Kotak Mahindra General Insurance Company Ltd

Anti-Fraud Risk Management Policy

1) INTRODUCTION

Increasing incidences of frauds affect not only the profitability of companies but also the reputation of the Company. Keeping in view, the ongoing innovative modus operandi adopted by fraudsters, a high level of care and alertness is required at various levels. There is an imperative need to be abreast of the latest strategies used by fraudsters and initiate control measures for timely prevention and detection of frauds across value chain.

This policy is prepared with a view to strengthen the precautionary measures and to make supervision & internal control mechanism more focused and effective.

Kotak Mahindra General Insurance Company Ltd (KGI) has stipulated a number of measures to be taken to address the various risks that it may face as required and stipulated by the regulator.
KGI has set up a Risk Management Committee (RCM) to have an overview of the risk management framework and policies.
In order to provide regulatory supervision and guidance on the adequacy of measures taken by insurers to address and manage risks emanating from fraud, the Authority has also laid down the guidelines requiring insurance companies to have in place the Fraud Monitoring Framework.

2) SCOPE AND CLASSIFICATION OF INSURANCE FRAUDS

Fraud in insurance is an act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties. Amongst other things, this may, for example, be achieved by:

- 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.

In order to adequately protect itself from the financial and reputational risks posed by insurance frauds, the company shall have in place appropriate framework to detect, monitor and mitigate occurrence of such insurance frauds within its company. The policy applies to all insurance transactions and services including e-commerce transactions conducted on the Insurance Self Networking Platform.The company would have in place departmental Standard Operating Procedures (SOP) wherever required and well laid down guidelines which would form the basis for their day to day functioning. The fraud control checks would be a part of the routine controls institutionalised at the departmental level which would facilitate the smooth functioning of the Risk Control Unit. The said framework shall, at the minimum, include measures to protect the insurer from the threats posted by the following broad categories of frauds:

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

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

- **Internal Fraud –** Fraud/ mis-appropriation against the insurer by its Directors, CEO, Manager and/or any other officer or staff member (by whatever name called).

3) FRAUD MONITORING MECHANISM

The Risk Control Unit (RCU) shall ensure effective fraud monitoring by adhering to **preventive** control measures. An indicative list is enumerated below

a) Implementation of Know your customer policy, where applicable
b) Sampling and reference checks of Client proposal
c) Random check of documentation to check unauthorized and tampered documentation.
d) Documentation in all big ticket proposal to be properly vetted and irregularities corrected.
e) Medical Centre seeding.
f) To liaison with all industry for devising preventive measures for guarding the company from attempted fraudulent acts and spurious media attacks on the company's image
g) To conduct regular seeding to ensure that processes are followed and frauds are prevented across functions.
h) To analyse the whistle Blowers and negative referrals to setup measures to avoid fraud in specific areas thus observed and act on the same
i) Mail Monitoring to prevent unauthorized data transfer.
j) Maintaining the privacy and security of data.
k) Regular maintenance of Integrity of the automatic data processing system.
l) Regular Vulnerability Assessment on Internet Applications.
m) Using updated & high quality software for running online portals.
n) Using improved and reliable third party payment processor.
o) Ensuring all websites representing online sales are secured with HTTPS.
p) Regular website scanning for malware and phishing attacks
q) Realtime Website scanning for Malware and Defacement
r) Strong password for Admin/Hosting/Dashboards/Systems.
s) Regular monitoring of SSL certificates.
t) Domain registration with reputed service provider.
u) State of Art Network and Security posture at Perimeter to prevent unauthorized access
v) Carrying out Fraud awareness campaigns

The RCU team shall ensure effective fraud monitoring by adhering to **corrective** control measures. An indicative list as enumerated below

a) Branch Referral investigations in suspected areas for the internal and external customer
b) To keep the management appraised of the negative happening and to take their advice on steps of governance.
c) To take corrective action on processes in conjunction with branches, Sales and Head Office concurrence so that frauds of a specific nature are not repeated.
d) Analysis of customer complaints received to identify areas and rogue channels which are prone to complaints and increase sampling for the areas from which complaints are in large numbers
e) Implementation of an effective concurrent / internal audit mechanism. Conducting regular audits by external certified (CISA/DISA) information system auditor.

4) POTENTIAL AREAS OF FRAUD

The following areas have been identified as high risk areas for fraud:

a) New Business/Renewal
b) Claims Intimation and Settlement
c) Premium collections particularly in cash
d) Cash Embezzlements
e) Payments to vendors
f) Outsourcing Arrangements
g) Data Security

5) CO-ORDINATION WITH LAW ENFORCEMENT AGENCIES

The Company shall take appropriate action for reporting of frauds such as illegal gratification, cash embezzlements, negligence, cheating, forgery, etc. to the appropriate authorities. Appropriate processes shall be set to ensure fraud reporting on timely and expeditious basis.

6) FRAMEWORK FOR EXCHANGE OF INFORMATION.

KGI shall lay down procedures for exchange of necessary information on frauds, amongst all insurers through the General Insurance Council

7) DUE DILIGENCE

KGI shall lay down procedures to carry out the due diligence on the personnel (management and staff)/ insurance agent/ Corporate Agent/ intermediary before appointment/ agreements with them.

8) REGULAR COMMUNICATION CHANNELS

KGI shall communicate on a periodic basis the various learnings to ensure that right behaviour is encouraged and unacceptable behaviour is cautioned against. The communication shall also be done with appropriate levels within the Company to enable dissemination of information

9) FRAUD MONITORING FUNCTION

In order to streamline the system of reporting fraud cases, the following procedures shall be adopted at the various levels in case of fraud/attempted fraud:

a) As soon as a fraud is detected, a flash report prepared by the unit head (branch/HO) should be sent to the respective Functional Head and the Risk Control Unit Head.
b) In case in-depth investigation has to be carried out the RCU team may involve an external party on a need basis.
c) The prime responsibility for timely reporting of frauds is of the unit head.
d) Ensure cases reported are closed through Action taken report. This report has to be filed with RCU Head or CEO as applicable.
e) Summary of fraud review report shall be presented in the Risk Management Committee
f) Details of frauds/attempted frauds in other companies shall also be studied to ensure learning from the same.

10) ANNUAL REVIEW OF FRAUDS

An annual review of the frauds will be conducted and a note will be placed in the Risk Management Committee. The RCM shall also review Anti-fraud policy at least annually. Note on fraud and changes to the policy shall be placed to the Board through the Risk Committee.

11) REPORTS TO THE BOARD BY THE RISK MANAGEMENT COMMITTEE

a) Fraud reporting will be done to the Board through the RCM as per set process.

b) RCU Team shall identify the systemic lacunae if any that facilitated perpetration of the fraud and put in place measures to plug the same.

c) Identify the reasons for delay in detection, if any, reporting to top management of the insurer.

d) Monitor progress on CBI/Police/Judicial bodies investigation and recovery position.

e) Ensure that staff accountability is examined at all the levels in all the cases of frauds and staff side action, if required, is completed quickly without loss of time.

f) Review the efficacy of the remedial action taken to prevent recurrence of frauds, such as strengthening internal controls

g) Give recommendations to strengthen process to prevent such frauds.

12) REPORTS TO THE AUTHORITY

The Company shall file the reports with the regulatory Authority (ies) pertaining to frauds in the format prescribed and within the timeline specified by the Authority (ies).

13) DISCIPLINARY ACTION

If investigation reveals that a staff member or an external party has committed a fraud, KGI will pursue disciplinary or legal action, in consultation with the Legal Advisers where need be.