collected from all relevant sources, including from agents and brokers to know sources of funds, genuineness of transaction, possibility of unaccounted money etc., as per Annexure I and II.

6.4.6 Proposal form may also have questionnaires/declarations on sources of fund.

6.4.7 All payments to be made through account payee cheques.

6.4.8 Large single premium should be backed by documentation to establish the source of funds.

6.4.9 Insurance premium paid by persons other than the person insured shall be looked into to establish insurable interest.

6.4.10 The company shall not enter into a contract with a customer whose identity matches with any person with known criminal background or with banned entities and those reported to have links with banned entities. (As per the guidelines issued by IRDA in March 2006, such entities would be informed by IRDA from time to time) Special attention/care has be paid/taken to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose and transactions as indicated in the Suspicious Transaction Report.

6.5. Monitoring and Reporting of Cash Transactions:

6.5.1 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.

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.

6.5.2 BJAZ 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 IRDA / FIU–IND from time to time.

6.6. Monitoring and Reporting of Suspicious Transactions:

Suspicious transaction means a transaction whether or not 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 3.1.6 of the Guidelines on Anti Money Laundering issued by the Authority irrespective of the monetary value involved in such transactions.

Broad categories of reason for suspicion and examples of suspicious transactions as suggested by FIU-IND are indicated as under:

6.6.1 Identity of client

- False identification documents
- Identification documents which could not be verified within reasonable time

6.6.2 Background of client

- Suspicious background or links with known criminals

6.6.3 Multiple Policies

- Large number of policies having a common policyholder with no rationale

6.6.4 Nature of transactions

- Unusual or unjustified complexity
- No economic rationale or bonafide purpose

- Nature of transactions inconsistent with what would be expected from declared business

6.6.5 Value of transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Value inconsistent with the client's apparent financial standing

An illustrative list of such transactions as suggested by IRDA 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.

Some more examples of suspicious transactions as suggested by IRDA are mentioned in **Annexure - III**.

BJAZ 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 IRDA / FIU–IND from time to time.

6.7. Compliance with Section 51A of UAPA:

By virtue of Section 51A of 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.

Updated list of such persons / entities as per the UNSC Regulation 1267 should be compared with the data of company. Incase any matching records are identified, the operations Team or IT Team or the respective department should inform such cases to Compliance Officer immediately. On receipt of such cases the Compliance Officer should immediately inform such cases to IRDA and such other Regulatory / Law Enforcement Authorities a may be prescribed in the manner as may be prescribed.

The compliance Officer shall also file a Suspicious Transaction Report with FIU-IND in respect of the insurance policies covered above, carried through or attempted, in the prescribed format.

6.8. Submission of Data on AML/CFT Guidelines:

By virtue of IRDA Circular No. IRDA/SDD/GDL/CIR/79/04/2013 dated 22nd April 2013, the Compliance Officer should file the following Forms with IRDA on wuarterly basis within 15 days of end of the quarter:

1. Form 1: Details of Compliance Officer for AML/CFT guidelines in the prescribed formats.
2. Form 3: AML Compliance data in the prescribed formats

7. Record Keeping:

7.1 The Company and its agents are required to maintain the records of types of transactions mentioned under Rule 3 of Prevention of Money Laundering (Maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing information and verification and maintenance of records of the identity of the clients of the banking companies, financial institutions and intermediaries) Rules 2005 and the copies of the Cash / Suspicious Transactions reports submitted to FIU as well as those relating to the verification of identity of clients.

7.2 In case of contracts which have been settled by claim, whether by death, surrender, cancellation, involving an amount equal to or exceeds Rs. 1.00 lakh, such records shall be preserved for 10 years after that settlement.

7.3 In case of customer identification data [as per this policy including KYC documents] obtained through the customer due diligence process, account files and business correspondence should be retained for at least 10 years after the business relationship is ended.

7.4 In situation 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 finally closed and 5 years thereafter. If closing of the case could not be confirmed then till such confirmation and 8 years thereafter. Insurance institutions are requested to seek and retain relevant identification documents for all such transactions and to report the offer of suspicious funds.

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

7.6 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) so as 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.

7.7 The background including all documents /office records /memorandums pertaining to such transactions, as far as possible, shall be examined by the Principal Compliance officer for recording his findings. These records are required to be preserved for ten years. 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.

8. Responsibilities

8.1 Management

8.1.1 BJAZ accepts the responsibility to 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.

8.1.2 The Management of BJAZ accepts the responsibility for the organizational and administrative arrangements to ensure that the organization has a sound and proper money laundering prevention safeguards. 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.

8.1.3 As required under IRDA AML guidelines, the CEO would appoint / re-appoint principal compliance officer for money laundering prevention.

8.1.4 However, the primary responsibility to ensure compliance with the AML policy and guidelines, including the responsibility of maintenance of relevant records (in formats wherever prescribed) for 10 years as required under the IRDA AML Guidelines, shall be with the respective Branch Managers/Area Managers/Zonal Managers and Regional Managers. They shall be required to submit periodic compliance reports and certificates to the Principal Compliance Officer based on which the Principal Compliance Officer shall certify compliance to the management. Internal Audit department may be required to verify such certifications from time to time.

8.1.5 The Branch Managers/Area Managers/Zonal Managers and Regional Managers are also responsible for a 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.

8.2 **Employees / Agents / Corporate Agents / Independent Contractors**

8.2.1 It is mandatory for all employees / agents / corporate agents / independent contractors to follow AML policy and must report violations of this policy / guidelines by another employee / agent / corporate agent / independent contractor to the principal Compliance Officer. The PCO 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 PCO 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).

8.2.2 Services of defaulting employees / agents / corporate agent / independent contractor would be terminated and the details would be reported to IRDA for further action.

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

8.3 **Principal Compliance Officer:**

The Principal Compliance Officer:

8.3.1 Should ensure that the Board approved AML program is being implemented effectively.

8.3.2 Should ensure that the employees and agents of the company have appropriate resources and are well trained to address questions regarding the application of the program in light of specific facts.

8.3.3 Principal Compliance Officer for AML guidelines and staff assisting the Principal Compliance Officer in execution of AML guidelines should have timely access to customer identification data, other KYC information and records

8.3.4 The Principal Compliance Officer for AML guidelines would be at a senior level and preferably not below the Head (Audit/Compliance) /Chief Risk Officer Level and should be able to act independently and report to senior management.

9. Recruitment, Monitoring and Training of Employees/Agents/Intermediaries

9.1 The agents / others 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.

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

9.3 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.

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

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

9.6 The following training requirements are considered essential based on the class of employees.

9.6.1 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 would be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority.

9.6.2 Sales/Advisory staff: Members of staff who are dealing directly with the public (whether as members 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 Company’s policy for dealing with non-regular customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

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

9.6.4 Administration/Operations supervisors and managers: Employees with the responsibility for supervising or managing staff would also be given appropriate training.

9.6.5 Ongoing training: There would be refresher training on a yearly basis to ensure that staff does not forget their responsibilities. A twelve or six-monthly review of training will be done to check if this is being implemented. Timing and content of training packages for various sectors of staff will be adapted.

9.6.6 Records of training imparted to staff in the various categories detailed above should be maintained.

10. Internal Control / Audit:

Internal Audit Department would verify on a regular basis, compliance with policies, procedures and controls relating to money laundering activities. 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.

11. Applicability:

The various parts of this policy become applicable as per dates mentioned in various IRDA 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.

(End of the Policy)

Annexure - I
Customer Identification Procedure
Any one documents to be obtained from Customers

Features	Documents
Insurance Contracts with individuals a) Legal name and any other names used	i. Aadhaar number & PAN / Form 60; ii. Where PAN is not submitted, one certified copy of an Officially Valid Document (OVD) should be submitted iii. Any other document as may be notified by the Central Government in consultation with the Reserve Bank of India iv. Any other document as may be required by the banking company or financial institution or intermediary v. 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 further that updated OVD with current address shall be submitted within a period of three months of submitting the above documents.
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)

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 I 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 - II

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

Annexure - III

Examples/Indicators of Suspicious Transaction:

- Customer insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information
- Cash based suspicious transactions for payment of premium and top ups over and above Rs. 5,00,000/- (Rupees Five Lakhs only) per person per month. It should also consider multiple DDs each denominated for less than Rs. 50,000/- (Rupees Fifty Thousand only)
- Frequent free look surrenders by customers
- Assignment to unrelated parties without valid consideration
- Policy from a place where he does not reside or is employed
- 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
- An established trend or pattern or frequent overpayment of premium with a request for refund of the overpaid amount.
- Frequent Cancelation of policies for the return of premium by an insurer's cheque.

The above indicators are 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 Janaury 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