Raheja QBE General Insurance Company Limited

ANTI-FRAUD POLICY

Reference:	Annual Review
Owner:	Chief Risk Officer
Frequency of review:	Annual
Approval:	RQBE Board of Directors
Approval date:	May 11, 2026
Version:	V.10
Points of contact:	Lokesh Agarwal Chief Risk Officer, Lokesh.agarwal@rahejaqbe.com

Table of Contents

RQBE Anti-Fraud Policy

Introduction

RQBE is committed to conducting business in an open and honest manner, and to ensure that only the highest ethical standards are displayed in all areas of our business.

Acts of fraud can greatly impact our profitability and reputation, as well as undermine our customers' confidence in our products and services. There may also be an indirect impact on policyholders through premium increases arising from high claims cost as a result of fraudulent activities.

As such, RQBE as part of its risk management practices seeks to avoid significant operational risk exposures or losses caused by:

- illegal conduct by RQBE personnel or agents;
- employee dishonesty, including internal fraud or collusion with external parties

RQBE, through its employees, seeks to do the right thing with its customers (including brokers, intermediaries, agents, end customers and business partners), its people, its shareholders and the communities which it works in (including regulators and Government).

It will respond to instances of suspected fraudulent acts whether internal or external with rigour and where appropriate by all legally available means.

The Board and Management of RQBE support a zero-tolerance approach to any acts of fraud committed to gain a business advantage. It is recognised that such acts pose significant regulatory, legal and reputational risks to the company and should be severely dealt with.
References to "**RQBE"** mean **"Raheja QBE General Insurance Company Limited".**

Purpose

This Policy provides Management and staff of RQBE with a framework to:

- managing and mitigating risks of fraud
- identify, measure, control and monitor fraud risk,
- investigate and report frauds,
- increase staff awareness of the types of fraudulent activities that RQBE may be exposed to in the course of business activities,
- create awareness among intermediaries and policyholders to counter insurance frauds, and
- ensure compliance with the relevant laws (including IRDA's Guidelines no. IRDAI/IID/GDL/MISC/112/10/2025 on Insurance Fraud Monitoring Framework) and policies which are applicable to each person in his/her role whilst carrying out business on behalf of RQBE.

Scope

This Policy applies to every director, officer, employee and contractor of RQBE.

I. Definitions

(I) **Fraud:** Fraud in insurance, as defined in the IRDAI Circular on Insurance Fraud Monitoring Framework, 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:

- misappropriating assets

- deliberately misrepresenting, concealing, suppressing or not disclosing one or more material facts relevant to the financial decision, transaction or perception of the insurer's status
- abusing responsibility, a position of trust or a fiduciary relationship.

Fraudulent activities can be internally or externally focused, or a mix of the two where collusion exists.

(II) **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.

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

II. Roles and Responsibilities:

It is the responsibility of every RQBE employee to adopt a rigorous approach to managing the risks of fraud. This ownership of risk is supported by RQBE's culture, the Board and dedicated risk management personnel with the responsibility for maintaining and implementing the Policy.

(a) RQBE Board

Responsible for:

- Setting the "tone at the top" that fraud will not be tolerated and ensuring that appropriate policy and procedures are in place to identify and mitigate fraud risks
- Approve and review the Anti-Fraud policy annually to ensure its continual effectiveness in preventing acts of fraud;
- Ensure that management has adequate resources, expertise and support to effectively implement the fraud management strategies, policies and procedures.

(b) Executive Management

Responsible for:

- Establish appropriate processes for fraud risk assessment, identification, measurement, control, monitoring, as well as the investigating and reporting of such acts;
- Review the fraud risk assessments and internal investigations to facilitate prompt responses to occurrences or suspicions of such activity;
- Review the Anti-Fraud Policy annually and recommending it to the Board for approval;
- Encourage the reporting of fraud cases and provide support as necessary for these employees or others who make such reports; and
- Support and actively promote a proactive fraud resistant culture to develop and grow within RQBE.

(c) Risk Owners/Managers

- Allocate adequate resources, expertise and support for the effective management of the fraud risks.
- Carry out periodic reviews and assessments of the controls in place to manage fraud risks through the Risk and Control Assessment process;
- Review the effectiveness of current control processes and procedures in deterring, preventing and detecting fraud regularly, or as and when there is a material change to the risk profile, such as a major change in the processes or systems;
- Ensure that cases of fraud are reported as per Clause No. XIV, where appropriate on a timely basis; and
- Support and actively promote a proactive fraud resistant culture to develop and grow within RQBE.

(d) All Employees

- Adhere to the RQBE Code of Conduct;
- Have a due responsibility to protect business assets, including information, goodwill and physical property;
- Undertake fraud risk awareness training, and champion the prevention of fraud within the business and functional units;
- Report any actual or suspected cases of fraud; and
- Be vigilant for any unusual signs and patterns which may suggest that an act of fraud is taking place;

(e) Agents

- Conduct their business with utmost good faith and integrity;
- Undertake fraud risk awareness training conducted by RQBE; and
- Report any actual or suspected cases of fraud, where it relates to RQBE.

III. Fraud Risk and Control Assessment

An assessment of the risks of fraud needs to be undertaken annually. This is completed as part of the company risk assessment based on the RQBE Risk Management Strategy.

IV. RQBE's Fraud Management Framework

The Fraud Management Framework ("FMF") encapsulates the:

a) Identification of potential areas of fraud and assessment of RQBE's risk profile

b) Processes and procedures to proactively identify, detect, investigate and report fraud

c) Roles and responsibilities of the parties responsible for fraud management

➢ Potential areas of frauds and assessment of risk profile

Financial Crimes, encompassing fraud, are a subset of operational risks. These fraud risks, however, differ greatly from other risks as they are deliberately perpetrated, involving the **elements of intent and concealment**, which could make them difficult to trace.

There are 5 broad categories of frauds, namely:

a) **Policyholder Fraud and/or Claims Fraud** - Fraud against RQBE in the purchase and/or execution of an insurance product, including fraud at the time of making a claim.

b) **Intermediary Fraud** - Fraud perpetuated by an insurance agent / Corporate Agent/ intermediary / Third Party Administrators (TPAs) against the RQBE and/or policyholders.

c) **Internal Fraud** – Fraud / mis-appropriation by its Director, Manager and/or any other officer or staff member, including collusion with parties internal or external to the RQBE and fraud perpetuated by any external party (e.g. auditors, consultants, loss adjusters) engaged as a service provider by the insurer.

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 insurance frauds may be found in **Appendix 1**. These instances include frauds perpetuated internally by insurance agents, corporate agents, intermediaries or TPAs, and instances of claims or policyholder frauds.

The risk profile should be established to determine RQBE's overall vulnerability to acts of fraud. The risk profile can be determined in the context of the following factors:

- Size, composition and volatility of business;
- Organisational structure;
- Products and services offered;
- Remuneration and promotion policies;
- Distribution modes;
- Market conditions/environment; and
- Past experiences of fraud.

Each factor should be assessed on how significant an impact it is likely to have on RQBE's overall vulnerability level. This will be based on the RMS rating scale of Critical, High, Medium and Low.

Key functional areas in RQBE carry out annual risk assessments to identify risks, including risk of frauds in their area of responsibilities, and assess the effectiveness of controls to mitigate these risks.

V. Risk & Control Assessment

Business entity should also identify areas of RQBE's business where fraud risks could have a potential material impact. These risks typically could emanate from various parts of the key business process; e.g. Claims, Finance, Procurement or Underwriting.

Key controls must be put in place to effectively reduce or mitigate the risks. RQBE should regularly monitor and review any changes to its risk profile and the effectiveness of its controls in managing the identified risks and ensure that the risk and control assessment is kept as updated as soon as possible to reflect any significant changes in the business or risk environment.

Red Flag Indicator:

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. Some of potential red flag indicators during the policy issuance and the course of insurance business is given below:

Potential policyholder and claims fraud indicators – red flags

Claimant's behavior

- The claimant threatens to bring in a lawyer if the claim is not settled swiftly.
- The claimant wants cash.
- To deal with the claim quickly, the claimant is willing to accept an inexplicably low settlement.
- The claimant is unwilling to co-operate during a reconstruction and/or gives evasive answers.
- The claimant handles all business in person or by phone, avoiding written communication.
- The claimant gives inconsistent statements to the police, experts and third parties.
- The policyholder has several policies with the same insured object and coverage.
- The insured requests that payment is made into different accounts.
- The insured changes address, bank or telephone details shortly before a claim is made.
- The claimant insists without proper reason on using certain contractors, engineers or medical practitioners or wants to use relatives.

- The policyholder has been denied insurance before and has not mentioned this when applying for insurance.
- The identity of the policyholder, the insured or beneficiary cannot be determined.
- The insured frequently makes high claims.

Documents

- The claimant is not able to provide documentary evidence for major losses, such as receipts or photographs (and minor losses are documented).
- Documents are changed or are unreadable.
- Original documents/receipts are missing, only copies are provided.
- There is different handwriting on various receipts.
- Receipts are provided from companies that do not exist, have ceased operating or are insolvent.
- Receipts with differing dates have successive numbering.
- The claim form is not completely filled in and/or not signed.
- Alterations are made in the claims form to create appearance of cover.
- There are inconsistencies between the application form and the claim form.
- There are variations in or additions to the policyholder's initial claims.
- Reports from medical practitioners or others are inconsistent.
- The diagnosis is incorrect or the adjuster receives conflicting medical opinions from medical providers.
- Prescriptions are cut or have been altered.
- The treatment being provided to the claimant is inconsistent with the report diagnosis.
- Medical terminology on the documents is misspelled or misused.
- The claimant changes attending physicians frequently.
- The attending physician is not in the same geographic region as the claimant.
- The attending physician's specialty is not consistent with the diagnosis.

Characteristics of losses

- The claim is filed either shortly after coverage becomes effective, or just before cover ceases or shortly after the cover has been increased or the contract provisions are changed.
- Actual loss is far higher than first reported loss.

Intermediary Fraud

- Premium diversion or misappropriation of funds.
- Frequent cancellations and re-issuance of policies.
- Intermediary unwilling to provide original documents or meet in person.
- Overly aggressive or evasive behaviour during investigation.

Internal Fraud

- Management turnover is high.
- Staff turnover in financial and accounting departments is high.
- There are indications of financial trouble, for example, inadequate capital or increase in unpaid debts.

External Fraud

- Discrepancies in KYC documents or mismatched details.
- Use of synthetic identities or unverifiable addresses.
- Reluctance to provide additional verification.
- Pressure to expedite transactions.

Affinity / Complex Fraud

- Employees and customers sharing unusual links or addresses.
- Common phone numbers, emails, or addresses across accounts.

VI. Processes to identify, detect, investigate and report fraud

Identification of fraud typically begins with a slight indication that something may not be right, such as the receiving of anonymous tips, unusual patterns in financial statements or control overrides. Each key functional unit has responsibilities to identify and manage fraud risks within their area of responsibilities.

VII. Roles and responsibilities for fraud management

i. Heads of Department and CXOs

- Take into account the business exposure to fraud and ensure that preventative controls are initiated for new and existing products, processes or systems
- Be aware of and alert to various types of expenses and procurement frauds that may be undertaken by both internal and external parties, whether alone or in collusion with another person
- Implement initiatives that enhance the effectiveness of fraud risk management and support and encourage the reporting of actual and suspected instances of Fraud i.e. gambling; illicit drug use etc.
- Ensure that all actual or suspected cases of fraud are immediately reported to the Managing Director & Chief Executive Officer
- Encourage an open and ethical culture where employees who report possible cases of fraud are protected accordingly through anonymity

ii. Underwriting function

- Consider the risk of fraud in relation to the risk selection and dealings with a customer, an employee or a supplier's perspective
- Ensure no conflict of interest situation in dealing with intermediaries or underwriting risks related to staff

iii. Insurance Claims Areas

- Be vigilant in detecting and investigating all known or suspected instances of client or customer fraud arising from workers compensation, or general insurance policies
- Ensure that all supporting claims documents/reports are valid and where needed, use accredited panel providers to conduct investigations in accordance with current legislation, company claims policy and best practices
- Maintain records of all matters investigated and subsequently reported to a prosecuting authority
- Undertake fraud risk assessments when required

iv. *Procurement & IT Assets Management*

- Consider and/or seek advice on fraud risks that may eventuate through, during or as a result of any contract with a supplier, agency or provider
- Obtain quotes from at least 3 vendors/suppliers for substantial procurement, and if not able to, with valid reasons and documented
- Conduct a rigorous due diligence process of all new and existing suppliers or providers prior to RQBE entering, or re-entering into a formal agreement with them
- Provide data as required to the Head - Human Resources for further analysis as required

v. *Human Resources (HR)*

- Responsible for updating and obtaining staff's annual acknowledgement of RQBE's Code of conduct and disclosure of conflict of interest situations
- Responsible for managing the staff-related disciplinary processes resulting from an internal investigation into fraudulent activity
- Ensure that all employees and contractors are employed in accordance with recruitment policies, with a sufficient amount of background checking
- Consult in accordance with the Fraud Response Plan on incidents and behaviours which identify possible fraudulent behaviours or risk being present within a business unit

vi. *All RQBE Employees*

- Recognise that risks associated with fraud are responsibility of all employees, suppliers and other people who carry out business in association with RQBE
- Report instances of actual or suspected fraudulent or dishonest behaviour to the appropriate management channel

vii. *Role and Responsibilities of the Management*

The Management is responsible for approving the final course of action based on investigations done by the Internal Audit Team. Other responsibilities include:

- Receiving fraud and related loss reports from managers and staff
- Ensuring investigations are conducted in a timely manner and in accordance with procedure
- Reporting fraud incidents and findings from investigations to the Board committees and Risk Management function
- Ensuring there is an ongoing fraud awareness program, including training for Management and staff in relation to their responsibilities for preventing, detecting and reporting fraud
- Support and promote reporting of all actual or suspected fraud and provide support as necessary for those employees or others who make reports of such Fraud, whether they are subsequently proved true or not

Fraud Monitoring Committee (FMC) :

Fraud Monitoring Committee (FMC) which shall be responsible for operationalizing the Fraud Risk Management Framework within the insurer and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.

FMC Composition:

- Headed by Chief Financial Officer and other members include Chief Claim Officer, Chief Compliance Officer, Chief Risk Officer and Chief Underwriting Officer.
- The Committee may form subcommittees for specialized areas (e.g., cyber fraud, claims fraud).
- Must avoid conflicts of interest in composition and functioning.

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.

Reporting
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.

Fraud Monitoring Unit (FMU),

The FMU is an independent unit, separate from internal audit, to support FMC in discharging its functions and effective implementation of measures suggested by FMC.

Composition of FMU:

FMU shall comprise of Chief Information Security Officer, Manager (legal & compliance), Head - Financial Control, DVP (Claims) and Associate (Risk).

VIII. Co-ordination with Law Enforcement Agencies:

- Fraud is a serious issue which will be dealt in a swift manner by RQBE.
- Cases and instances, wherein sufficient information/proof is available post conduct of investigation, efforts will be taken to ensure that they are reported to the relevant law enforcement agencies, in consultation with the appropriate authority, for initiating action under the criminal law of the land.
- Employees/ Third parties/ Intermediaries, who possess relevant information or are linked to the instant issue, shall be requested to co-operate with the law enforcement agencies in order to facilitate the expeditious completion of the investigation.

IX. Due Diligence

Enhanced employee due diligence is strongly encouraged within RQBE. Its importance is further reinforced during the risk training sessions for employees. Due diligence process should include the following:

(a) For employees during recruitment:

- Disclosure of any conflict of interest situations
- Declarations of civil or criminal records (past and current)
- Background screening at recruitment stage, including character reference checks

(b) For agents prior to appointment:

- Disclosure of any conflict of interest situations
- Declarations of civil or criminal records (past and current)
- Character reference checks
- Corporate searches on bankruptcies, insolvencies, etc. where available

(c) For third parties prior to entering into contract:

- There is a policy to obtain at least 3 quotations, unless not practical with reasons properly documented
- Disclosure of any conflict of interest situations
- Review track record of third parties, including searches on public databases

X. Framework for Exchange of Information:

- Relevant information/findings, collected during investigations and reviews, shall be disseminated within the organization, as may be deemed necessary
- Relevant information/findings shall be shared, with other insurance companies, on a common platform (of General Insurance Council presently) to increase the knowledge repository. Also, wherever deemed necessary, such information/findings shall be sent out over e-mails for the attention of other insurance companies. While sharing the information/findings, it shall be ensured that no personal information of the individuals involved are disclosed
- Information received through the common framework shall be shared with the relevant department and used to strengthen the internal controls framework
- The information obtained from the investigations/ reviews shall be used to carry out risk trainings, wherever necessary

XI. Declaration of Conflict of Interest

- RQBE expects all employees to maximise their full working time and efforts to RQBE's interests and to avoid any activity which may result in a conflict of interest with RQBE's interests.
- All employees, including Directors, are required to make a declaration of any potential conflicts of interest which may arise due to personal, financial or other reasons. This is done annually or when the conflict situation arises.

XII. Code of Conduct Signoff

RQBE's Code of Conduct covers the following guidelines on:

- Employee Conflict of interest
- Dealing honestly with customers (which include insured, agents, brokers and outside suppliers)
- Providing gifts, entertainment and other business courtesies to any customers
- Acceptance of business courtesies from customers or suppliers for procurement
- Dealing with any government or foreign officials

It is against RQBE's policy to:

- Give kickbacks to any customers;
- Contribute or donate RQBE funds, products, services or other resources for any political cause, party or applicant.

All employees are also required to annually sign their acceptance of the Code of Conduct to indicate that they have read through the policy and that they understand the behaviour which is expected of an employee of RQBE.

XIII. Embedding Anti-fraud management

- ***Risk Awareness & Training***

Every employee should have a general awareness of fraud and how he or she should respond if such activity is detected or suspected. This could be heightened through a fraud awareness training on a regular basis to raise their overall awareness. The training should include:

- A clear definition of the types of behaviour which constitute fraud;
- The measures which are currently in place within RQBE to manage the risks of fraud;
- A reminder on the severity of such offences, as well as the consequences if an employee is found guilty of them; and
- An unequivocal statement that such practices will not be tolerated within RQBE.

XIV. Detection, Reporting & Investigation for Employees and Contractors

A developed detection and monitoring system should also be in place to increase the likelihood of detecting fraud within RQBE. This includes:

- Identifying fraud risk indicators for the various areas of business – in the event that an indicator is triggered, a more in-depth investigation and follow-up actions should be taken;
- Post-transactional reviews by personnel unconnected with the business unit in which the transactions were effected; and
- Analysis of management accounting reports to identify suspicious trends.

Employees and contractors should report all actual or suspected fraud matters directly through their line manager, or their two-up manager. Line manager / two-up manager should in turn report to Head-Human Resources

If the employee is not comfortable reporting to his or her line manager, or one of these people is suspected of involvement in the fraud itself, they should contact Head-Human Resources.

The incident report should, at the minimum, comprise the following details:

- Date of the incident;
- Name and identification of the alleged offender;
- Relationship between the offender and RQBE;
- Brief description of the offence;

- Estimated dollar amount involved in the offence; and the
- Recommended management action plan.

Those complaints deemed to be vexatious will be investigated and disciplinary action may be taken and may result in dismissal.

XV. Investigation Response

Following any incident report of fraud, the Head-Human Resources will:

- Inform and update the FMC instances involving internal fraud and provide a monthly report on the developments of the investigation;
- Conduct a thorough investigation of the incident;
- Involve the Internal Audit Team where necessary to commence investigations with the presence of a HR Liaison and an External Liaison as appropriate;
- Notify the relevant local regulatory authorities (including lodging a police report) as necessary;
- Take necessary legal actions to recover lost assets/money or require restitution by defrauding parties as appropriate.

XVI. Fraud Response Plan

RQBE has developed a Fraud Response Plan (FRP) to detect, investigate and report any instances of fraud. The FRP includes the following:

i. Determining the appropriate course of action
ii. Initial reaction to allegations of fraud
iii. Investigation procedure
iv. Managing external relations
v. Recovering assets
vi. Taking the necessary disciplinary action
vii. Taking the appropriate follow-up action

When informed of a fraud, managers:

- should listen carefully and with respect to staff, ensure that every report is treated seriously and sensitively,
- give every allegation a fair hearing.

Managers should obtain as much documentation and information as possible regarding the alleged fraud, including any notes or evidence, and they should reassure staff members that they will be protected and will not suffer any reprisal for having reported allegations made in good faith.

Managers are required to prepare a written report of the details of any suspected fraud that has been reported to them, and provide it to the Head-Human Resources within 5 working days after receiving all information.

Managers should not confront the alleged perpetrator or carry out an investigation themselves. Instead, the matter should be reported immediately to Head-Human Resources. If the Head-Human Resources is not available, then the manager should report it to the CEO.

(a) *Determining the Appropriate Course of Action*

- As a matter of principle, once an alleged fraud is reported to the Head-Human Resources, he/she will disclose all relevant information to the FMC.
- If any of these persons are thought to be involved, then the report should bypass the person.

- The FMC will determine in consultation with the CEO, and the Head-Human Resources, whether the case can be dealt with internally, or whether external involvement is necessary. Any decision made to contact external experts or police have to be recorded.
- A decision to involve an external source will depend on the magnitude and the complexity of the fraud and the individuals involved.
- The FMC will advise the Chief Executive Officer on the involvement of the police in the given case. The final decision to involve the police will be at the Chief Executive Officer's discretion.
- The FMC could seek the advice and require the involvement, as necessary, from the Internal Auditor, the Risk Committee of the RQBE, and any other specialist accountant and financial investigators

(b) *Initial Reaction to Allegations of Fraud*

- The FMC in consultation with Head – Human Resource will act promptly to determine a course of action commensurate with the seriousness of the alleged offence. Appropriate actions could range from taking the individual out of his/her position into another position during the investigation, enforcing paid or unpaid leave, or even suspension. In all cases involving employee fraud, the course of action will be determined in consultation with HR Team and if necessary seek Legal Advice. If the suspected person(s) are allowed to remain on the premises and/or continue with their employment duties, arrangements must be made to keep the person(s) under close surveillance.
- The FMC will ensure that all information in the possession of the suspected individual is secured for investigation.
- The FMC will mitigate the risk of future losses by immediately adjusting procedures in order to protect assets and to preserve evidence, including, if necessary, suspending payments (such as of salary or of invoices).
- Relevant insurers will be notified immediately of any loss or damage to RQBE's insured property.

(c) *Investigation Procedure*

- Depending on the magnitude and the complexity of the fraud, investigations will be either:

  (1) carried out in-house by the Head – Human Resource.

  (2) carried out by external parties such as external audit firms with specialized forensic accounting expertise and access to criminal law expertise;

  (3) carried out based on whatever deemed appropriate by the police. The decision whether to use internal or external investigation services, or a combination of both, will be made by the Chief Executive Officer on the advice of the FMC and Head – Human Resources, with the assistance of local legal counsel where necessary.

- Investigations will be conducted without regard to any person's relationship to the organization, position or length of service. The FMC will keep records of all the actions taken in the investigation for any potential future criminal, civil or disciplinary action.
- The FMC will determine who should not be involved in the investigation to avoid a situation of a conflict of interest for staff members and managers with close working relationships with the individual(s) in question.
- The FMC will ensure that full access of files and computers is granted to the Head – Human Resource and any external body assisting him/her to search the work area in question. All searches are to be conducted in a lawful manner, to ensure that evidence is admissible in court if required. The FMC will keep records of any actions taken or handling of evidence.
- Interviews, if necessary, will be structured and documented as much as possible. The FMC in consultation with Head – Human Resource will develop the procedure, in consultation with the Legal Adviser.

- The Head – Human Resource will issue a report detailing the findings and conclusions of every concluded investigation, including recommendations for future actions within 30 days of reporting of incident to Head – Human Resource for investigation carried out inhouse. For cases involving external parties, the Head – Human Resource shall issue a report within 15 days from the receipt of final reports from the external parties. Results of investigations will be disclosed to and discussed with FMC and anyone with a legitimate need to be involved. This is important as it avoids damaging the reputation of those suspected of wrongdoing and subsequently found innocent, and to protect the Company from potential civil liability and loss of reputation and goodwill.

(d) *Managing External Relations*

- In the case of substantiated fraud, RQBE will take immediate steps to mitigate potential loss of RQBE's reputation and credibility with stakeholders and partners. Where an investigation confirms that an act of fraud was committed, the Chief Executive Officer, in consultation with the FMC, if need be, will disclose the details of the fraud, the assets / resources affected, and the efforts being made to remedy the situation to any stakeholders and partners with an interest in the affected area. This must be done in a timely manner and with great care to be transparent and responsible while not unduly alarming stakeholders or partners.
- In high profile cases of fraud, the Chief Executive Officer will be responsible for managing and monitoring any media response.

(e) *Recovering Assets*

Where RQBE has suffered pecuniary loss or loss of other material assets, efforts will be made to seek restitution from the individual(s) responsible for the fraud. This can be done through the following methods:

- Making arrangements for voluntary payment
- Making deductions from benefits payments or a pension scheme if permitted by law
- Considering an insurance claim
- Taking civil action to obtain a judgment for the loss
- Obtaining compensation orders in criminal cases
- Considering any other appropriate means of recovery

(f) *Disciplinary Action*

Where the Head – Human Resource's investigation reveals that an RQBE staff member has committed a fraud, the Chief Executive Officer, in consultation with the FMC, will pursue disciplinary or legal action as appropriate. Criminal prosecution should be pursued if necessary. Otherwise, depending on the nature of the case, one or more of the following options may be applied, consistent with the perpetrator's relationship with RQBE and the rights and obligations therein under the applicable law:

- Counselling
- Loss of privileges
- Greater scrutiny or increased controls
- Transfer to another area
- Demotion
- Suspension
- Termination
- Immediate dismissal

Disciplinary action could also be brought against supervisors whose failures have contributed to the conduct of fraud or against staff members who deliberately make an allegation in bad faith.

(g) *Follow-up Action*

- Following a case of fraud, the FMC in consultation with CEO will ensure that all managers and staff in the affected area are debriefed on the process and outcome of the investigation. There should also be a follow-up with the individual(s) who reported the initial suspicion of fraud to provide assurance that their claims have been taken seriously.
- Depending on the circumstances, the Chief Executive Officer will consider the need for communication with staff, stakeholders and partners on a larger scale.
- The Chief Executive Officer will ensure that the organization conducts a thorough review of operating procedures in the areas affected by the fraud and that improvements are made where necessary.
- Where applicable, lessons learned should be disseminated throughout the company to strengthen the system of internal control and to foster an anti-fraud culture. A report on actions taken will be submitted to the Risk Management Committee of RQBE.

XVII. Policy Review

This Anti-Fraud Policy shall be reviewed annually to ensure that the contents of the Policy accurately reflect the changing business environment and regulatory requirements within the RQBE.

XVIII. Non-Compliance with this Policy

- Non-compliance with this policy will result in disciplinary action which could include the termination of the employment or agency contract of the errant employee or agent respectively, and/or reporting of the incident to the relevant local authorities as appropriate.
- RQBE reserves the right to pursue legal action(s) against the responsible party to recover any stolen property or assets, or for any exposure it may have to criminal and/or civil liability (including financial penalty or liability for damages) as a result of any acts of dishonesty by employees, agents or any party against RQBE.

XIX. Legislation and Policies and Standards

- Insurance Fraud Monitoring Framework Circular issued by IRDAI
- RQBE Code of Conduct
- RQBE Conflict of Interest Policy
- Fraud Response Plan – Internal Investigation Procedures

XX. Reporting to IRDAI

The statistics on various fraudulent cases which come to light and action taken thereon shall be filed with IRDAI in forms IRDAI_RET_199- FMR 1 and FMR 2 providing details of:

i. outstanding fraud cases; and
ii. closed fraud cases

This should be completed annually within 30 days of the close of the financial year.
Forms FMR 1 and FMR2 are given at **Appendix 2**

XXI. Whistle Blower Policy:

The company has a strong and well defined whistle blower policy and mechanism in place as one of the mitigation measures against the risk of fraud.

XXII. Review process to identify "missed" insurance fraud detection opportunities

Process to identify and analyze missed fraud detection cases, strengthen controls, and update fraud risk management practices across all business lines, including underwriting, claims, distribution, and vendor management.

- FMU is responsible for leading the review process for missed fraud detection opportunities. It will maintain comprehensive records of all reviews, document findings, and prepare detailed reports for submission to the Fraud Monitoring Committee (FMC). FMU also ensures that corrective actions are tracked and implemented effectively.
- FMC will review and approve corrective actions recommended by FMU,

Process Overview

- **Post-Incident Analysis:** After closure of a fraud case, conduct a thorough root cause analysis to determine why the fraud was not detected earlier. Document gaps in controls, monitoring systems, or application of RFIs (Red Flag Indicators).
- **Data Mining & Pattern Analysis:** Utilize historical claims and policy data to identify patterns that were previously overlooked. Re-scan past transactions for anomalies and missed indicators.
- **Cross-Functional Review:** Engage underwriting, claims, legal, and IT teams to review missed cases collaboratively, identify systemic weaknesses, and recommend process improvements.
- **Update RFIs:** Incorporate newly discovered fraud indicators into the Anti-Fraud Policy and detection systems to prevent recurrence.
- **Training & Awareness:** Share insights and learnings from missed cases through emails and broadcast messages to strengthen fraud detection capabilities across the organization.
- **Audit & Compliance:** Schedule fraud-sensitive audits focusing on areas where detection failed. Ensure findings are reported to FMC and Risk Management Committee (RMC) for corrective action.
- **Documentation:** Maintain a **Missed Detection Log** capturing all cases reviewed, gaps identified, and actions taken. Include these findings in the Annual Comprehensive Fraud Risk Assessment.

XXIII. Further Information

Further information can be obtained by contacting the Head – Human Resource.

Appendix 1:

Illustrative List of Insurance Frauds

The potential areas of fraud include those committed by the officials of the insurance company, insurance agents, corporate agents, intermediaries, TPAs or the policyholders. Some of the examples of fraudulent acts or omissions include, but are not limited to, the following:

1. Internal Fraud:

a) misappropriating funds
b) fraudulent financial 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 accounts
j) falsifying documents
k) selling insurer's assets at below their true value in return for payment.

2. Policyholder Fraud and Claims Fraud:

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

3. Intermediary fraud:

a) Premium diversion - intermediary takes the premium from the purchaser and does not pass it on to the insurer
b) Inflating the premium, passing on the correct amount to the insurer and pocketing the difference
c) Non-disclosure or misrepresentation of the risk to reduce premiums
d) Commission fraud - insuring non-existent policyholders while paying an initial premium to the insurer, collecting commissions and annulling the insurance by ceasing further premium payments

4. External Fraud

a. Fake Vendor Setup

- A fraudster creates a fictitious company and registers it as a vendor.
- Submits invoices for services never provided.
- Payments are made because the vendor passed initial checks due to weak onboarding controls.

b. Inflated Billing

- A legitimate vendor colludes with an internal employee.
- Vendor bills for 1,000 units instead of 500 units delivered.
- Employee approves the invoice in exchange for kickbacks.

c. Business Email Compromise (BEC)

- Fraudster hacks or spoofs a vendor's email.
- Sends an email requesting payment to a new bank account.
- Organization processes the payment without verifying the change.

d. Substandard Goods or Services

- Vendor delivers low-quality materials but charges for premium quality.
- Detection is delayed because quality checks are skipped or manipulated.

e. Collusion in Tendering

- Vendor wins contract unfairly, leading to inflated costs.

5. **Affinity Fraud or Complex Fraud**

a. Vendor employee collusion
b. Broker-hospital-customer collusion
c. multiple vendor colluding
d. Insider–Surveyor–Repair Shop Collusion
e. Affinity Group Fraud

Appendix 2:

FMR – 1

Fraud Monitoring Report

Name of the Insurer:

Part I
Frauds Outstanding- Business segment wise *:

Sl. No.	Description of Fraud	Unresolved Cases at the beginning of the year		New cases detected during the year		Cases closed during the year		Unresolved Cases at the end of the year	
		No.	Amount involved (`lakh)	No.	Amount involved (`lakh)	No.	Amount involved (`lakh)	No.	Amount involved (`lakh)
	Internal fraud								
	Distribution channel fraud								
	Policyholder and/or Claims Fraud								

	External fraud								
	Affinity Fraud or Complex Fraud								
	Total								

In addition to the above, irrespective of the category of fraud, details of Cyber / New Age Fraud shall be reported separately in the following table.

Sl. No.	**Brief description of Cyber Fraud (nature of data used to carry out the fraud, modus operandi, etc)**	**Financial Impact**	**Other relevant details**

I

Part II

Statistical details: Age-wise analysis of unresolved cases *

Sl. No.	**Unresolved Cases at the end of the year (age-wise)**	**No. of Cases**	**Amount Involved (` lakh)**
1	30-60 days		
2	60 – 180 days		
3	180 – 360 days		
4	More than 360 days		
	Total		

Part III

Cases Reported to Law Enforcement Agencies

Sl. No.	**Description**	**Unresolved Cases at the beginning of the year**		**New cases reported during the year**		**Cases closed during the year**		**Unresolved cases at the end of the year**	
		No.	**` lakh**	**No.**	**` lakh**	**No.**	**` lakh**	**No.**	**` lakh**
	Cases reported to Police								
	Cases reported to CBI								
	Cases reported to Other agencies (specify)								
	Total								

* Business segments shall be as indicated under IRDAI (Actuarial, Finance and Investment Functions of Insurers) Regulations 2024

CERTIFICATION

Certified that the details given above are correct and complete to the best of my knowledge and belief and nothing has been concealed or suppressed.

Date: Signed/-
Place: Name of the Chief Executive Officer of the Insurer

FMR – 2

Fraud Cases closed during the year

Name of the Insurer:

Sl. No.	Basis of closing a case	Number of cases closed
1.	The fraud cases pending with CBI/Police/Court were finally disposed off	
2.	The examination of staff accountability has been completed	
3.	The amount involved in the fraud has been recovered or written off	
4.	The insurer has reviewed the systems and procedures; identified the causative factors; has plugged the lacunae; and the portion taken note of by appropriate authority of the insurer (Board, Committee thereof)	
5.	Insurers are allowed, for limited statistical / reporting purposes, to close those fraud cases, where: The investigation is on or challan / charge sheet not filed in the Court for more than three years from the date of filing of First Information Report (FIR) by the CBI/Police; or Trial in the courts, after filing of charge sheet / challan by CBI / Police has not started, or is in progress.	

CERTIFICATION

Certified that the details given above are correct and complete to the best of my knowledge and belief and nothing has been concealed or suppressed.

Date: Signed/-
Place: Name of the Chief Executive Officer of the Insurer

 # Closure of Fraud Cases:

For reporting purposes, only the following instances of fraud cases can be considered as closed:

1. The fraud cases pending with CBI/Police/Court are finally disposed of.
2. The examination of staff accountability has been completed
3. The amount of fraud has been recovered or written off.
4. The insurer has reviewed the systems and procedures, identified the causative factors and plugged the lacunae and the fact of which has been taken note of by the appropriate authority of the insurer (Board / Audit Committee of the Board)
5. Insurers are allowed, for limited statistical / reporting purposes, to close those fraud cases, where:
    a. The investigation is on or challan / charge sheet not filed in the Court for more than three years from the date of filing of First Information Report (FIR) by the CBI/Police, or
    b. The trial in the courts, after filing of charge sheet / challan by CBI / Police, has not started, or is in progress.

Insurers should also pursue the CBI for the final disposal of pending fraud cases especially when the insurers have completed the staff side action. Similarly, insurers may follow up with police authorities and/or the court for the final disposal of fraud cases.