

Magma General Insurance Limited

To set forth a fraud monitoring framework to enforce policies, procedures and controls to aid prevent, detect, monitor and mitigate the risk of fraud in the company

Anti-Fraud Policy

Effective Date: 1st April 2026

Approval Date: 10th February 2026

Version No. 11

Approved By: Board of Directors

Policy Owner: Chief Risk Officer

This document is confidential in nature and supersedes any Anti-Fraud Policy existing in the Company and should be read in conjunction with the most recent policies and procedures documented and held on file.

Subject:	Original Issue Date: 26.04.2013	Effective Date: 01.04.2026
Anti-Fraud Policy	Revision Dates: 24.10.2013, 04.05.2017, 27.07.2018, 18.07.2019, 24.07.2020, 21.10.2021, 09.11.2022, 01.11.2023, 24.10.2024, 21.07.2025, 10.02.2026	Policy No: 11

Governing Guideline Policy	:	IRDAI Circular No. IRDAI/IID/GDL/MISC/112/10/2025 dated 09th October 2025
Initial Document Prepared by	:	Umesh Chaudhary
Functional aspects Checked by	:	Manish Mhadgut

Contents

1. Purpose of this document 4

2. Scope of Policy 4

3. Definition and Classification of Insurance Fraud 4

4. Purview of the Policy 6

5. Reporting of Fraud 17

6. Confidentiality 17

7. Administration of the Policy 18

8. Conclusion 18

1. Purpose of this document

This Anti-Fraud policy has been created to support Magma General Insurance Limited (hereinafter Magma or the Company) in its commitment to protecting its reputation, revenues, assets, and information from any attempts of fraud, deceit or other improper conduct by employees, policyholders, claimants, intermediaries or any other third parties.

This document sets forth a fraud monitoring framework to enforce policies, procedures, and controls to aid prevent, detect, monitor, and mitigate the risk of fraud in Magma.

The intent of the policy is to promote consistent legal and ethical organizational behavior by assigning responsibility for the development of controls, and providing guidelines for reporting, conduct of investigation and undertaking corrective action in respect of any suspected fraudulent behavior or fraud. The Company will also endeavor to work towards creating deterrents to prevent or mitigate frauds on the Company by suitably working with law enforcement agencies.

This Anti-Fraud Policy is intended to supplement all applicable laws, rules and regulations and other corporate policies, including the code of business conduct and ethics.

2. Scope of Policy

This policy applies to any fraud or suspected fraud in Magma, involving employees (including contractual employees), policyholders / their nominees, insurance agents / Corporate agents / intermediaries as well as consultants, vendors, suppliers, service providers, contractors, outside agencies and / or any other parties with a business relationship with Magma.

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/ title, or relationship with Magma.

3. Definition and Classification of Insurance Fraud

(a) "Insurance Fraud" (hereinafter referred to as 'Fraud') shall 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:

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

There can be different forms of fraud. It may be a simple act involving one person or it may be complex operation involving a large number of people from within and outside the company.

In order to adequately protect itself from the financial and reputational risks posed by insurance frauds, Magma has put in place through this policy a framework to detect, monitor and mitigate occurrence of such insurance frauds within the Company. This framework includes measures to protect the insurer from the threats posed by the following broad categories of frauds:

3.1. Classification of Frauds

Every insurer shall establish appropriate systems and processes across its functions to deter, prevent, detect, report and remedy frauds; and report such frauds according to the following categories:

- a) **Internal fraud:** Fraud / misappropriation against the insurer by its Director, Manager and /or any other office or staff member (by whatever name called) on his/her own or in collusion with others who are either internal or external to the insurer.
- b) **Distribution Channel Fraud:** Fraudulent activities involving insurance distribution channels such as agents, corporate agents, or intermediaries. These frauds typically occur during the sale or servicing of insurance policies and may include acts like premium diversion, inflating premiums, misrepresentation of risk, commission fraud, collusion etc with policyholders to commit claims fraud.
- c) **Policyholder fraud and/or Claims Fraud:** Fraud against the insurer in the purchase, servicing and/or execution of an insurance product, including fraud at the time of making a claim by one person or people in collusion by obtaining wrongful coverage or payment.
- d) **External Fraud:** Fraudulent activities involving external parties such as service providers, vendors, suppliers or other third parties.
- e) **Affinity Fraud or Complex Fraud:** Fraudulent activities involving collusion among one or more fraud perpetrators across different categories (such as internal, external, policyholder, or distribution channel fraud). They often exploit trust within groups or networks to commit large-scale or sophisticated frauds. (Fraud involving collusion among one or more fraud perpetrators in the above categories)

Red Flag Indicator or RFI means a possible warning sign, that points to a potential fraud and may require further investigation or analysis of a fact, event, statement, or claim, either alone or with other indicators.

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

Distribution Channels shall have the same meaning assigned to it under sub clause (8) of clause 5 of IRDAI (Protection of Policyholders' Interests and Allied Matters of Insurers) Regulations, 2024.

Appendix I provides an illustrative list of actions which can be considered as Insurance frauds/red flag indicators. These instances include frauds perpetuated internally; by insurance agent/Corporate Agent/intermediary/TPAs; and instances of claims / policyholder frauds.

*Source: IRDAI circular on Insurance Fraud Monitoring Framework

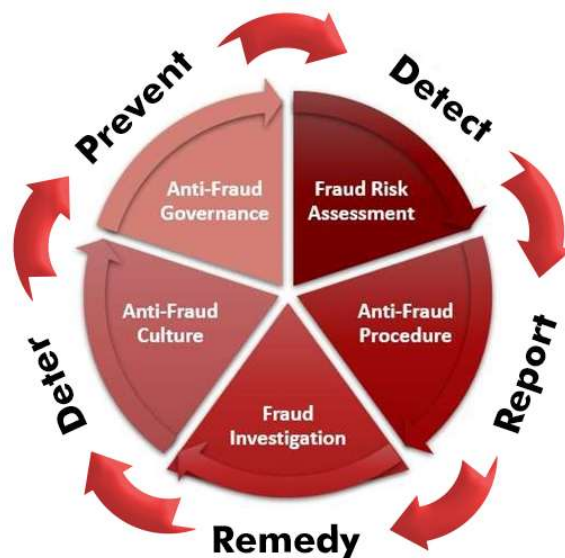
4. Purview of the Policy

The anti-fraud policy will comprise the following sections:

- a) Fraud Risk Management Framework
- b) Roles and responsibilities for fraud monitoring
- c) Procedures for fraud monitoring
- d) Reporting requirements
- e) Identify potential areas of fraud
- f) Co-ordination with law enforcement agencies
- g) Framework for exchange of information
- h) Due diligence
- i) Fraud Monitoring Committee
- j) Cyber and New age fraud

4 (a) Fraud Risk Management Framework

The company shall have the following framework to deter, prevent, detect, report and remedy fraud and ensure that there are adequate procedures in place, the framework given below is specific to Magma's business considering the nature of business, size, risk profile, overall business strategy, products, distribution channels, technology infrastructure and other parameters applicable,



a. **Deter** - implementing strategies to discourage fraudulent claims, misrepresentation, or unethical practices before they occur

- i Zero tolerance policy
- ii Customer verification process
- iii Training and awareness

- b. Prevent:** Though absolute prevention of fraud may not be possible, but the Company shall focus on prevention of fraud so that fraud can be prevented from entering into the system. Fraud can be prevented by taking the following steps into consideration.
- i. Robust internal control processes
 - ii. Data analysis to identify potential areas of fraud and suggest change in processes
 - iii. Training & awareness of employees at all levels
 - iv. Customer awareness programs
 - v. Identification, implementation, and periodic review of fraud triggers into the system and processes of the Company
- c. Detect:** There will be frauds which cannot be prevented even after taking strong fraud prevention measures, to detect such frauds the company must have elaborate mechanism in place broadly covered below.
- i. Fraud reporting tool for employees or associates of the company in the form of a common e-mail id and IFCU portal
 - ii. Analysis of claims and underwriting data such as claims frequency report
 - iii. Seeding in functions prone to fraud
 - iv. Specialized projects for detection of fraud
 - v. Red flag indicators are in place as applicable
- d. Report:** Established frauds shall be reported periodically in the following manner.
- i. Employee/Associate related fraud shall be reported to Disciplinary committee
 - ii. All fraud cases shall be reported to Fraud Monitoring committee, excluding employee related
 - iii. External frauds shall be reported to suitable law enforcement agencies
 - iv. The Risk Management Committee on quarterly basis as per the severity/relevance framework
- e. Remedy:**
- i. Ensure the action is taken as per Code of conduct and discipline
 - ii. Recover losses wherever required
 - iii. Initiate legal action as per process
 - iv. Investigate and close fraud cases.
 - v. Enhance fraud detection systems.
 - vi. Identify and strengthen process gaps and build controls
 - vii. Conduct staff training on compliance and ethics.
 - viii. Improve internal audit and monitoring frameworks.

f. Components to Fraud framework:

a. Anti – Fraud Governance:

The Board of Directors, Managers and Officers set the “tone at the top” for ethical behaviour by behaving ethically and openly communicating expectations for ethical behaviour to employees.

The Anti-Fraud policy is clearly communicated to all officers and staff members of the Company in an understandable fashion. The policy shall be communicated by the IFCU to all the employees of the Company and other persons dealing with the Company, through email, circular, or display on the Notice Board/ display on the Intranet, etc. In addition, regular and periodic training (including new-hire orientation and refresher training) shall be provided to all personnel, upon joining the organization and throughout their association with the Company, in order to clearly communicate expectations for ethical behavior to staff members. Directors, employees and contractors shall internally self-disclose potential or actual conflicts of interest to Company Secretary, Head of Legal and /or Head of Compliance / HR. As part of the Company’s due diligence for fraud detection and mitigation, background checks on new employees and personnel (management and staff) / insurance agent / corporate agent / intermediary shall be carried out in order to prevent fraud at the source.

b. Fraud Risk Assessment:

IFCU shall be working with each Vertical Heads to perform fraud risk assessments for each department of the Company as part of the annual risk assessment in accordance with Fraud Risk Management procedure.

The process of Fraud Risk Assessment will be as follows.

- Identifies fraud risks that affect achievement of goals and objectives
- Identifies various means of perpetrating fraud by creating fraud scenarios / indicators
- Determines the most appropriate business response to each fraud risk
- Evaluates health of existing internal controls and reports on how well the chosen responses are being implemented
- Assess the extent of exposure and determining action plans to address gaps, if any, to address the fraud risks

Identification of fraud risks and fraud risk scenarios / indicators shall be carried out by each vertical of Magma as per fraud framework above.

Fraud risk assessment provides a standard and consistent process for Magma and its business verticals to consider the extent to which potential fraud risks might have an impact on achievement of its objectives.

c. Risk response relates to the policies, procedures, processes, controls, and other actionable steps implemented to address the identified fraud risks associated with specified future events. Response to a fraud risk must be considered in light of costs to be incurred and consequent benefits (typically measured in terms of as estimate of the quantum of reduction in risk exposure).

The risk of fraud may increase if a control is inadequate. As the Company's operations change, the fraud risk assessment should be updated, where feasible, and the adequacy of the operating controls used to prevent or detect fraud should be evaluated.

These fraud risk assessments shall be subject to review and comment by the IFCU staff when performing their routine or special audits.

d. Anti – Fraud Procedures:

The fraud risks / triggers identified through the Fraud Risk Assessment process shall be monitored by respective Verticals on regular basis. Any case qualifying the criteria shall be reported by the respective Verticals to IFCU for investigation.

Magma shall have detailed Anti-Fraud procedures / process for detection and investigation of fraud risks. This process shall include the procedure for detection, investigation, reporting of fraud along with the process for actions to be initiated on investigation findings and various reporting to be done to the regulator, Board and Risk Management Committee

e. Fraud Investigations:

Cases reported to IFCU shall be investigated independently by IFCU or with the help of an external agency. The investigation reports shall be discussed with the respective Vertical Heads and needs to be placed at the Fraud Monitoring Committee and Disciplinary Committee, if the case requires initiation of Disciplinary action.

The document for Anti – Fraud Procedures shall incorporate the process to be followed for Fraud Investigations.

In conjunction with Annual Code of Conduct training to all employees, The Anti-fraud Policy should be reviewed annually

f. Whistleblower protection framework

The Company has Breach of Integrity and Whistle Blower Policy to supplement the Code of Conduct & Discipline Rules and Anti-Fraud Policy of the Company. Through this Policy, the Company intends to encourage its various stakeholders to report matters without the risk of subsequent victimization, discrimination or disadvantage. It serves as a guideline to deal with directors, employees, channel partners, customers, service providers or others who are reported to have breached integrity or committed fraudulent act(s).

The identity and details of the Whistle Blower shall be maintained in strict confidence

For detailed framework regarding Whistle blower protection please refer to the Breach of Integrity and whistle blower policy

g. Cyber fraud or new age fraud

In order to prevent Cyber or New Age fraud, CISO shall ensure to establish and implement robust cybersecurity framework to protect against evolving cyber frauds or threats. continuously monitor and strengthen systems and processes for fraud risk management, such as incident databases, customer verification, and access control.

Information Security: Utilize a team with relevant risk and technological expertise to manage cyber fraud risks across various insurance business lines of the Company

4 (b) Roles & Responsibilities for Fraud Monitoring

In summary, the specific roles, and responsibilities for preventing and responding to fraud in Magma are the following:

Responsibility of Board

- Responsibility for effective and responsible fraud governance.
- Setting the tone for fraud risk management within the organization.
- Oversee and monitor management's actions to manage fraud risks.
- Ensure that management designs effective fraud risk management policies that encourage ethical behaviour, including processes for employees, customers, and external business relationship partners to report instances where those policies are violated.
- Maintain oversight of the fraud risk assessment by ensuring that fraud risk has been considered as part of the organization's risk assessment and strategic plans.
- Review reports on fraud investigations and corrective actions taken by the management to manage fraud risks and obtain reasonable assurance on the effectiveness of the fraud risk management program and controls addressing fraud risks.

a) red flag indicators, as applicable.

b) adequate procedures to deter, prevent, detect, report and remedy fraud in each category of fraud across various activities

c) responsibilities, delegation of authorities for all relevant functions including for identified sensitive posts

Responsibilities, delegation of authorities for all relevant functions including for identified sensitive posts

- Chief Risk Officer (CRO) – responsible for overall fraud risk oversight.
- Finance / Treasury / Accounts Payable – responsible to report cases of financial fraud
- Claims – to report fraud cases based on claim data analysis for region/zone wise
- Underwriting – fraud Risk Identification before accepting risk
- Investigation & Fraud Control Unit (IFCU) – manage fraud detection, investigations, and reporting.

- Compliance – enforce regulatory norms
- Internal Audit – conduct fraud-sensitive audits and internal checks
- IT Security– cyber controls and report cyber fraud
- Procurement / Vendor Management – report fraud cases
- Operations – quality control and report fraud cases

The above authority may delegate responsibility to their senior employees for further action.

Non-compliance with the FRMF may be detected through monitoring, audits, system alerts, or whistleblower reports. IFCU will analyze business and claims data to identify fraud and complete investigations.

For missed fraud cases detected late—post-payout, during audits, or through whistleblowers—IFCU will run targeted projects to identify fraud indicators and implement measures to address process gaps.

Risk Management Committee

- Sponsors the fraud monitoring framework.
- Provides concurrence to the fraud monitoring strategy, policy, and process.
- Evaluates the effectiveness of fraud monitoring framework, policy, process, and structure in the organisation. Evaluate management’s identification of fraud risks and the implementation of anti-fraud measures, and to provide the tone at the top that fraud will not be accepted in any form.
- Oversee controls to prevent or detect management fraud.
- Oversee the organization’s assessment of fraud risks and use internal auditors, or other designated personnel, to monitor fraud risks

Audit Committee:

- Oversee senior management’s compliance with appropriate financial reporting and for preventing senior management override of controls or other inappropriate influence over the reporting process.
- Establish mechanisms to ensure it receives accurate and timely information from management, internal and external auditors, and other stakeholders regarding potential fraud occurrences.
- Require information on frauds based on investigation reports and management responses through disciplinary and / or legal actions and improvements in fraud related internal controls and any other measures taken.
- Provides the external auditors with evidence that the committee is committed to fraud risk management and will discuss with the external auditor the auditors’ planned approach to fraud detection as part of the financial statement audit.

Fraud Monitoring Committee:

Fraud Monitoring Committee (FMC) which shall be responsible for operationalizing the Fraud risk management framework within the Company and oversee activities appropriate to ensure fraud deterrence, prevention, detection, reporting and remedying.

Composition of FMC:

- Fraud Monitoring Committee (FMC) comprising of: Chief Risk Officer (CRO), Head -UW, Head of claims, Head of Legal and Head FCU. FMC may form sub-committee, if required

Chairman: The Committee shall be chaired by CRO

Invitee(s): The Committee may, at its discretion, invite such other officials of the Company as may be considered necessary for effective discharge of its functions, external consultants, forensic experts, auditors etc. as may be considered necessary for effective discharge of its functions.

Responsibilities of FMC:

1. Recommend and regularly update, based on experience, fraud risk management to various functions
2. Oversee prompt responses to instances or suspicions of fraud
3. Maintain all relevant details pertaining to each instance of fraud
4. 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.
5. 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.
6. Identify areas for improvement and adaptation of the Fraud Risk
7. For operational purposes any member of FMC shall be designated as SPOC for submitting reports to RMC and Board through secretarial team.
8. FMC shall report to the Audit Committee, in addition to the RMC, in case of all internal frauds

4 (c) Fraud Risk Identification, Mitigation and Monitoring:**Investigation and Fraud Control Unit (IFCU)**

The IFCU oversees the process by which business verticals detect, monitor, and mitigate occurrence of insurance fraud risks within Magma.

IFCU's primary role is to ensure effective implementation of the anti-fraud policy of the company and is also responsible for the following:

- Set the overall tone to reinforce the message that fraud will not be tolerated.
- Designs, develops, and periodically updates the anti-fraud policy and framework, including an appropriate control environment and a fraud response plan.
- Promote and implement the anti-fraud policy by enhancing the level of risk awareness within the Company and through the development of appropriate procedures and the commitment of resources.
- Ensure adherence to anti-fraud policy and procedures and that the fraud monitoring framework is sustainable by continuously evaluating its effectiveness.

- Oversee the fraud risk management process by which business verticals prevent, detect, monitor, and mitigate occurrence of fraud risks within the company.
- Assesses the vulnerability of Magma to fraudulent activity by development of an organizational risk profile, including consideration of fraud risks, and regular review of the fraud risks associated with organizational objectives.
- Create awareness among employees, customers, and external business relationship partners to counter and report frauds.
- Establish mechanisms and procedures for reporting suspected fraud and issues with fraud risk management.
- Investigation of whistle-blower cases as referred by HR.
- Ensure that staff knowledge of anti-fraud policies is sufficient, and that appropriate training is provided.
- Encourage staff to report reasonable suspicions of fraud, treating all allegations seriously, and promptly reporting allegations to IFCU, HR or Line Managers.
- Shall carry out Investigations and take appropriate actions.
- Ensure that swift action is taken to respond to allegations and substantiated cases of fraud.
- Review information on frauds reported and their status based on investigation reports and management responses through disciplinary and / or legal actions and improvements in fraud related internal controls and any other measures taken.
- Report to the Board on what actions have been taken to manage fraud risks and regularly reporting on the effectiveness of the fraud risk management program. This includes reporting any remedial steps that are needed, as well as reporting actual frauds.
- Establish procedures, checks and controls to prevent fraud and detect fraud as and when it occurs.
- Ensure that regular feedback is given to the respective departments so that control systems can be strengthened continuously
- Create a culture through words and actions where it is clear that fraud is not tolerated, that any such behaviour is dealt with swiftly and decisively, and that whistle-blowers will not suffer retribution.
- Interview and communicate regularly with those conducting the organization's risk assessments, as well as others in key positions throughout the organization, to help them ensure that all fraud risks have been considered appropriately.
- All the actions on non-employees would be routed through IFCU
- Action to be initiated on agents / intermediaries and PI agencies actions would be decided by IFCU post seeking views from respective departments
- For any action to be taken on any employee, IFCU team to inform HR for the same along with all the relevant details.
- FCU to ensure to present the quarterly reports to FMC. FMC in turn shall submit quarterly report to RMC on its activities, findings, and recommendations, including the financial impact of fraud on the insurer.
- Report to the Audit Committee, in addition to the RMC, in case of all internal frauds.
- Identify red flag indicators for detection of fraud and incorporate appropriately. Such RFIs shall be reviewed regularly for continued relevance and effectiveness in detective frauds

- The FCU shall maintain database of person: convicted of or attempting fraud, conducting fraud-sensitive audits for compliance with the Fraud Risk Monitoring Framework. tracking business trends from distribution channels, continuously monitoring vendor activities for compliance with fraud prevention measures and contractual obligations analyzing customer grievances and complaints to detect and prevent fraud.
- FCU team accessing the IIB website shall ensure that database distribution channels, hospitals, third party vendors and fraud perpetrators blacklisted reported as fraud is shared with IIB. FCU shall ensure (post IIB informing them about submissions to be made) submissions to IIB through compliance team.
- Learning and Development Team along with FCU shall conduct periodic training program for the employees and the senior management including the board members. FCU along with Marketing Team to create contents to educate policyholders and the general public about the risk of fraud and how to prevent and protect against it. FCU along with Business team to conduct fraud awareness programs for distribution channels.
- The IFCU shall implement appropriate measures to proactively detect and prevent fraud, including:
 - Maintaining an Incident Database of individuals involved in, or attempting, fraudulent activities
 - Conducting fraud-sensitive audits to ensure compliance with the Fraud Risk Monitoring Framework
 - Tracking business trends across distribution channels to identify unusual patterns or emerging fraud risks.
 - Continuously monitoring vendor activities for adherence to fraud-prevention measures and contractual obligations.
 - Analyzing customer grievances and complaints to detect fraud indicators and strengthen preventive controls.
 - Data claim data analysis.
- The internal turnaround time from identification to remedy is 45 days, The IFCU has mechanism for reporting fraud to CRO, IFCU portal and Whistleblow email id, and CRO is designated officer for reporting incidents of fraud and report submission.

Human Resource

- For actions of employee:
 - Issuance of Show Cause Notice to concern employees under investigation, seeking explanation on the incident reported, where applicable.
 - Based on the recommendations of the Disciplinary Committee / investigation report, take appropriate actions against perpetrators of fraud and / or supervisors whose failures have contributed to the commission of fraud, and ensure that appropriate action is taken to recover assets, modify processes and restore company's reputation and goodwill.
- Take appropriate measures in case of frivolous or bad faith allegations.
- Keep updated records of any reported fraud or suspected fraud allegations made, any subsequent actions taken, and the ensuing result.
- Assist management in educating and providing training sessions to staffs on anti-fraud policy and program.

Disciplinary Authority / Committee: Cases of employee misconduct relating to fraud or non-compliance. All such cases shall be placed before the Disciplinary Committee, for detailed framework regarding Disciplinary Committee refer to the Whistle blower Policy.

Compliance Officer

Compliance Officer is responsible for the following:

- Liaison with Regulatory Authority on fraud reporting requirements.
- Furnish various reports on frauds to the Regulatory Authority as stipulated in this regard.

4 (d) Reporting requirements

Reporting to IRDAI:

In order to file reports to IRDAI under fraud monitoring, date of IFCU's investigation report would be considered as date of detection of fraud and Compliance team would file the case specific reports to IRDAI within the time frames stipulated by the IRDAI.

The Compliance team, with the assistance of IFCU, will submit fraud monitoring reports on yearly basis or as may be required under applicable regulations w in the prescribed forms/formats

FCU shall inform compliance team for frauds involving distribution channel for informing IRDAI.

Reporting to Risk Management Committee of the Board:

Critical cases wherein fraud has been established would be reported to the Risk Management Committee of Board on quarterly basis. The criticality matrix shall form part of the Standard Operating Procedures and will be reviewed and updated as and when required.

4 (e) Identify Potential Areas of Fraud

Risk Management and Internal Control:

Risk management is at the heart of effective fraud control, especially through the development of risk criteria and implementation of effective controls. Magma will undertake a comprehensive evaluation of its overall vulnerability to fraud as well as the scope and magnitude of fraud risk in specific areas at least every two years, or more frequently as part of an on-going rolling risk assessment process. Findings will be reported to the Board and Risk Management Committee of Magma. The Board and Risk Management Committee of Magma:

- Expect the Chief Risk Officer to exercise proactively his/her responsibility for the overall management of fraud risk and for the management of specific fraud risks.
- Will monitor the implementation of mitigation measures /actions designed to reduce or mitigate fraud risk.

- Where there is insufficient or lack of management response to fraud, report the matter to Board and Risk Management Committee with recommendations for appropriate action.

IFCU will:

- Establish internal controls to deter, prevent, detect, report and remedy deter fraud that are cost effective and commensurate with the magnitude of identified risks.
- Ensure that staff are comfortable to report fraud without any fear.
- Initiate and facilitate fraud detection and reporting.
- Determine whether each risk, judged according to its probability and severity, should be prevented, mitigated, transferred, or accepted.
- Report on the implementation of actions designed to reduce fraud risk.

The company shall follow the Fraud Risk Assessment procedure, as defined in this policy

4 (f) Co-ordination with Law Enforcement Agencies

Any communication or co-ordination with law enforcement agencies like Police, CBI, etc. in connection to fraud or suspected fraud shall be represented by IFCU in consultation with Legal team of Magma.

A log of all such communications with law enforcement communications is to be maintained by IFCU.

This communications log shall include:

- Date of communication(s);
- Name, department, and location of the law enforcement official.
- Applicable Fraud Case number and details (to be assigned by IFCU) and
- Information sought by law enforcement.

This communication log will be maintained by the IFCU and shall be produced for the regulatory authorities upon request.

4 (g) Exchange of information between insurers

Relevant information about internal fraudsters and fraudulent policyholders, claimants, beneficiaries, intermediaries and other third parties faced by the Company to be shared with General Insurance Council on a periodic basis.

The Company will also provide full cooperation with other insurance stakeholders.

4 (h) Due Diligence

Due Diligence procedures followed by the Company on their personnel (management and staff) / Insurance agent / Corporate Agent / intermediaries/Vendor before appointment / agreement with them as below:

i. **Personnel (management and staff)**

After selection of candidate by the Concerned vertical and HR, Branch / HO HR team on receipt of duly filled Application Form (AF) and required documents perform all the below scrutiny and checks:

- a) Completeness check of AF
- b) Documents verification
- c) Background verification by external agency

ii. **Intermediaries – Insurance Agents / Corporate Agent/Vendors, etc.**

Due Diligence shall be conducted by the respective sales team and the Agency Support team at the time of appointment of insurance agents / intermediaries. And for vendors, due diligence shall be conducted by respective stake holders/vertical heads at the time of appointments.

5. Reporting of Fraud

- If employee of company prefers to report fraud, they can by sending an email to **whistleblow@magmainsurance.com**.
- Write a letter to The Chief Risk Officer, Equinox Tower 3, Second Floor, Ambedkar Nagar, Corporate Park, Kurla (West), Mumbai, Maharashtra – 400070
- Directly report the suspected fraud cases on IFCU portal using the below link **<https://fasttrack.magmainsurance.com/IFCU/Complaint/Home/RaisedComplaint#>**

6. Confidentiality

No employee or person acting on behalf of Magma in attempting to comply with this policy shall:

- Be dismissed or threatened with dismissal.
- Be disciplined or suspended or threatened with discipline or suspension.
- Be penalized or have any other retribution imposed; or
- Be intimidated or coerced.

based upon the fact that the employee or other person has reported an incident or participated in an investigation in accordance with the requirements of this policy. Violation of this section of the policy shall result in disciplinary action, up to and including dismissal.

If an allegation is made in good faith, but is not confirmed by the investigation, no action will be taken against the originator. However, malicious allegations will result in disciplinary action against such individuals.

7. Administration of the Policy

IFCU is responsible for administration, interpretation, application, and periodical review of this policy. However, the decision of Board will be final in the case of difference in the interpretation of any of the clauses in the Policy.

Magma's Board of Directors shall review and ratify this policy based upon recommendation of the Risk Management Committee on annual basis and at such other intervals as it may be considered necessary.

Document review and approval

Document Name	Anti-fraud Policy
Document Version	11.0
Release Date	01.04.2026
Frequency of review	Annual

Document Owner	CRO
Document Reviewer	Head - IFCU
Document Approver	Board of Directors

8. Conclusion

Fraud Prevention and Control is extremely important in the context of Magma. It is always preferable to prevent frauds from occurring in the first place. The enunciation of the anti-fraud policy and implementation of the same in letter and spirit will go a long way in achieving the said objective.

Appendix - I

Illustrative List of Insurance Frauds / Red flag indicators

Broadly, the potential areas of fraud include those committed by the officials of the insurance company, insurance agent/corporate agent/intermediary/TPA/Vendor and the policyholders / their nominees. Some of the examples of fraudulent acts / omissions include, but are not limited to the following:

*Source: IRDAI circular on Insurance Fraud Monitoring Framework of 2025

1. Internal Fraud:

- a) Inflated expense claims or overbilling by employees.
- b) Payment of false or inflated invoices, either self-prepared or obtained through collusion with suppliers.
- c) Approving special prices or privileges to customers or awarding business to favoured suppliers in exchange for kickbacks.
- d) Forging signatures on official documents.
- e) Unauthorized removal of funds from customer accounts (e.g., CD accounts).
- f) Falsification or forgery of documents.
- g) Selling organizational assets below their true value in return for personal gain.
- h) Creating fake insurance policies
- i) Creating agent code in the name of a family, friend & relative
- j) Siphoning premium amount
- k) Taking advantage of system or process gaps to pass benefits to wrong entities
- l) Business/confidential data sharing to wrong entities/recipient's

2. Distribution Channel Fraud:

- a) Agents using shared login credentials or common passwords.
- b) Unusual spike in business from a single intermediary or specific location.
- c) Multiple policies issued from the same IP address or device outside routine usage.
- d) Intermediary linked to multiple suspicious or fraudulent cases.
- e) Multiple failed login attempts followed by successful access.
- f) Unusual system activity occurring outside normal business hours.
- g) Use of VPNs or masked IP addresses during policy issuance or claim filing
- h) Creating fake insurance policies

3. Policyholder Fraud and/or Claim Fraud:

- a) Misrepresenting age, health condition, or occupation.
- b) Concealing pre-existing vehicle damage and medical conditions.
- c) Multiple policies issued to the same individual within a short timeframe.
- d) Frequent changes in beneficiary or nominee details or endorsement/s.
- e) High Sum Insured policies with a single premium payment without a clear source of funds.
- f) Policies booked using common IP addresses or devices.
- g) A single party making payments for multiple policies.
- h) The same KYC details used across multiple policies.
- i) Insured person changes address, bank account, or contact details shortly before filing a claim.

- j) Customer consistently avoids verification calls or provides contradictory information during the process.
- k) Submission of forged or altered documents, such as identity proofs or medical reports.
- l) Payments are structured through multiple small transactions or routed via third-party accounts.
- m) Close proximity claims (break in, rollover/renewal & NCB)
- n) Single driving license against multiple claims
- o) Frequent claims against multiple losses for single vehicle
- p) Claims filed shortly after policy issuance, especially for high-value amounts.
- q) Submission of inconsistent or incomplete documentation for claims.
- r) Frequent claims originating from the same Garage, hospital or service provider.
- s) Claimant unwilling to provide original documents or cooperate during investigations.
- t) Claim triggers should be reviewed semi-annually to strengthen the claim processing system.
- u) Any suspected or fraudulent case must be investigated promptly, beyond standard triggers.
- v) Claimant has a history of problematic or fraudulent claims.
- w) Identity of the policyholder, insured, or beneficiary cannot be verified.
- x) Staging accidents, Inflating repair costs.
- y) Approving and settling fraudulent claims
- z) Wrong reserving

4. External Fraud:

- a) Hospitals or garages inflating bills or charging for services not rendered.
- b) Collusion between service providers and policyholders generate fraudulent claims.
- c) Using stolen or fake identities to purchase policies or to file claims.
- d) Impersonating policyholders to divert claim payouts.
- e) Mis-selling policies with false promises.
- f) Pocketing premiums without issuing valid policies.
- g) Collusion with customers for fraudulent claims
- h) Phishing attacks to steal customer data.
- i) Unauthorized access to insurer systems to manipulate policy or claim details.
- j) Use of VPNs or masked IPs for fraudulent transactions.

5. Affinity Fraud or Complex Fraud

- a) Group-Based Misrepresentation: Fraudsters may market fake or misleading insurance products to members of a community, claiming special benefits or discounts.
- b) Collusion with Community Leaders: Trusted leaders may be manipulated into endorsing fraudulent insurance schemes, making members more likely to buy policies.
- c) Ponzi or Multi Level Mktg/Pyramid Schemes: Premiums collected from new members are used to pay claims or returns to earlier members, creating an illusion of legitimacy.
- d) Fake Group Policies: Offering “exclusive” group health or insurance plans that do not exist or have hidden exclusions.
- e) Collusion Among Multiple Actors: Fraudsters may include policyholders, intermediaries, service providers (hospitals, garages), and sometimes even employees of the insurer.

- f) Organized Networks: Groups work together to stage accidents, fabricate medical treatments, or create fake documentation for large-scale claims.
- g) Layered Transactions: Use of multiple accounts, intermediaries, and third-party vendors to obscure the fraud trail
- h) Cross-Border or Multi-Jurisdictional: Fraud schemes involving international entities or offshore accounts to complicate investigations.

Change Control Record

Version No.	Change Request by	Memorandum of Change	Approval Date
2.0	Sajjan Kumar Kedia	Changes made in reporting of fraud, investigation of the fraud/suspected fraud, reporting to IRDA and insertion of process modification.	24.10.2013
3.0	Anand Roop Choudhary	Ownership of the policy redefined Responsibilities has been bifurcated between Audit Committee and Risk Management Committee Responsibility for carrying out investigations and other activities listed in the policy has been shifted to the Fraud Control Unit	04.05.2017

Version No.	Change Request by	Memorandum of Change	Approval Date
4.0	Anand Roop Choudhary	<p>The Fraud Risk Management Structure and various channels of communications have been replaced with a comprehensive Fraud Framework which encompasses the following.</p> <ol style="list-style-type: none"> 1. Fraud Risk Assessment 2. Anti-Fraud Procedures 3. Fraud Investigations 4. Anti-Fraud Culture 5. Anti-Fraud Governance <p>Investigation of whistle-blower cases referred by HR Two tiers of Disciplinary Committee defined:</p> <ol style="list-style-type: none"> 1. Consisting of Head of HR, Head of Internal Audit and CFO for cases having involvement of employees with grades above Sr. Manager 2. Consisting of Head of Internal Audit, Financial Controller and Zonal Head HR for cases having involvement of employees with grades of Sr. Manager and below <p>Procedures of Fraud Monitoring has been detailed in a separate SOP. This policy mentions the various aspects that needs to be covered in the SOP</p> <p>The log of communications with Law enforcement agencies for cases pertaining to fraud is to be maintained by IFCU</p>	27.07.2018
5.0	Anand Roop Choudhary	Included Head of Legal and Compliance as the permanent member of the Disciplinary Committee	18.07.2019
6.0	Amit Bhandari	<p>Chief Risk Officer (CRO) is the new policy owner</p> <p>Quorum of any Disciplinary Committee shall consist of at least three members</p> <p>Critical cases and update on fraud is to be provided to Risk Management Committee every quarter</p>	24.07.2020
6.0	Amit Bhandari	No change in policy	22.07.2021
7.0	Amit Bhandari	Change in constitution of Disciplinary Committee	21.10.2021
8.0	Amit Bhandari	<p>Changes in Classification of Insurance Fraud- it is further classified in to</p> <ol style="list-style-type: none"> 1. Vendor Fraud 	09.11.2022

Version No.	Change Request by	Memorandum of Change	Approval Date
		<p>2. Fraud relating to Insurance Self Network Portal (ISNP) and e-commerce</p> <ul style="list-style-type: none"> • Changes made in Fraud Framework • Changes made in Components to Fraud Framework <ol style="list-style-type: none"> 1. Anti- Fraud Governance 2. Fraud Risk Assessment 3. Fraud Investigation- Anti Fraud policy should be reviewed annually 4. Anti- Fraud Culture: Awareness Raising and Training- Shifted under Fraud Investigation due to repetition 5. Constitution of Disciplinary Committee excluded from Disciplinary Authority / Committee definition 6. Excluded Procedure for Fraud Monitoring 7. Reporting Requirements <ul style="list-style-type: none"> • Co-ordination with Law Enforcement Agencies shall be represented by IFCU in consultation with Legal team of Magma • New addition in Due Diligence – Due diligence of Vendors has been added in Due Diligence • Reporting of Fraud – different modes of reporting incorporated • Modified Appendix I: Illustrative list of Insurance Fraud: list of insurance fraud for Vendors and Insurance Self Network Portal (ISNP) incorporated. • Modified Appendix II: Illustrative List of Cyber Frauds in the insurance sector: Various cyber frauds incorporated. • Excluded Fraud Monitoring Template and Guidance for Fraud Cases to be considered as Closure for reporting from Appendix II 	
8.0	Amit Bhandari	No change in policy	
9.0	Amit Bhandari	<p>Change made in Roles & Responsibilities for Fraud Monitoring:</p> <ol style="list-style-type: none"> 1. New addition in Roles & Responsibilities for Fraud Monitoring: Investigation and Fraud Control Unit (IFCU) - For any action to be taken 	24.10.2024

Version No.	Change Request by	Memorandum of Change	Approval Date
		<p>on any employee, IFCU team to inform HR for the same along with all the relevant details.</p> <p>2. New addition in Roles & Responsibilities for Fraud Monitoring: Human Resource - For actions of employee, Issuance of Show Cause Notice to concern employees under investigation, seeking explanation on the incident reported, where applicable.</p> <p>3. Excluded from Roles & Responsibilities for Fraud Monitoring: Compliance officer - Sign and accept the Anti-Fraud Policy as an integral part of their employment contract</p>	
10.0	Kishore Khanchandani	<p>Changes made in Reporting of Fraud</p> <p>1. whistleblow@magmaininsurance.com</p>	21.07.2025
11.0	Kishore Khanchandani	<p>Changes made in</p> <p>1. Governing guideline policy</p> <p>2. New addition of Definition and Classification of Insurance Fraud</p> <ul style="list-style-type: none"> Claim fraud, Distribution fraud, External fraud & Affinity fraud Excluded from Definition and Classification of Insurance Fraud Intermediary fraud, Vendor fraud, Insurance Self Network Portal fraud <p>3. New addition in Purview of the policy</p> <ul style="list-style-type: none"> Replaced Fraud framework with Fraud Risk Management framework Added Fraud Monitoring Committee Added Cyber and New age fraud <p>4. New Additions to Fraud Risk Management Framework</p> <ul style="list-style-type: none"> Deter, Report and Remedy Excluded Respond Replaced responsibility of policy communication from Head Legal and Compliance to IFCU <p>5. New addition to Components to Fraud Framework</p> <ul style="list-style-type: none"> Periodicity of assessment of Fraud Risk Assessment modified to annually Review of Anti-fraud policy shifted under document review and approval Whistleblower protection framework 	10.02.2026

Version No.	Change Request by	Memorandum of Change	Approval Date
		<ul style="list-style-type: none"> • Cyber fraud or new age fraud • Information Security <p>6.New additions to Roles & Responsibilities for Fraud Monitoring</p> <ul style="list-style-type: none"> • Responsibility of board aligned with new regulation • Fraud Monitoring Committee, • Composition of FMC, • Responsibility of FMC • Delegation of authorities for all relevant functions including for identified sensitive posts <p>7.New addition to Fraud Risk Identification, Mitigation and Monitoring</p> <ul style="list-style-type: none"> • Modified Investigation and Fraud Control Unit (IFCU), a, The FCU shall maintain database of person convicted or attempting to commit fraud, b, FCU team accessing the IIB website, c, Learning and Development Team along with FCU shall conduct periodic training • Internal turnaround times for FIP from identification to remedy, designated officer(s) for reporting incidents of fraud and report submission • Excluded Disciplinary Authority / Committee The quorum of Disciplinary Committee shall consist of at least four members • Compliance Officer responsibility realigned <p>8.New addition to Identify Potential Areas of Fraud</p> <ul style="list-style-type: none"> • IFCU will create control to deter, prevent, detect, report and remedy <p>9.Modified Appendix I: Illustrative List/Red flag indicators (RFI), which are Internal fraud, Distribution fraud, Policy holder and/or claim fraud, External fraud and Affinity fraud/Complex fraud. (*Source: IRDAI circular on Insurance Fraud Monitoring Framework of 2025)</p>	