



UNITED INDIA INSURANCE COMPANY LIMITED



UNITED INDIA INSURANCE COMPANY LIMITED

FRAUD RISK MANAGEMENT POLICY

(VERSION 2.0)



Table of Contents

Sr. No.	Contents	Page No.
1.	Introduction	5
2.	Objective	6
3.	Scope	6
4.	Definition	6
5.	Classification	7
6.	Fraud Risk Management Framework	8
7.	Fraud Prevention, Detection, Mitigation and Monitoring Strategies	8
8.	Reporting	11
9.	Roles & Responsibilities	12
10.	Risk Appetite	13
11.	Benefits accruing from the Implementation	13
12.	Challenges	13
13.	Review of the Policy	14
14.	Sum-Up	14
	Annexure A - Standard Operating Procedures	15
	Annexure B – Fraud Prevention and Detection Procedures	17
	Annexure C – Format for Reporting of Fraud	19



Fraud Risk Management Architecture





FRAUD RISK MANAGEMENT POLICY

1. Introduction

Backdrop

Financial Fraud poses a serious risk to all segments of the financial sector including Insurance Sector. In addition to financial implication, increasing trend of frauds reduces consumer and other stakeholders' confidence; and can affect the reputation of individual insurers as well as the insurance sector as a whole. It also has the potential to impact the very economic stability of the organisation. It is, therefore, required that United India Insurance Company Ltd. understand the nature of fraud and take steps to minimize the vulnerability of their operations to fraud.

Regulatory Dimension

- Insurance Regulatory and Development Authority (IRDA) vide circular IRDA/SDD/MISC /CIR/ 009/ 01/2013 dated 21st January 2013 has laid down the guidelines requiring insurance companies to have in place a comprehensive Fraud Monitoring Framework which includes developing an Anti-Fraud Policy.
- The revised guidelines issued by IRDAI on the Corporate Governance vide circular ref. no, IRDA/F&A/GDL/CG/100/05/2016 dated 18th May 2016 provides that Insurers are well advised to
 - i. Formulate a Fraud monitoring policy and framework for approval by the Board.
 - ii. Monitor implementation of Anti-fraud policy for effective deterrence, prevention, detection and mitigation of frauds.
 - iii. Review compliance with the guidelines on Insurance Fraud Monitoring Framework dated 21st January, 2013, issued by the Authority.

The guidelines also reiterate Whistle Blower Policy which has to be in place as per clause 12.

- Further, in March 2017 IRDAI has issued guidelines on Insurance E-Commerce vide circular ref. no. IRDA/INT/GDL/ECM/055/03/2017 dated March 09, 2017 wherein clause 18 provides for fraud detection measures in e-commerce activities undertaken by the company.
- As provided in the above mentioned clause, our Company's Insurance Self-Network Platform (ISNP) shall have a pro-active fraud detection policy for the e-commerce activities which is approved by our Board of Directors.
- The policy shall amongst other things include the following areas:
 - i. Manner of detecting and identifying frauds
 - ii. Follow-up mechanism for prosecuting persons who committed fraud
 - iii. Cooperation amongst market participants to identify frauds



- iv. Building a database of those committing frauds and sharing with other market participants

2. Objective

- The Policy aims at preventing, detecting, monitoring and mitigating occurrence of insurance fraud in the Company by developing effective processes and building equally effective fraud monitoring framework in this respect.
- The Company is committed to conducting business in an environment of fairness and integrity, and will strive to eliminate fraud from all operations. The Company adopts a “Zero-Tolerance” approach to fraud and will not accept any dishonest or fraudulent act committed by internal and external stakeholders.
- To comply with regulatory and legal requirements in respect of fraud risk management.

3. Scope

- The framework applies to any fraud or suspected fraud in United India Insurance Company, involving employees, customers, vendors, suppliers, contractors and intermediaries like insurance agents, corporate agents, brokers, panel TPAs, panel surveyors, panel advocates or any other external agency who have a business relationship with United India
- To have in place, a policy for outsourcing third-party services in order to control risks relating to third-party service providers.
- Develop a policy in relation to whistle-blowers which includes protection of whistle-blowers and complainants, and treatment of any information received as confidential.
- The Company would also ensure deployment of proactive fraud detection measures to protect its e-commerce activities.

4. Definition

There is absence of commonly accepted definition of fraud therefore, we resort to IRDAI Circular ref no. IRDAI/ SDD/ MISC/ CIR/ 009/ 01/ 2013 on Fraud Monitoring Framework dated 21 Jan 2013, according to which “Fraud” in Insurance means 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:

- i. Misappropriating assets;
- ii. 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;
- iii. Abusing responsibility, a position of trust or a fiduciary relationship



5. Classification

Though it is possible to classify insurance frauds in many ways but to begin with and for uniformity sake we, again resort to the same IRDAI circular which seeks to classify insurance frauds as under:

Internal Fraud: Fraud/ mis-appropriation against the Company by its Director, Manager, employee and/or anyone else (by whatever name called). Some of the examples of fraudulent acts/omissions, under this category, include, but not limited to, the following-

- Misappropriating funds
- Fraudulent financial reporting
- Stealing cheques
- Overriding decline decisions so as to open accounts for family and friends
- Inflating expenses claims/over billing
- Paying false (or inflated) invoices, either self-prepared or obtained through collusion with vendors
- Permitting special prices or privileges to customers or granting business to favoured vendors, for kickbacks/ personal favours
- Forging signatures
- Removing money from customer accounts
- Falsifying documents
- Selling Company assets at below their true value in return for personal benefit

Policyholder Fraud/Claims Fraud: Fraud against the Company in the purchase and/or execution of an insurance product, including fraud at any time during the term of the policy and at the time of making a claim. Some of the examples of fraudulent acts/omissions, under this category, include, but not limited to, the following-

- Staging the occurrence of incidents
- Reporting and claiming of fictitious damage/loss
- Medical claims fraud
- Fraudulent Claims
- Exaggerating damages/loss

Intermediary fraud: Fraud perpetuated by an Insurance agent /Intermediaries/Third Party Administrators (TPAs) and service providers against the Company and/or policyholders. Some of the examples of fraudulent acts/omissions, under this category, include, but not limited to, the following-



UNITED INDIA INSURANCE COMPANY LIMITED

- Premium diversion-intermediary takes the premium from the purchaser and does not pass it to the Company
- Inflates the premium, passing on the correct amount to the Company and keeping the difference
- Non-disclosure or misrepresentation of the insurance risk to reduce premiums
- Commission fraud - Insuring non-existent policyholders or seeking wrongful commissions, by any other means.

6. Fraud Risk Management Framework

The Company seeks to establish and maintain a robust framework to provide reasonable assurance that dishonest acts are prevented or promptly detected and acted upon, which have been reinforced through this Policy and outlines the procedures in relation to prevention, detection, responding, monitoring, reporting and eventually, based on the learnings, reinforcing the systems, processes and operations.

In order to ensure effective control and monitoring, the company has Board Sub-Committee on Risk Management, named as RMC and an internal Fraud Risk Management Committee (FRMC), to be constituted by CMD from time to time. Nodal Officer nominated by CMD will be the designated person to coordinate with ERM department for implementation.

7. Fraud Prevention, Detection, Mitigation and Monitoring Strategies

Based on an analysis of risk, costs and benefits, the Company shall control both internal and external fraud risks by:

- Implementing fraud monitoring systems for risks that are evaluated as high as per the risk assessment methodology;
- Detection, mitigation, Monitoring and reporting on fraud;
- Monitoring compliance with regulations;
- Joining hands with G I Council in its efforts aimed at fraud risk management; and
- Creating Awareness among staff about fraud detection, mitigation, monitoring, and management.

In managing fraud risks, the Company shall remain committed to the highest ethical standards in its dealings with customers and all other stakeholders.



Creating Awareness

Nodal Officer in coordination with ERM Department shall create awareness about insurance frauds, their adverse potential impact and prevention/detection strategies, among the employees of the Company/business intermediaries/policyholders/other agencies dealing with the company, by conducting seminars, workshops or by other means of communication.

Internal Manual

- All departments should have a standard operating procedure manual/guidelines which includes a framework for handling frauds.
- This would also include the methodology for documentation and reporting of the frauds identified/detected.
- An internal committee may be constituted by CMD for periodic review of internal manuals/guidelines.
- Preparation of fraud risk management manual for Company as a whole for all departments/work processes

Sourcing of Information on Potential Frauds and Incidents

Information on potential frauds and incidents can be obtained from various sources, including:

- Internal and External Audits and Inspections
- Vigilance reports/complaint
- Whistle-blowing reports
- Complaints to Regulator/Authorities
- Customer Grievance
- Internal Reviews of operations/processes
- Experiential learnings in the areas of transfer policies
- Reconciliation matters and deviations therefrom

Coordination with Internal Audit and Vigilance Departments

- The ERM Department shall hold quarterly meetings with the Internal Audit and Vigilance department to ascertain compliance with the said procedures by the operating offices.
- The two departments shall be advised to specifically report major procedural lapses and systemic issues observed which could facilitate perpetration of frauds or render the operations vulnerable to frauds.



Preventive Mechanism

- ERM Department shall work with all the departments concerned to define and establish controls to detect and prevent frauds.
- Appropriate notices will be included in the insurance contracts/ relevant documents/ standardized MOUs to caution potential/ existing clients /intermediaries about the deleterious consequences of submitting a false statement and/or incomplete statement, forged documents, misrepresentation/mala fide action of any nature and consequence.

Due diligence of Personnel and Intermediaries

Due diligence on personnel and business intermediaries is a key preventive action in a Fraud Risk Management policy.

- ERM department shall facilitate the HR department and other business verticals to lay down procedures (for example, designing due diligence reporting format) to carry out the due diligence, before recruiting the employees and agents.
- Based on the learnings, similar checks may be extended to the other intermediaries and specific insurance service providers.

Deployment of Technology

- Advances in Information Technology and emergence of Big Data solutions have made it possible to deploy data analytics tools and predictive models for fraud detection in insurance transactions which seeks to examine the relationships between items like people, places and events. IT department shall examine deployment of suitable technology solutions for fraud detection and prevention in our operations.
- The enormous amounts of data now available can be sifted to detect patterns indicative of fraud that even a few years ago might have been undetectable.
- Algorithms can be developed to identify information applicable to fraud cases, and as data is added, these algorithms can become more accurate. Advancement in computing and data science are likely to be major tools in respect of fraud control and monitoring.
- The Company seeks to consider engaging services of experts in the field and then develop in-house expertise.

Building Fraud Risk Profiles and Data base

- ERM department shall facilitate the building of profiles of potential frauds for each specific function/department.
- All stakeholders and domain decision makers shall contribute to building the risk profiles.



- Prepare a database on internal and external fraud for monitoring purposes and for enhancing the efficiency of insurance fraud risk management.

Strengthening the internal control mechanism

Control framework is the backbone of Anti-Fraud mechanism and it is essential that the controls remain current and effective at all times. Internal Audit is a useful source of information on the effectiveness of controls.

- ERM department shall work closely with Internal Audit to continually assess the effectiveness of the Anti-Fraud controls.
- ERM department shall also work with various departments to facilitate periodic review of controls in their key locations/departments.
- All weak or ineffective controls shall be addressed on priority.
- A specific and separate report in respect of vulnerability of systems/controls can be devised and sought from IAD/Vigilance teams after each inspection
- Consideration of a special system audit, at regular intervals, by engaging experts in the field and then development of in-house expertise

It is important to share the details of new controls implemented in a particular office/department, with other departments/offices to allow them to assess if their own local circumstances warrant this additional new control.

Employees to comply with FRM Policy

A copy of FRM policy to be shared with each and every employee/officer of the Company with specific advice for due compliance by each one of them. In the same communication, we also seek their inputs on the policy and its effectiveness.

Fraud trigger points, detection and prevention procedures

Fraud trigger points, detection and prevention procedure are provided in the Annexure A (illustrative) and Annexure B.

8. Reporting

Internal Reporting

- The ERM Department shall collect the information relating to policyholders and intermediary type of frauds (from the operating offices, IAD & vigilance as also the technical departments at HO), analyze, classify and report along with action taken to the RMC on **quarterly basis**.



UNITED INDIA INSURANCE COMPANY LIMITED

- ERM Department shall put in place required procedure and format for reporting by the said stakeholders.
- ERM department shall also make out advisories on a regular basis to the domain departments/verticals on the systemic changes that need to be effected to arrest/prevent/detect early frauds.
- ERM team to specify events and sources of internal and external insurance fraud risks, which include any of its operations that may have potential to substantially affect company's income, capital fund, reputation, or the very existence.

External Reporting

- Wherever cases are to be reported to local law enforcement agencies, it is the responsibility of respective operating office to do so, in consultation with concerned Regional In-charge. However, where the CBI or other central agencies are involved, CVO in consultation with CMD will initiate appropriate action.
- CRO to coordinate, in consultation with FRM Committee, reporting and sharing of data to GI Council or such other forums to create database for the benefit of industry as a whole

Reporting to Regulator

The reports, as advised by the Authority, shall be filed by the ERM Department as per the periodicity prescribed by the Authority/ Regulator, based on the inputs provided/reported by the various departments/operating offices/IAD/vigilance department. The formats, in this regard, shall be shared with these stakeholders to enable them to report to the ERM department.

A compliance report shall also be filed with the RMC on submission of such returns to the Authority.

9. Roles and Responsibilities

Fraud Risk Management - Roles & Responsibilities

1. The Board of Directors is responsible for defining the appetite for Fraud Risk and setting the tone and direction for the management of fraud risk in the Company.
2. Risk Management Committee shall maintain oversight of the management of fraud risk through periodical reporting by the CRO.
3. ERM Department shall be responsible for:
 - a) Implementing the Fraud Risk Management Policy and supporting the business units and departments in setting up the necessary controls and processes.
 - b) Periodically testing the controls established by the operating offices and departments, with the help of Internal Audit Department.



UNITED INDIA INSURANCE COMPANY LIMITED

- c) Gaining assurance on the effectiveness of anti-fraud controls through audit reports/inspections carried out by the Internal Audit and Vigilance Departments.
 - d) Monitoring the level of fraud risk against the Risk Appetite and implementing remedial actions wherever necessary.
4. Operating Offices and HO Departments shall be responsible for identification, monitoring and reporting of frauds in their day to day activities.
 5. Each employee working in the Company and every individual/organisation/entity dealing with the Company shall comply with the norms laid down in this policy. Non-compliance shall be deemed violation of terms and conditions of employment /engagement or terms and conditions of contract (as the case may be) and shall be dealt with as per the Company's disciplinary procedures/terms of engagement or terms of the particular contract(s) or the law as applicable and appropriate.
 6. All employees/officers are responsible to bring to the notice of their supervising officers/management about any fraud detected, as soon as it comes to their notice, in the prescribed format (Annexure C). It is the responsibility of employees/officers to ensure that within their span of control all reasonable and necessary steps are taken to prevent fraud and necessary action taken in case of reasonable suspicion of occurrence of a fraud or detection thereof.
 7. The CRO shall drive the Fraud Risk Monitoring Function across the domains and report at regular intervals to the Risk Management Committee (RMC) as well as the Board.
 8. The CMD will constitute a Committee called 'Fraud Risk Management Committee' and nominate a Nodal Officer as per the terms of the procedures annexed herewith.

The procedure to identify, detect, investigate and report the frauds is described in Annexure B.

10. Risk Appetite

The Company's appetite for Internal/External Fraud is expressed in the Risk Appetite Statement.

11. Benefits accruing from Implementation of the Policy

It is opined that following a proper implementation of the FRM Policy, the anti-fraud mind-set would be established within the Company and every employee would contribute to fraud-proof the Company.

The benefits accruing to the Company would be far out-weighting the incremental cost that would be incurred in implementation of the policy.

12. Challenges

Fraud Risk Management is a necessity which cannot be denied but while implementing



the same, we need to be aware about some inherent challenges and find ways to mitigate the same.

- It involves substantial cost and efforts yet may not provide immediate return or gains
- Fear of loss of reputation
- To match with rapidly evolving technology and complexity, more particularly, with respect to emerging cyber risk

13.Review of the Policy

The FRM Policy shall be reviewed-

- At least, once a year,
- Mid-term review in case of any new regulatory direction or guidelines

The revised policy to be placed before Risk Management Committee and Board of Directors for their approval

14.Sum-up

At the end of the day, fraud prevention and detection in the Company is not the responsibility of the risk team or that of internal audit alone but it is a part of the overall corporate risk management strategy. For a comprehensive fraud management framework to work successfully there has to be an appropriate blend of the right policies and procedures, appropriate preventive and monitoring structures, robust fraud detection and response mechanism supported by an appropriate communication strategy.



Annexure A

Fraud Risk Management Policy

Standard Operating Procedures

Fraud trigger points (Illustrative)

I. Fraud can happen at underwriting or claims stages.

- Close proximity claims
- Unreasonable Delay in reporting the accident
- Misrepresenting material facts to make claim payable
- Documentary Frauds of different nature for different purpose
- Suspicious-looking or handwritten receipts for repairs or replacement of covered property. Corrections in receipts.
- Medical documentation that appears to be altered or fraudulent.
- Damages to vehicle exaggerated, non-existent, pre-existing
- Multiple claims under the same policy or successive policies
- Alterations made to the policy without sufficient/proper authorisation

II. Fraud can also perpetuated by Intermediaries.

- An unscrupulous insurance agent might collect premiums from a customer without passing them along to the company. The consumer believes that their premiums are being properly handled while the insurance company thinks the policyholder is not paying their premiums and, therefore, cancels or not renews the consumer's policy. If the policyholder does not receive an insurance ID card or a copy of your policy in a timely manner, this could be an indication that the premiums have not been paid to the insurance company
- Intermediaries assuring clients coverage different from what has been negotiated with the insurer.
- Fake insurance documents carrying the company's logo.

III. Internal Frauds

- Fraudulent transfer of Assets (Fixed Assets, Land, Investment Assets, etc.,) of the Company by the employee.



UNITED INDIA INSURANCE COMPANY LIMITED

- Misappropriation of funds by Cashier or others who handle cash/cheque
- Exaggerated/ false bills for expenses like LTS etc.,
- Transfer of business between development officers /intermediaries without appropriate authorisation
- Payments made on the basis of photocopies of bills
- Misuse of cheques
- Accepting gratification other than legal remuneration/favour from clients / vendors.

Fraud Detection

1. Exception reports to be generated through IT
2. Data analytics tools may be deployed to see the pattern in order to detect frauds.
3. Escalation matrix to be in place when fraud is detected.
4. Investigation mechanism to be strengthened.

Fraud Prevention: Fraud can be prevented by:

1. Following a robust internal control mechanism with maker checker controls.
2. Imbibe an anti-fraud culture in the organisation
3. Obtaining proposal forms complete in all respects– all required details should be filled in.
4. Internal Manual to be updated and circulated
5. Internal audit to be strengthened and trained to detect fraud due to lapses in the systems so that such lapses can be plugged immediately.
6. Periodical reconciliation of bank accounts.

REVIEW

The SOP will be reviewed and updated as per the experience gained over the period.



Annexure B

Fraud Prevention and detection procedures

1. **Placing the policy on the Intranet and Website:** The Fraud Risk Management Policy will be placed on the Intranet and the Website (to enable outsiders to inform fraudulent activities to the nodal officer) of the company immediately on its approval by the Board
2. **Nomination of Nodal officer:** A senior level officer shall be nominated as the Nodal Officer to receive the information and take necessary action under the policy. The nodal officer shall report to the CRO of the company. The name of the person nominated as nodal officer shall be put on the website.
3. **Fraud Risk Management Committee:**
 - **Constitution:**
 - FRMC shall be constituted by CMD from time to time.
 - FRMC shall meet once in a quarter to discuss the matters relating to Fraud Prevention and monitoring.
 - The Nodal officer shall be the convenor of Fraud Risk Management Committee.
 - **Responsibilities:**

FRMC is responsible to have mechanism -

 - to devise the FRM Policy /& whistle Blower policy and periodically review the same
 - to identify the departments /areas potentially prone to fraud
 - to design the procedures for reporting, investigating and for taking action against the persons committing fraud
 - for designing modules for creating awareness among employees to identify red flags
 - for recovery of the loss from the persons committing fraud against the company
 - to coordinate with the Internal Audit and Vigilance mechanism in the company
 - to report to the RMC and Board
4. **Notification of fraud to the Nodal Officer:** Any outsider(s) or employees(s) who is in the knowledge or come across any fraud /fraudulent practices committed by an intermediary or policyholder or employee can notify the same through any Operating office(s) or to the Nodal Officer at Head Office, directly, if he deems it necessary. Suggestion box shall be kept at HO and all ROs, initially. Subsequently after gaining experience suggestion box shall be placed at the DOs.



UNITED INDIA INSURANCE COMPANY LIMITED

5. **Notification in Writing:** All such information shall be notified in writing to Nodal Officer giving complete information and the *modus operandi* of the instances of fraud. If the issue has already been investigated by the Operating office(s), then such investigation report shall also be forwarded to the nodal officer. No action shall be taken on anonymous/ pseudonymous complaints and such complaints shall be filed.
6. **Further Investigation:**
 - The Nodal Officer or the FRMC may decide to further investigate the matter by engaging professional investigators or rely on the report submitted by the operating offices.
 - Wherever, employees are involved the Nodal Officer shall refer the same to the Vigilance department for further investigation and action.
 - Wherever the case relating to outsider or employees has to be referred to CBI/ Law enforcing authorities, the nodal Officer shall route the same through the CVO.
7. **Initiating action and Recovery of pecuniary Loss:** Reporting of such cases to local law enforcement agencies and initiating recovery process is responsibility of respective operating office in consultation with concerned Regional In-charge. However, where CBI or other central agencies are involved, CVO in consultation with CMD will initiate appropriate action.
8. **Reporting:** The Nodal Officer is responsible to file periodical returns to the Authority/RMC/Management and the Board as prescribed in the extant regulations/guidelines.
9. **Rights of Nodal Officer:** The Nodal Officer is authorised to take original records from any operating office /take copies /or emails/telephone calls or other communication and such other records and interrogate such persons as he may decide for the purpose of establishing the fraud committed.
10. **Creating Awareness:** The Nodal Officer, in coordination with ERM Dept., shall implement the modules suggested by the FRMC to create awareness among the employees and officers in fraud detection and mitigation.



UNITED INDIA INSURANCE COMPANY LIMITED

ANNEXURE C

UNITED INDIA INSURANCE COMPANY LIMITED
REGISTERED OFFICE : 24, WHITES ROAD, CHENNAI

FORMAT FOR REPORTING OF FRAUD

Name /Designation and address of the reporting person	
Business Segment (like Health/Motor etc.)- Policy number/claim number if available.	
Details of Fraud (Complete information and Modus Operandi/distinct pattern if any, of the instance of fraud)	
Name of the person alleged to have committed the Fraud	
Supporting documents a) If the issue has already been investigated by the operating office, investigation report to be enclosed. b) Any other document in support of the instance of fraud. c) If it is taken up with Law enforcing authorities like police etc., the details thereof d) If employee related, whether reported to vigilance department.	
Amount involved (Rs.) Amount recovered, if any	



UNITED INDIA INSURANCE COMPANY LIMITED

Corrective steps taken if any (any system corrections / procedural enhancements may be explained.)	
Any other details to be specified	

Place :

Date :

Signature