ICICI LOMBARD GENERAL INSURANCE COMPANY LIMITED

Anti-Fraud Policy

ICICI LOMBARD GENERAL INSURANCE COMPANY LIMITED (the Company) has adopted a 'ZERO TOLERANCE POLICY' towards the commission or concealment of any kind of fraudulent or illegal acts. This Anti-fraud policy (the Policy) covers all employees and officers of the Company. Additionally, this policy covers all vendors, customers, distribution channels and business partners to the extent that any resource of the Company is involved or impacted.

The Policy recognizes the principle of proportionality and reflects the nature, scale and complexity of the business and risks which it is exposed to. Due consideration has also been given to organizational structure, insurance products being offered; technology used, market conditions and evolving patterns of fraud.

1. Objective:

The Insurance Regulator, Insurance Regulatory and Development Authority of India (IRDAI) issued a circular with respect to Insurance Fraud Monitoring Framework on October 09, 2025, applicable to all the Insurers, Reinsurers and Distribution Channels. The circular requires all Insurers to put in place an "Anti-Fraud Policy" duly approved by its Board and also have in place a detailed set of procedural guidelines so as to establish a comprehensive framework in order to deter, prevent, detect, report and remedy fraud risks effectively across the Company.

2. Fraud Definitions:

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.

b. "Red Flag Indicator (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.

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

d. "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.

[Note: The extract of clause 5 sub clause (8) of IRDAI (Protection of Policyholders' Interests and Allied Matters of Insurers) Regulations, 2024 has been reproduced below for ease of reference:

"*Distribution Channels" include insurance agents, intermediaries or insurance intermediaries, and any persons or entities authorised by the Authority to involve in sale and service of insurance policies.*"]

Any other Words and expressions used and not defined in these guidelines but defined in the Insurance Act, 1938 (4 of 1938), Insurance Regulatory and Development Authority Act, 1999 (41 of 1999) shall have the meanings respectively assigned to them in those Acts, Rules, Regulations, Guidelines issued under those Acts, as the case may be.

3. Fraud Classifications:

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 involving internal staff, including employees and / or senior management.

b. Distribution Channel Fraud:
Fraud involving distribution channels.

c. **Policyholder Fraud and/or Claims Fraud:**
Fraud involving any person(s), in obtaining coverage or payment during the purchase, servicing, or claim of an insurance policy.

d. **External Fraud:**
Fraud involving external parties / service providers / vendors etc.

e. **Affinity Fraud or Complex Fraud:**
Fraud involving collusion among one or more fraud perpetrators in the above categories.

In conjunction with the IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025; the Company has a put in place a framework/ guiding principle to draw practical interpretation for amount involved in fraud under various scenarios:

Amount Involved in Fraud:

The amount involved shall be arrived by the nature of fraud;

- Amount in policy related forgery or tampering shall be premium

- In case of claims fraud, which was identified and the claim was repudiated or the policy was voided by the Company, the fraud amount involved shall be the claim reserve insured but the actual loss shall be "Nil"

- If the fraud has been identified post payment of claims, then the total amount paid shall be considered as loss.

- For instances of proven cash/ cheque misappropriation, the amount misappropriated shall be equal to the actual loss

- In case of expense fraud, the actual amount paid shall be the amount of loss

- In case of commission fraud, the actual amount paid shall be the amount of loss

- In case of commission received fraud, the actual amount received is the amount involved in fraud

- In case of expense fraud/ commission fraud identified before payment/ receipt the amount involved should be fraud amount, but the actual loss should be 'NIL'.

4. Fraud Risk Identification, Mitigation and Monitoring:

To mitigate the risk of insurance fraud, the Company shall identify business areas, processes, and departments that are vulnerable to fraud and establish a comprehensive framework. The framework shall provide for the identification, deterrence, prevention, detection, investigation, reporting, and remediation of insurance frauds, including technology-enabled and online frauds related to policy issuance and claims, and shall incorporate defined fraud risk categories, relevant red flag indicators, and adequate controls across all key activities. The detailed processes, roles, responsibilities and delegation of authority for all relevant functions including for identified sensitive posts, escalation mechanisms, investigation procedures, and review mechanisms including periodic assessment to identify any missed fraud detection opportunities shall be set out separately in the Company's procedural guidelines.

5. Fraud Monitoring Committee (FMC):

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

The Operational Risk Management Committee (ORMC) of the Company as specified under the Operational Risk Management Policy shall act as the Fraud Management Committee (FMC) and shall carry out all the functions of FMC as specified herein above.

6. Fraud Monitoring Unit (FMU):

The FMC shall setup a Fraud Monitoring Unit (FMU), independent from internal audit, to support it in discharging its functions and effective implementation of measures suggested by it.

The FMU shall be responsible for facilitating the investigation of suspected frauds, including adherence to defined internal turnaround timelines from identification to closure and remedy, coordination of reporting through designated officer(s), and timely submission of fraud reports. The framework shall also provide for a mechanism to initiate appropriate action in cases of non-compliance with the fraud risk management framework and against identified fraud perpetrators.

The Company shall ensure that the FMU is supported by adequate and appropriate resources, including skilled personnel, systems, and tools, to enable it to carry out its functions effectively, with detailed processes and operating procedures set out in the procedural guidelines.

7. Co-ordination with Law Enforcement Agencies:

To enable timely and expeditious reporting of fraud for the purpose of investigation and prosecution, a process for coordination with the law enforcement agencies shall be formulated by the Company.

8. Exchange Information:

IRDAI has mandated Insurance Information Bureau (IIB) to constitute and implement a Fraud Monitoring Technology Framework (FMTF), which will help insurers to prevent fraud in insurance sector. The objective of the FMTF is to help industry to combat fraud and protect policyholders and all stakeholders.

IIB shall maintain an industry wide database (hereinafter referred to as "caution repository") which will facilitate timely threat intelligence sharing; on attempted/ suspected and reported fraudulent activities within the insurance industry. In order to implement the caution repository, IIB has been mandated to adopt unique identifier. In consultation with the Life Insurance council and General Insurance council, IIB has to implement unique identifier, procedure and timelines for reporting necessary details to maintain caution repository.

In order to facilitate IIB's implementation of FMTF, the Company shall share necessary details of distribution channel, hospital, third party vendor and fraud perpetrator blacklisted with IIB, from time to time.

9. Due Diligence:

Process shall be formulated for carrying out due diligence on personnel (management and staff), distribution channels, vendors and TPAs before appointing them or entering into an agreement with them.

10. Framework for Cyber or New Age Fraud:

In order to safeguard against evolving cyber frauds risks or threats across various insurance business lines, the Company shall establish, implement, monitor and strengthen a robust cybersecurity framework. The specifics of cybersecurity framework are covered in the procedural guidelines.

11. Framework for Reinsurance Business:

IRDAI Guidelines 2025, mandates that Insurers carrying on reinsurance business or ceding insurance business can reduce their exposure to fraudulent claims by understanding the fraud risk management systems the counterparties have in place.

Accordingly, these guidelines apply mutatis mutandis with respect to reinsurance business. Further, IRDAI suggests that Insurers in reinsurance business shall implement the framework prescribed by the host jurisdiction of their parent entity or the framework outlined here, whichever is more comprehensive.

Accordingly, the Company shall implement the appropriate framework, as applicable.

12. Creation of Fraud awareness:

Fraud prevention and early detection are dependent on a strong culture of awareness across the organization and among stakeholders. The Company shall establish procedural guidelines and structured initiatives to promote fraud awareness among employees, senior management, board members, distribution channels, policyholders, and the general public.

13. Whistle Blower Protection:

The Company shall provide a secure and confidential whistle blower mechanism to report suspected or actual frauds in good faith, with assurance of anonymity and protection against retaliation, in accordance with the Company's Whistle Blower Policy and applicable laws.

14. Reporting and Review Mechanism:

The FMC shall quarterly report to the Audit/Risk Committee of the Board of Directors on the events of fraud identified, established and eliminated.

The Company shall also submit to the Authority, an annual report of the statistics on various fraudulent cases which comes to light and action taken thereon in appropriate forms prescribed by the Authority. The annual report must be submitted within 30 days of close of the financial year.

In the event of fraud committed by distribution channels registered by IRDAI, the Company shall promptly escalate and report the matter to IRDAI without delay.

Further, the Board of Directors of the Company shall review the anti-fraud policy on at least an annual basis and at such intervals as may be considered necessary.