Bajaj General Insurance Limited

Anti-Fraud Policy

1. Introduction

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

- To establish a comprehensive framework in order to deter, prevent, detect, report and remedy fraud risks effectively pertaining to the Company and protect the interests of the Policyholders.
- 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 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 Fraud Monitoring Committee'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 co-operation among Management, the Fraud Monitoring Committee and the Internal Audit, Compliance & Legal, Human Resources, Corporate Communication and Risk Management functions, which should be achieved by timely exchange of information.

2. Definition of Fraud

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; The definition of Fraud shall also include the meaning assigned to the term "insurance fraud" under the IRDAI (Insurance Fraud

Monitoring Framework) Guidelines 2025 ("the Guidelines"), which is defined to mean an act or omission intended to gain advantage through dishonest or unlawful means, for a party committing the fraud or for other related parties; including but not limited to:

a. Misappropriating funds;
b. Deliberately misrepresenting/concealing/not disclosing one or more material facts relevant to any decision / transaction, financial or otherwise
c. Abusing responsibility, position of trust or a fiduciary relationship.

ii. Wrongful gain for the purposes of above definition shall mean the gain by unlawful means of property to which the person gaining is not legally entitled;
iii. Wrongful loss for the purposes of above definition shallmean the loss by unlawful means of property to which the person losing is legally entitled.

The said Guidelines have also categorized frauds as under:

a) Internal Fraud: Fraud involving internal staff, including employees and/or senior management.
b) Distribution Channel Fraud: Fraud involving distribution channels.
c) Policyholder Fraud and/or Claims Fraud: Fraud involving any person(s), in obtaining coverage or payment during the purchase, servicing, or claim of an insurance policy.
d) External Fraud: Fraud involving external parties' / service providers / vendors etc.
e) Affinity Fraud or Complex Fraud: Fraud involving collusion among one or more fraud perpetrators in the above categories.

An illustrative list of frauds is given in **Annexure 1** to this Policy.

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, as per the Guidelines, the, Company is required to 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 including the Fraud Monitoring Committee, Executive Risk Management Committee Risk Management Committee of the Board, Audit Committee, etc. However, the Fraud Monitoring Committee holds primary responsibility including its applicability, monitoring, reporting and implementing corrective measures. The Risk Management Committee (RMC) of the Company shall be responsible for effective implementation and oversight of the fraud risk management framework. The Fraud Risk Management Framework shall be calibrated to the Company's specific business, considering the nature of business, size, risk profile, overall business strategy, products, distribution channels, technology infrastructure, and other applicable parameters.

The framework further provides for setting up dedicated processes and team of specialists who would constitute Fraud Monitoring Unit of the Company as prescribed under the said Guidelines, which role is entrusted to the Investigation and Loss Mitigation (ILM) Team of the Company.

In order to discharge its responsibilities of companywide monitoring and reporting of frauds, ILM works closely with:

a) Claims Investigation Unit: Claims unit assesses the requirement for investigation on a case-by-case basis for reported claims. The suspected claims are subjected to investigation and, based on incriminating evidences so procured, the claims are repudiated.

b) Underwriting Unit: Underwriting function aims to mitigate the underwriting and operational fraud risk at the time of policy issuance. The unit identifies exceptional/ suspicious cases through back end analytics and for suspicious transactions performs further checks including field verifications.
c) Analytics Team: High Risk cases identified by Analytics team are sent to ILM for investigations
d) Grievance Redressal Team: Complaints from customers on fraud are sent to FPU for investigation
e) HR team: Drive consequence action process on the employees in proven Fraud cases; and Other relevant functions.

3.1 Fraud Monitoring Committee

3.1.1 Pursuant to Clause 5.3.2 of the Guidelines, the Company shall establish:

a) A Fraud Monitoring Committee (FMC) which shall be responsible for operationalizing the Fraud Risk Management framework of the Company and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.

b) a Fraud Monitoring Unit (FMU), independent from internal audit, to support FMC in discharging its functions and effective implementation of measures suggested by FMC. The ILM team of the Company would be the Fraud Monitoring Unit for the purposes of this Policy.

3.1.2 **Composition of the FMC:** The FMC: -

a) FMC constitutes following senior members/KMPs as part of the Committee:
   1. Chief Financial Officer as the KMP and who would also be the Chairperson of the FMC
   2. Chief Human Resources Officer
   3. Chief Risk Officer
   4. Chief Compliance Officer
   5. Head – Corporate Legal and Company Secretary
   6. Head – ILM.
b) may form subcommittees, as required, for its effective functioning.
c) shall avoid conflicts of interest in its composition and functioning.

3.1.3 **Functions of the FMC:** The FMC shall, inter alia

a) recommend and regularly update, based on experiences, appropriate measures on fraud risk management to various functions.
b) oversee prompt responses to instances or suspicions of fraud
c) maintain all relevant details pertaining to each instance of fraud
d) facilitate collaboration with industry peers / bodies, law enforcement agencies and regulatory bodies to pursue cases of fraud and share information / intelligence on known fraud schemes and perpetrators.
e) conduct an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines and activities for fraud, using past experiences, emerging trends & Red Flag Indicators (RFIs), etc.
f) identify areas for improvement and adaptation of the Fraud Risk Management Framework.

3.1.4 **Reporting Requirements**: The FMC shall: -

a) submit quarterly reports to the RMC on its activities, findings, and recommendations including the financial impact of fraud on the insurer.
b) submit report of the Annual Comprehensive Fraud Risk Assessment before the Board of Directors through RMC.
c) report to the Audit Committee, in addition to the RMC, in case of all internal frauds.

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 based on the recommendation of the FMC and RMC. 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 shall also be equal responsible for effective implementation of this Policy. .

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 / Off roll resources / vendors Involvement and Whistle-blowing

Employee / Off roll resources / vendors 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 / Off roll resources / vendors 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 by checking the background (professional and educational) of the new hires as applicable.
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 Health Administration Team before entering into agreements with them.
5. **Vendors**: Due Diligence for vendors (covered under IRDAI's Outsourcing Regulations) is conducted by Procurement as per the Procurement Policy before entering into agreements with them.

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 for unethical favour 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 Indicators'.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.

d) Cyber or New Age Fraud means any insurance fraud carried out using digital or new age technologies.

In order to prevent Cyber or New Age fraud, Company will inter alia ensure as under:

a) establish and implement robust cybersecurity framework to protect against evolving cyber frauds or threats.
b) continuously monitor and strengthen systems and processes for fraud risk management, such as, incident databases, customer verification and access control
c) utilize a team with relevant risk and technological expertise to manage cyber fraud risks across various insurance business lines.

e) 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.

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 FMC shall conduct an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines and activities for fraud, using past experiences, emerging trends and Red Flag Indicators (RFIs). The FMU shall identify and maintain RFIs based on its lines of business, activities, past experience and trends, incorporate them into operations, and review them regularly for continued relevance and effectiveness. RFI Framework is mentioned in **Annexure 2** of the Policy. The FMC shall also periodically review such RFIs.

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 FMC’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 FMC 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 FMC'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. Training, Education and Awareness

Training, education, and awareness are vital for strengthening fraud prevention efforts. In this regard, The Company shall conduct:

18.1 regular fraud awareness programs to educate policyholders and the general public about the risk of fraud and how to prevent and protect against it.
18.2 periodic training programs, as appropriate:
18.2.1 to the functions being carried out for the employees and the senior management including the board members.
18.2.2 to distribution channels on fraud risk management.

19. Internal Audit

ILM team shall be independent from internal audit, to support FMC in discharging its functions and effective implementation of measures suggested by FMC.

20. Documentation / Local Implementation

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

21. Reporting

The Company shall report incidents of fraud to Law Enforcement Agencies and / or other relevant agencies subject to applicable laws. The Company shall file annual returns with Authority in forms FMR-1 as prescribed under the guidelines, within 30 days of close of the financial year.

22. Insurance Information Bureau (IIB)

In order to ensure that the data available with insurers is effectively utilized to prevent frauds in insurance sector, the Company will participate in the Fraud Monitoring Technology Framework, as applicable to its businesses, made available by the IIB, to help the industry to combat fraud and protect policyholders and all stakeholders.

The IIB shall, through the industry-wide database, facilitate timely threat intelligence sharing on attempted, suspected and reported fraudulent activities within the insurance industry. For the platform to be effective, suitable mechanism for identifying policyholders irrespective of insurer, such as a unique identifier, shall be adopted.

The Company shall share to IIB the details of distribution channels, hospitals, third party vendors and fraud perpetrators blacklisted and IIB shall maintain the caution repository concerning all such details in order to safeguard the integrity of the insurance sector by preventing the involvement of those with a record of fraudulent activities.

IIB, in joint consultation with the Life insurance council and General Insurance council, shall adopt unique identifiers, procedure and timelines for reporting necessary details for caution repository to be maintained.

***

Annexure 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
      Unauthorized use of company logo, printing / use of company letter heads and other intellectual property of the Company

4. **Intermediary frauds:**
   a) Fake Policy
   b) Stolen Identities
   c) Cyber Frauds
   d) Phishing Scams
   e)
5. **Complex/Affinity fraud :**
   a) Staged Motor Accidents with Collusion

b) Medical/Health Insurance Fraud Rings
c) Ghost Policies & Premium Diversion
d) Organized Theft & False Claims
e) Multiple Claims Across Insurers

Annexure 2: illustrative list of Red Flag Indicators

Sr.No	Red Flag Indicators
1.	Backdation
2.	Channel based Triggers
3.	Contridictory Information
4.	Customer behavior
5.	Deceased based Triggers
6.	Delayed reporting
7.	High value Triggers
8.	Hospital based Triggers
9.	ICD based
10.	Inflation based Triggers
11.	Insured Related Triggers
12.	Intermediary related Triggers
13.	Location Based triggers
14.	Odd hours Trigger
15.	Pharmacy based Triggers
16.	Product based Triggers
17.	Profile based Triggers
18.	Profitability based triggers
19.	Proximity based Triggers
20.	Repeated Incidences
21.	Rollover triggers
22.	Scoring based Triggers
23.	Backdation