Bajaj General Insurance Limited
Anti-fraud Policy

1. Introduction

The objectives of the Company's Anti-Fraud Policy is to emphasize the *Management's commitment of zero tolerance to fraud* and to:

- Understand, detect, pre-empt and prevent fraud and take steps to minimize impact of fraud, address the fraud committed in an efficient and effective manner which acts as a deterrent for others
- Define the responsibilities for assessing and addressing fraud risks;
- Define procedures, roles and responsibilities for managing and reporting fraud cases;
- Facilitate the development of controls and mitigation measures, which will aid in the detection and prevention of fraud.
- Detect, monitor and mitigate any fraud and to initiate appropriate remedial and preventive measures.

This Anti-fraud 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 automatically. This Policy draws provisions commensurate with the nature, spread, size and complexity of the Company's business operations, organizational structure of the Company, products sold, business lines composition and overall market conditions prevalent in general. It is the Management's responsibility to amend this Policy as may be required in view of changes in such factors. The Company may implement specific measures for respective lines of business, such as Health, Motor, etc in view of the threats / vulnerabilities of each line of business vary from others.

The Company recognizes the necessity of having a common framework for assessing and addressing the risk of fraud. Fraud ranges from insurance claims fraud, underwriting fraud, fraudulent manipulation of IT-data, to the intentional misstatement of financial data. Fraud may be committed by either internal or external parties. Fraud can be considered as an exceptional event. However, experience has shown that the occurrence of fraud is sometimes indicated by signs of early warning. Therefore, the efficient prevention of fraud requires close cooperation among the Management and the Internal Audit, Compliance & Legal, Human Resources, Corporate Communication and Risk Management functions, which should be achieved by timely exchange of information. This Policy is effective from the year 2013-14 and implemented from the date approval by the Board of Directors.

2. Definition of Fraud

As per section 447 of Companies Act 2013:

i. "Fraud" in relation to affairs of a company or any body corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss;
ii. "Wrongful gain" means the gain by unlawful means of property to which the person gaining is not legally entitled;

iii. “Wrongful loss” means the loss by unlawful means of property to which the person losing is legally entitled.

IRDAI’s Circular on Fraud Monitoring Framework dated 21 January 2013 clarifies that fraud in insurance is an act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties. This may, for example, be achieved by means of:

i. Misappropriating assets;
ii. Deliberately misrepresenting, concealing, suppressing, or not disclosing one or more material facts relevant to financial decision, transaction or perception of the Company’s status; and
iii. Abusing relationship, a position of trust or a fiduciary relationship.

The said Circular has also categorized frauds as:

a) Internal Frauds: Fraud / misappropriation against the Company by its Directors, Managers and/ or any other officers or staff members or employees or ex-employees and vendor associates of the Company by whatever name called
b) Policyholders’ / Claims Frauds : Frauds by policyholders / third parties against the Company in the purchase and/ or execution of an insurance product, including fraud at the time of making a claim
c) Intermediary Frauds: Fraud perpetuated by an Agent Advisor/ Corporate Agent/ Intermediary/ Third Party Administrator (TPAs) against the Company and/ or Policyholders

An illustrative list of frauds is given in Appendix 1 to this Policy. Collusion occurs when internal employees and external parties work together to defraud the Company. Collusion shall be considered as internal fraud.

3. Fraud Monitoring Framework

In response to the growing threat of fraud and vulnerability due to significant size of its operations and the nature of business, the Company should put in place a comprehensive Fraud Monitoring Framework. This framework should recognize fraud risk as part of the key risks and provides for its periodic review by the Management and also by the various review committees such as Management Risk Committee (RiCo), Risk Management Committee of the Board, Audit Committee, etc. However, the Management holds primary responsibility including its applicability, monitoring, reporting and implementing corrective measures.

The framework further provides for dedicated processes and teams of specialists embedded within Investigation and Loss Mitigation (ILM) Team.

The ILM Team shall ensure effective implementation of the Anti-Fraud Policy of the Company and shall also be responsible for the following as part of monitoring framework:

a. Laying down procedures for internal reporting

b. Creating awareness among employees / intermediaries / policyholders to counter insurance frauds,

c. Furnishing various reports on frauds to the regulatory authorities and

d. Furnish periodic reports to the Board of Directors or various committees thereof for their review in order to discharge its responsibilities of companywide monitoring and reporting of frauds.

ILM Team works closely with:

a) Claims departments: Claims units assess the requirement for investigation on a case by case basis for reported claims. The suspected claims are subjected to investigation.
b) Other departments: Such as HR, Underwriting, Internal Audit, Marketing, Risk Management, Operations, etc with an aim to mitigate the underwriting and operational fraud risk at the time of procurement of business and subsequent stages up to claims. Exceptional / suspicious cases identified through various means including analytics, field verifications, etc are also investigated by ILM Team.

4. Area of Application

This Policy should serve all departments as a best practice paper to provide guidance and recommendations in the area of fraud prevention and detection.

5. Approval and Updating

The responsibility for updating the Company's Anti-Fraud Policy rests with the Management of the Company and the same should be approved by the Board of Directors. The Head of Investigation and Loss Mitigation Department is designated as the Anti-fraud Coordinator (AFC).

6. Anti-Fraud Principles within the Company

The Anti-Fraud concept is not a series of instructions or procedures, but is rather a collection of activities which, in the aggregate, form a sound approach for addressing the risk of fraud.

7. Management Accountability

The Management of the Company is responsible for effectively implementing the Company's anti-fraud activities and controls. This is achieved by promoting the importance of internal controls and creating a control-conscious organizational culture, proactively implementing anti-fraud activities and taking consistent and appropriate actions toward remediating deficient controls and addressing internal control violations.

8. Code of Conduct

One of the most important elements of any control environment is "the tone at the top." Therefore, to promote a culture of honesty and ethical behavior, the Company has adopted and implemented a Code of Conduct (CoC) for its employees. The CoC has been communicated to all employees. The Company ensures that the acceptance of the CoC occurs at each level and sufficient training is imparted.

9. Employee Involvement and Whistle-blowing

Employees' awareness of potential fraudulent activities and their commitment to preventing fraud are vital to successful implementation of Anti-fraud Policy. Therefore each employee is responsible for maintaining security over all aspects of his/her work and

to protect the Company's assets, resources and information. Risk of fraud and suspected frauds, as well as violation of rules and regulations, must be brought to the attention of the appropriate level of Management as soon as possible.

Alternatively, if an employee becomes aware of any illegal or questionable activity in the Company, he or she should either inform the Whistle Blowing Committee or any other department (e.g. Internal Audit) that has the competency and objectivity to handle such matters. No employee, who communicates a bona-fide concern, shall be exposed to retaliation based on such communication. Such communication may be made anonymously. In all such cases where any matter has been reported under the said provisions would be investigated and all decisions/actions on such complaints would be reported to the Whistle Blowing committee. While anonymous complaints are allowed, the employees must also note that the repercussions for making frivolous complaints would be very strict. It is the responsibility of the Management to make employees aware of the existence of the Whistle-blowing Policy and its use as well as of other escalation procedures. All the requirements referred to above regarding employee involvement and the Whistle- blowing must be in compliance with existing local laws and regulations and may therefore be amended accordingly.

10. Due Diligence Procedures

Due Diligence is a process of verifying the background and credentials of the personnel, agents, intermediaries, TPAs, vendors, suppliers, lawyers, investigators, hospitals, garages, e-commerce websites and other online market places and other third parties with whom the Company deals.

The Company has laid down the following procedures for conducting due diligence:

1. **Employees:** Employee background verification is conducted by Human Resources department, which would include checking the background (professional and educational) of the new hires. At minimum, the Company must have Aadhaar number and PAN of every employee, updated local and permanent addresses and proofs, contact details of family members (spouse / parents / siblings or a reference person in absence of all these family members)
2. **Agents**: Agent background verification is conducted through reference checks and Know Your Customer (KYC) checks by the Agency Team before their appointment.
3. **Intermediaries**: Due Diligence for Corporate Agents and Intermediaries is conducted by the concerned department / vertical before entering into agreements with them.
4. **TPAs**: Due Diligence for TPA is conducted by the HAT before entering into agreements with them.
5. In case of all other engagements, the concerned departmental head should be responsible for due diligence of the business partners.

As an organization, the Company has three lines of defense, wherein the line function is the first line of defense. Risk Management, Legal and Compliance, Internal Auditor and ILM are the second line of defense and external auditors are the third line of defense for the organization.

11. Regular Communication Channels

The Company should generate fraud mitigation communication internally at periodic intervals and / or ad-hoc basis, communicating this Policy to all concerned. A strong

whistle blower framework is crucial for this purpose. The Company shall also formalize the information flow amongst the various departments and functions for exchange of information.

12. Identification and Detection

Fraud identification and detection includes a combination of the following techniques:

a) Department wise anti-fraud procedures are embedded into processes such as:

- Segregation of duties;
- System access controls – access rights restricted as per job responsibilities;
- Quality checks;
- Scrutiny of application / proposal forms;
- Delegation of authority matrix;

b) Customer Complaint Management System – Centralized system for logging and tracking policyholder grievances (received through letters, online, on call or email) for monitoring market conduct issues, etc. The team handling customer complaints should be trained to direct the relevant complaints to the ILM Team when there is need of such investigation. E.g. when a customer alleges that a surveyor has asked bribe to settle the claim, the customer care executive should direct that compliant to the ILM Team for investigation instead of the claims department for redressal. The Company also has a Whistleblower Policy which aims to provide employees an avenue to raise concerns regarding violation of Code of Conduct and instances of non-compliance to policies and procedures, laws and regulations, frauds, etc.

c) Offsite Monitoring / Surveillance: Under the Fraud Monitoring Framework, data-mining procedures using analytical techniques on an ad-hoc, repetitive or continuous basis will be part of the surveillance conducted. It is particularly useful for analyzing operational and transactional information to highlight anomalies or identify fraud 'Red-Flags'. Information derived from data mining is acted upon and reviewed by ILM Team. Mystery shopping as a tool is proactively used to identify and detect frauds. The list above is illustrative only, not exhaustive.

d) Industry Collaboration: ILM Team is a part of strong group of anti-fraud professionals of other market participants across the general insurance industry. The purpose of such group is to share negative experiences of their own company with peers so as to blacklist the fraudsters in the general insurance industry, thus preventing the fraudulent elements from spreading. The information may be shared including name of customers, agents, employees, vendors, websites, e-commerce groups, their contract details, etc. The ILM Team should participate in all initiatives taken at industry level including by the GIC, IIB, IRDAI, etc.

13. Investigation

The Company must investigate any possible fraudulent activity thoroughly, assess the facts of the case and related internal controls and then decide on appropriate and consistent measures. These may range from internal disciplinary actions to criminal prosecution. The Company has a well-documented internal investigation process, with clear responsibilities, for the handling of fraud-related issues. For this purpose an "Investigation Procedures Manual" has also been prepared. Results of these investigations should be communicated to the appropriate Committees as mentioned above. All parties in receipt of information relating to fraud must treat this in a confidential manner. All employees who suspect fraudulent activities must not attempt to personally conduct any investigation. Appropriate care must be taken to avoid false accusations or alerting suspected individuals that an investigation is underway.

Detailed process for investigation is set out in the Appendix 2 of this note.

ILM Team is responsible to ensure:

a) Utmost confidentiality is maintained of the person reporting the incident in good faith.
b) Information relating to investigation is shared strictly on 'need to know' basis.
c) Reported cases are investigated within least possible time and reports issued accordingly.
d) To abstain from any conflict of interest

Members of the ILM Team are empowered to:

a) Have free and unrestricted access to the Company's records and premises
b) Obtain full co-operation from any employee or associate of the Company
c) Obtain written and / or oral statements from persons they may deem fit, provided such enquiries are under the scope of current investigation
d) Examine, copy, and / or seize / obtain all or any portion of the contents of files, desks, cabinets and other storage facilities including personal items linked to the fraud on the premises without prior knowledge or consent of any individual who may use or have custody of any such items or facilities when it is within the scope and subject of their investigation.

The ILM Team, while carrying out investigation of any employee, is required to keep the HR Team informed about the same.

All the relevant evidences obtained during the course of investigation must be preserved as the same may be required to support legal proceedings. Responsibility of care and custody of all such items rests with the ILM Team.

Where legally required by law enforcement and regulatory bodies or government agencies, Management is to ensure that all cases of fraud or malpractice are adequately reported.

14. Risk Assessment

Each functional department must identify and assess its specific fraud risks, which may differ depending on the market scenario, the structure of the department organization and its processes. This assessment must include the potential for fraudulent financial and non-financial reporting, misappropriation of assets and unauthorized or improper receipts and expenditures. The Risk Management team of the Company should conduct the fraud risk assessment for each department /function and guide them in terms of identification of

potential fraud risk areas and processes, quantification of such risks and drawing mitigation measures for the same. The fraud risk assessment by the Risk Management team should be done at least once in a year and will be shared with the Anti-Fraud Coordinator.

Because of the importance of information technology for all business processes, special consideration should be given to the security of the IT environment. Therefore, the risk assessment of each function / department should place special emphasis on IT security controls. The additional risks posed by such dependence and weaknesses that may develop in our IT Systems should be considered while designing the systems as well as while making any changes therein.

When assessing fraud risks, the following should be considered among other factors:

- Possible exposure or value at risk within a process / product
- State of the implemented controls
- Vulnerability of a process to the Management override and potential schemes to circumvent existing control activities
- Potential for fraudulent financial and non-financial reporting, misappropriation of assets and unauthorized or improper receipts and expenditures
- Motives and possible schemes

15. Control Activities

Based on the risk assessment performed for each function / process / department, the Anti-fraud Coordinator should recommend appropriate fraud risk controls and procedures and implement mitigation measures in consultation with respective Heads of Departments to effectively prevent and detect fraud. Emphasis should be placed on prevention and deterrence measures. These control activities may include, but not limited to:

- Safeguarding of assets
- Segregation of duties
- “Four-eye” Principle (i.e. review procedures)
- Approval and authorization
- Verification and reconciliation

Financial controls for areas with a potentially higher risk (e.g. estimates, revenue recognition, non-standard journal entries and manual journal entries), as well as controls over the financial reporting process, and the possibility of management override, should be included.

16. Communication of Fraudulent Activities

When fraudulent incidences are identified, usually, the employee’s first point of contact is their superior (hierarchical escalation). However, as mentioned above, there are alternative means of escalation (e.g. Whistle-blowing and the reporting to Internal Audit / Corporate Legal & Compliance). The Internal Audit and Legal departments should coordinate appropriate measures and inform top Management, as well as law enforcement authorities, if necessary.

Within each department, information concerning potential fraudulent activities and actual fraud cases should be collected and evaluated. A regular reporting to the Audit Committee of the Board of Directors of significant fraud cases should be established.

17. Monitoring Process

While it is the Management's responsibility to continuously ensure that the implemented anti-fraud controls are sufficient and operate effectively, the ILM Team should monitor the frauds and shall be responsible for effective implementation of this Policy. In all cases of organizational and process changes, the implemented fraud controls should be re-evaluated in case of each impact / change therein. An important part of the regular supervisory activities of the Management is the evaluation of proper working of implemented anti-fraud controls. Significant deficiencies and material weaknesses in internal controls, which are discovered either as part of the Management's assessment of the internal control system or through issues reported by internal or external auditors, should be evaluated for possible fraud exposures and detailed action plans should be implemented.

18. Preventive Mechanism

The Company invests considerable efforts into prevention / mitigation measures such as:

a. Training and Awareness
   - Training and awareness on internal controls, fraud detection and prevention is conducted by the ILM Team in coordination with the HR department through various training programs and communications.
   - Advisories on emerging fraud risks are published by the ILM Team through various communications based on their learning
   - Classroom sessions on Do's and Dont's to mitigate the risk of fraud for the sales team is conducted by ILM Team
   - Training on compliance and regulatory framework (including Anti Money Laundering) is done by Compliance function for employees and by the Agency Training Team for agents to cover employees / agents.

b. The Company shall inform potential and existing clients about the anti-fraud policy of the Company. Necessary caution should be appropriately included in the insurance contracts, duly highlighting the consequences of submitting a false statement and/or incomplete statement.

19. Role of Internal Audit

The Investigation and Loss Mitigation department is the eyes and ears of the entire Company as far as its anti-fraud stand and policy implementation is concerned. The assessment of the Internal Control System is one of the fundamental tasks of the Investigation and Loss Mitigation department. Beginning with the risk assessment of audit topics to the performance of regular audits and special investigations, fraud risks are considered in various aspects of audit work.

20. Role of Legal department.

The legal department should help in assessing (wherever possible based on available data) legal risks involved because of the fraudulent activity. The department would also suggest legal action against the persons involved and also help in completing legal formalities with the concerned department.

21. Documentation / Local Implementation

Each functional department should take this Anti-Fraud Policy as a benchmark to implement anti fraud procedures.

Appendix 1: Illustrative Examples of Fraud

Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

1. **Internal Frauds:**
   a) Misappropriating funds
   b) Fraudulent financial and non-financial information reporting
   c) Stealing cheques
   d) Overriding decline decisions so as to open accounts for family and friends
   e) Inflating expenses claims / over billing
   f) Paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
   g) Permitting special prices or privileges to customers, or granting business to favoured suppliers, for kickbacks/favours
   h) Forging signatures
   i) Removing money from customer, agent or other unclaimed accounts
   j) Falsifying documents
   k) Selling Company's assets at below their true value in return for payment.

2. **Policyholder Frauds and Claims Frauds:**
   a) Exaggerating damages / loss
   b) Staging the occurrence of incidents
   c) Reporting and claiming of fictitious damage / loss
   d) Medical claims fraud
   e) Fraudulent Death Claims
   f) Obtaining a policy on a predeceased person

3. **Intermediary frauds:**
   a) Premium diversion-intermediary takes the premium from the purchaser and does not pass it to the insurer
   b) Inflates the premium, passing on the correct amount to the insurer and keeping the difference
   c) Non-disclosure or misrepresentation of the risk to reduce premiums
   d) Commission fraud - insuring non-existent policyholders while paying a first premium to the insurer, collecting commission and annulling the insurance by ceasing further premium payments
   e) Submitting fictitious KYC documents and bank account details in the name of fictitious persons
   f) Unauthorized use of company logo, printing / use of company letter heads and other intellectual property of the Company

Appendix 2: Process of investigation

----------End of Document----------

Version 1 approved by the Board of Directors on 10 May 2013
Version 2 approved by the Board of Directors on 16 January 2018
Version 3 approved by the Board of Directors on 17 July 2020