

INDUSIND GENERAL INSURANCE COMPANY LIMITED (“IGICL”)

ANTI-FRAUD POLICY

FEBRUARY, 2026

VERSION 1.0

ANTI-FRAUD POLICY

Index

Sr. No.	Particulars
1	Introduction
2	Definitions
3	Scope and classification of Frauds
4	Fraud Monitoring Committee
5	Fraud Risk Monitoring Framework
6	Fraud Investigation Procedure
7	Cyber or New Age Fraud
8	Insurance Information Bureau (IIB)
9	Framework for Reinsurance business
10	Framework for Distribution Channels
11	Training, Education and Awareness
12	Consequences of failure to comply with the Policy
13	Annual Review and Update of Anti-Fraud Policy
14	Mandatory Reporting Protocols

1. Introduction

Fraud poses a significant threat to all segments of the financial sector, particularly in the insurance industry, which is inherently vulnerable to fraudulent activities. Such fraud affects the company's reputation, goodwill, and finances and can severely undermine the confidence of policyholders and shareholders. Customers also feel the direct impact, as they must shoulder the burden of increased premiums resulting from efforts to offset losses caused by fraud. Ultimately, the overall cost of fraud is significant for both the industry and consumers.

To provide regulatory oversight and guidance on the adequacy of measures taken by insurers to address and manage risks associated with fraud, the Insurance Regulatory and Development Authority of India (IRDAI) issued a guideline having reference No. IRDA/IID/GDL/MISC/112/10/2025 dated 09/10/2025. This guideline requiring insurance companies to implement a Fraud Monitoring Framework with a zero-tolerance approach to fraud.

This Policy shall come into effect from **1st April 2026** (01/04/2026) in line with the commencement date of the IRDAI Insurance Fraud Monitoring Framework Guidelines, 2025.

2. Definitions

2.1 Insurance Fraud (herein after referred 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, suppressing, or not disclosing one or more material facts relevant to any decision/ transaction, financial or otherwise.
- Abusing responsibility, a position of trust or a fiduciary relationship.

2.2 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.

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

2.4 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.

2.5 Fraud Monitoring Unit (FMU)

The Fraud Monitoring Unit (FMU) alias Risk Containment Unit (RCU) at the Company is a team of professionals functionally independent of Internal Audit, responsible for supporting the Fraud Monitoring Committee (FMC) in discharging its functions and ensuring effective implementation of fraud risk management measures as recommended by the FMC.

2.6 Incident Database

The Incident Database shall be a repository of all persons convicted of, or attempting, insurance fraud across the industry, maintained and shared through the Insurance Information Bureau (IIB) and internally used for underwriting, claims assessment, and vendor/intermediary due-diligence decisions.

2.7. **The Company** means IndusInd General Insurance Company Limited.

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

3. Scope and classification of Frauds

Fraud in the insurance industry can manifest in various forms and involve multiple parties, such as company officials, agents, corporate agents, intermediaries, third-party administrators (TPAs), Key workshops, policyholders, and external entities.

The fraudulent activities can occur across pre-sales and post-sales covering key departments. These procedures focus on prevention, identification, and mitigation of frauds.

A) Internal Fraud Fraud involving internal staff, including employees and/or senior management. Examples include:

- a. Financial Misappropriating, unauthorized diversion or misuse of funds and deliberate manipulation of financial statements for personal gains.
- b. Fraudulent transactions which may involve stealing or misusing cheques, discounting cheques, fraudulent electronic Transfers, and submitting inflated expense claims etc.
- c. Corruption and favouritism resulting in granting special prices or favour's to customers or suppliers in exchange for kickbacks etc.
- d. Document falsification / Forgery.

B) Distribution Channel Fraud

Fraud perpetuated by distribution channel (an insurance agent/ Intermediary/ Insurance intermediary, and any persons or entities authorised by IRDAI to involve in distribution and services of Insurance policies.

C) Policyholder Fraud and Claims Fraud: Fraud involving any person(s), in obtaining or making payments during the purchase, servicing, or claim of an insurance policy.

Examples include but not limited to:

- (a) Document falsification / forgery or sharing of incorrect information for taking a policy.
- (b) Manipulation of facts.
- (c) Inflation/ exaggeration of claims.
- (d) Presenting duplicate or inflated invoices during claim settlement.

D) External / Third-Party 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.

4. Fraud Monitoring Committee

4.1) The Company has established

A) Fraud Monitoring committee (FMC) who are responsible for operationalizing the fraud risk management framework within the insurers and oversee activities, to ensure fraud deterrence, prevention, detection, reporting and remedying.

At Company level, FMC shall comprise of;

- (i) Chief Financial Officer,
- (ii) Chief Risk Officer,
- (iii) Chief Human Resources Officer,
- (iv) Chief Compliance Officer

Apart from the above it shall include senior representative from relevant departments.

The FMC may form sub-committees, as required, for its effective functioning (e.g., separate subcommittees for claims fraud, underwriting fraud, cyber fraud, etc.) and shall avoid conflict of interest.

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

4.2) Functions of the FMC: The FMC Shall, inter alia:

4.2.1. Recommend and update Fraud risk measures: The FMC regularly recommends, and updates measures for fraud risk management across various functions, based on evolving experiences and trends.

4.2.2. Oversee prompt response: to ensures a swift and effective response to any instance or suspicion of fraud.

4.2.3. Maintain detailed records: The committee is responsible for documenting all relevant information pertaining to instances of fraud.

4.2.4. Facilitate collaboration and intelligence sharing: The committee fosters coordination with industry peers, law enforcement agencies, regulatory bodies, and collaborates in pursuing and sharing information on known fraud schemes and perpetrators.

4.2.5. Conduct Annual Comprehensive Fraud Risk Assessment (ACFRA): To leads an annual comprehensive fraud risk assessment across business lines using insights from past incidents, emerging trends, and red-flag indicators etc.

4.2.6. Identify framework improvement areas: Based on assessments, the FMC identifies areas of improvement and updates the fraud risk management framework accordingly.

4.3) Reporting requirements of the FMC: The FMC shall;

4.3.1. Submit quarterly reports to the Risk Management Committee (RMC), detailing activities, findings, recommendations, and financial impact of fraud on the Company.

4.3.2. Submit reports of Annual comprehensive Fraud Risk Assessment (ACFRA) to the Board through the RMC.

4.3.3. Additionally, report internal frauds to the Audit Committee.

4.4) The Company had established a Fraud Monitoring unit (FMU), operationalized through the Risk Containment Unit (RCU), to support the FMC in discharging its function and ensuring effective implementation of measures suggested by the FMC.

- (i) Red flag indicators and Fraud Risk Identification: A structured framework for Red Flag Indicators (RFIs) shall be maintained and reviewed quarterly. RFIs shall be aligned and updated based on emerging fraud patterns. Automated systems shall trigger alerts for high-risk proposals, claims, and transactions. The RFIs along with monitoring control and primary functions related are detailed in the annexure to this policy.
- (ii) Fraud monitoring procedures are tailored based on the type of fraud, the stakeholders involved, the complexity of the business, and the overall economic environment.
- (iii) The Policy holders and claim frauds require both reactive and proactive approach for mitigating fraud risk. Hence the company builds certain check points at various stages to detect moral hazards, appropriate disclosures, and due diligence. Suspicious claims are triggered to the Risk containment unit for a detailed investigation and submission of the final report.
- (iv) Dedicated email ID for Reporting Suspected Frauds: The company has a dedicated email address, alert@indusindinsurance.com, for reporting suspected fraudulent activities.
- (v) Due Diligence: The Company has put in place processes with respect to due diligence on employees, intermediaries, insurance intermediaries and vendors (including TPAs), The HR Department shall conduct due diligence of employees at the time of on- boarding. The due diligence of intermediaries, insurance intermediaries, vendors, Hospitals, Garages etc. shall be carried out by the respective departments. All employees shall be required to confirm their adherence to this Policy and declare any Conflict of Interest, once in a year.
- (vi) Internal Control Framework: A strong internal control framework is the strongest deterrence to Fraud. The business/ operations, support groups review various systems and controls on regular basis to remove gaps if any and strengthen the internal process of the company.
- (vii) Framework for Exchange of Information: The Company shall report identified frauds to IRDAI in compliance with applicable regulatory requirements and shall also report such frauds on the FRM

Portal developed by the GI Council or any other portal as directed by the regulatory body. Additionally, the Company shall fully cooperate with law enforcement authorities, take appropriate disciplinary actions, and implement awareness programs. The Fraud Management Risk (FMR) report shall be submitted to the RMC and the Board on a quarterly basis.

- (viii) Co-ordination with law enforcement agencies: The Company's authorized officials will regularly engage with law enforcement agencies to file complaints in relevant fraud cases. They will also provide all necessary information and support required by the authorities during the investigation.

5. Fraud Risk Monitoring Framework

Fraud monitoring procedures need to be tailored based on the type of fraud, the stakeholders involved, the complexity of the business, and the overall economic environment.

- a) The company targets a zero tolerance for fraud and the Management retains primary responsibility of placing appropriate fraud risk management framework to enable it to deter, prevent, detect, report and remedy insurance frauds.
- b) The Risk Management Committee (RMC) of the Company shall be responsible for effective implementation and oversight of the fraud risk management framework.
- c) The company shall have a dedicated email address alert@indusindinsurance.com, for reporting suspected fraudulent activities.
- d) This Policy is reviewed on annual basis and upon material changes by the Board to ensure alignment with regulatory changes, emerging fraud risks, and operational requirements.

6. Fraud Investigation Procedure

RCU shall be responsible for investigating and handling all cases highlighted as Frauds. It shall take prompt and appropriate action with respect to such frauds to remediate the circumstances giving rise to occurrence of such frauds.

Investigation & Evidence Gathering:

- Conduct detailed investigations into potential fraud incidents while ensuring no conflict of interest. In case of conflict of this Policy with any internal Standard Operating Procedures, it will have an over-riding effect and shall prevail upon. Subsequently the user department should take steps to eliminate such conflict.
- Further, it shall also analyse the data based on frauds detected during field investigations.
- RCU shall investigate the cases as per the TAT defined under the RCU SOPs or elsewhere as defined under the respective governing regulations
- RCU shall investigate all such cases and render report to the Fraud Monitoring Committee (FMC) duly highlighting the breaches of conduct, process and system etc. Report shall also highlight the financial implication, if any.
- Impacted departments shall be responsible for implementing the decisions by FMC, wherever applicable and report back the closure to FMC.
- The company shall have a separate Whistle-blower Policy which shall safeguard / protect the Whistle-blower.

7. Cyber or New Age Fraud

- To collaborate with the cybersecurity risk management team to establish and implement robust cybersecurity framework, which in turn supports cyber fraud risk management
- Continuously monitor and strengthen systems and processes for fraud risk management, such as incident databases, customer verification, and access control.

8. Insurance Information Bureau (IIB)

The Framework for reporting and utilization of triggers shared by Insurance Information Bureau (IIB):

The Company adheres to all regulatory requirements mandating the sharing of information with the Insurance Information Bureau (IIB). This includes providing details of distribution channels, allied hospitals, and individuals or entities that have been blacklisted due to confirmed involvement in fraudulent, unethical, or non-compliant activities.

- (i) The Company shall maintain an internal caution list repository that captures details of vendors, intermediaries, and entities involved in confirmed or suspected fraud.
- (ii) Fraud risk management processes are designed to ensure that entities with a history of fraudulent activities are prevented from engaging with our company across any distribution or service channel.
- (iii) System integration efforts shall be undertaken to ensure that the Company can receive, process, and act upon alerts, risk indicators, fraud patterns, and watch-list information generated through IIB's threat intelligence system.

All relevant functions shall collaborate to ensure completeness, accuracy, and timely reporting of information to IIB, as well as effective utilization of insights obtained from IIB.

9. Framework for Reinsurance business

Fraud with regards to Re-Insurance can be considered as below:

- **Risk Description:** Forged Cover notes / Signed Re-Insurance slips submitted by brokers.
- **Control Description:** Verify the genuineness of Reinsurance placement by thorough examination of documents and confirmation from Reinsurers should be obtained about Signed Line confirmation & actual Premium Receipt confirmation and coverage authenticity from the Reinsurer.

Entire Risk Control Matrix is explained in Reinsurance Facultative/ Treaty Placement Process.

10. Framework for Distribution Channels

Establish a zero-tolerance, end-to-end framework to deter, prevent, detect, report, and remedy fraud in intermediary operations, including solicitation, onboarding, servicing, claims support, commissions, incentive programs, and digital journeys. All intermediaries/insurance intermediaries engaged in

distribution and/or servicing of Insurance policies, including TPAs and any outsourced distribution partner put in place internal policies procedures and controls to deter, prevent, detect, report and remedy frauds, including:

Distribution channels those not covered above shall comply with the Company's anti fraud policies, procedure and controls. Whenever there is a suspicion of Fraud which may also impact the Company, the same shall be informed to the Company providing all relevant details.

11. Training, Education and Awareness

Training and awareness of the Staff are vital for strengthening fraud preventive efforts and developing an anti-fraud risk awareness culture within the organization.

It should be developed by imparting to staff the necessary knowledge to identify, report & refrain from indulging into fraud. Periodic training programmes shall be conducted, and awareness be created among employees/ intermediaries to combat insurance frauds. Hence case studies on frauds, communication of Anti-fraud emailers and training module at the time of employee induction are various tools at the disposal of Company for creation of Anti-fraud culture within the Company and awareness to its customers, agents & third parties via various mediums.

12. Consequences of failure to comply with the Policy:

The Company expects all its employees to act in full compliance with this Policy in conjunction with the Code of Conduct, Whistleblower Policy and such other policies in a manner consistent with the highest ethical standards. This Policy and its relevant provisions shall be adequately publicised and made known to all concerned including employees, agents, intermediaries and other channel partners.

Any employee found to have been involved in a fraudulent activity or other misconduct or to have failed to report a known or suspected instance of Fraud will be subject to disciplinary action up to and including termination. Furthermore, such conduct of the employees or other parties if found to be in violation of the law then it may result in civil or criminal action.

Failure to adhere to this Policy may result in appropriate actions pursuant to this Policy

The Policy shall be hosted on the intranet of the Company with the objective of creating awareness amongst the employees and an excerpt of the same shall be put up on the website of the Company for the consumption of intermediaries and policy-holders to counter insurance frauds.

13. Annual Review and Update of Anti-Fraud Policy

The Anti-Fraud Policy shall be reviewed and updated annually by the Board to ensure alignment with regulatory changes, emerging fraud risks, and operational requirements. The review shall include delegation of authority, investigation timelines, resource allocation for FMU, and whistle-blower protection measures.

14. Mandatory Reporting Protocols

The Company shall file annual Fraud Monitoring Reports with the IRDAI in Form FMR-1 (as prescribed in Annexure I of the IRDAI Insurance Fraud Monitoring Framework Guidelines, 2025) **within 30 days of close of the financial year** (i.e., by 30 April).

All confirmed frauds shall be reported to law enforcement agencies promptly. Fraud involving registered distribution channels shall be escalated to IRDAI without delay.

Annexure: Red Flag Indicators and Monitoring Controls

Classification of Fraud	Red Flag Indicators and Monitoring Controls	Remarks for coverages
Policyholders & Claim Fraud	Close Proximity Claims	Motor & Health Claims
	Fake / Manipulated Documentation	Motor & Health Claims
	Mis-represented claim information	Motor & Health Claims
	Reimbursement claims from Network hospital post Cashless denial	Health Claims
	Multiple Diagnosis and recurring non-surgical incidents	Health Claims
	Claim from Negative list of Hospitals / Garage	Motor & Health Claims
Affinity fraud	Premium Siphoning: Identification / tracking of unauthorised links / website on internet having Company's name	All LOBs Sales and UW
Internal fraud	Commission Siphoning: Employee / Relatives details (PAN, contact details of self/family matched with Agent's details	All LOBs Sales and UW
	Negative / bypass penny drop cases pertaining to motor & health claims	Claims
	Irregular Patterns of employee expense reimbursement	All employees
Internal / Distribution / Affinity fraud	Refund Siphoning: Avoidance of Penny drop process.	All LOBs

Please note that parameters for the aforesaid triggers are dynamic and would vary depending on the evolving use of any particular method(s) and hence are not prescribed here; the FMU shall highlight the same to the FMC periodically, which shall review the same alongwith the aforesaid RFIs

Product segment-wise RFIs and procedures are already defined in the SOPs.