
# The New India Assurance Company Ltd

## Corporate Anti- Fraud Policy

Version – 3.0/2026

| | |
|---|---|
| **Title: Corporate Anti-Fraud** | |
| **Prepared by:** ERM Dept. | **Date:** 22/04/2026 |
| **Reviewed by:** Board | **Last Updated date:** 22/04/2026 |
| **Approved by:** Board | **Effective date:** 22/04/2026 |
| **Process Owner:** ERM Dept. | **Review- timelines: Yearly** |

**Version Control**

| Version | Date of Issuance | Version |
|---|---|---|
| 1 | 01/07/2013 | CORP. ANTIFRAUD POLICY 2013 V1.1 |
| 2 | 03/02/2018 | CORP. ANTIFRAUD POLICY 2018 V1.2 |
| 3 | 09/08/2019 | CORP. ANTIFRAUD POLICY 2019 V1.3 |
| 4 | 11/02/2022 | CORP. ANTIFRAUD POLICY 2019 V1.3 |
| 5 | 09/02/2024 | CORP. ANTIFRAUD POLICY 2019 V1.3 |
| 6 | 19/05/2025 | CORP. ANTIFRAUD POLICY V2.0 |
| 7 | 22/04/2026 | CORP. ANTIFRAUD POLICY V3.0/2026 |

# Contents

## 1] Introduction:

The New India Assurance Co. Ltd. (NIA), established in 1919, is India's premier multinational general insurance company. Committed to making insurance easy to understand and accessible, NIA offers a range of user-friendly digital platforms to facilitate insurance purchases and claims processing. With its nationwide network of offices, NIA further enhances accessibility. As a multinational general insurance company, it operates in 25 countries and is headquartered in Mumbai, India.

The New India Assurance Company Limited has been a cornerstone in the general insurance sector, dedicated to spreading insurance awareness and mobilizing resources for the welfare of the masses. Recognizing the potential risks of fraud in the insurance industry, the company has established a robust Corporate Anti-Fraud Policy to safeguard its financial systems, resources, and the integrity of its operations.

## 2] Preamble:

The New India Assurance Company Limited has been playing a significant role in spreading the general insurance business amongst the masses and in mobilization of people's money for the welfare of the masses.

The New India Assurance Company, in the course of its business may encounter possible fraud, intended to gain advantage for the party committing the fraud or for other parties.

This can take many forms and may be perpetrated by any party involved in insurance, e.g. staff, intermediaries, claim adjusters, third party claimants, service providers, policyholders, etc. In addition to causing undue financial loss for the Company, frauds have the potential to reduce consumers' and shareholders' confidence and also affect the reputation of the company.

In order to protect its financial systems, resources, assets, the integrity of its employees and intermediaries and above all Policyholder's welfare, the Company had established a Corporate Anti-Fraud Policy as a part of Fraud Monitoring Framework in accordance to IRDAI Guidelines ref: IRDAI/IID/GDL/MISC/112/10/2025 dated Oct 09, 2025

In the light of the foregoing, it is imperative to provide regulatory supervision and guidance on the adequacy of the measures to be taken by the Company to address and manage risks emanating from fraud. To establish an independent Fraud Risk Management framework across the company, The New India Assurance Co Ltd. (The Company) following principles of Corporate Governance has revised the Corporate Anti-Fraud Policy (hereinafter called the Policy) to prevent (to the extent possible) detect, monitor and mitigate occurrence of fraud in the Company. It would facilitate the development of controls which will aid in the deterrence, detection, prevention and management of fraud against the Company. Hence, this Corporate Anti-Fraud Policy has been reviewed and is being published herewith for study, wider publicity and in spirit implementation.

## 3] Objective and Scope of the policy:

The Policy titled as Fraud Risk Management Policy also known as "Corporate Anti-Fraud Policy" on records, aims at providing a singular focus on the Fraud Prevention and Management function. Hence, the sole purpose of the policy is to keep on record and provide directions to the Company for deterrence, prevention, detection, mitigation, reporting and rigorous follow up of the frauds. This would be applicable to all the offices of the Company read in conjunction with related operational guidelines/instructions issued by the Company from time to time. This policy is also an enabling document for effective investigation in fraud cases and for prompt as well as accurate reporting of fraud cases to the appropriate regulatory and law enforcement authorities including Insurance Regulatory and Development Authority of India. In succinct, the policy inter alia intends:

i. To provide ample understanding of "What Fraud is" and its implications
ii. To create a "Fraud Awareness" and "Fraud Prevention Culture" in the Company and to send across a message to all its stakeholders as well as public at large that frauds fall within "Zero Tolerance Policy" of the Company.
iii. That Company will be on proactive path to deal with frauds through an integrated policy of Fraud Risk Management.

## 4] Definitions and Classification of Fraud:

Commission of "Fraud" is a wilful act committed by an Individual(s)/Entity(ies) – by deception, misrepresentation, suppression, cheating or any other fraudulent or any other illegal means, thereby, causing wrongful gain(s) to self or any other individual(s) and wrongful loss to the Company.

Insurance Regulatory and Development Authority of India (IRDAI) defines fraud in its Insurance Fraud Monitoring Framework Guidelines. According to these guidelines, 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**

The IRDAI Circular referred at the outset above recognizes that company typically face prospects of fraud into below mentioned 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.
f. **Cyber or New Age Fraud**: Cyber or new age frauds are defined as any fraud carried out using digital or new age technologies.

It can reasonably be stated that the Company can expect that a fraud could be perpetrated against it by any of the following acting alone or in combination with another but are not limited to the following:-

a. Employee(s), ex-employee(s)
b. Persons engaged for work or assignment on temporary/ad-hoc/contract/daily-wage basis and/or their individual employees/representatives.
c. Advisor(s), consultants and similar providers of professional expertise including Surveyors/Valuers/Loss Adjusters, Lawyers, Investigators and/or their individual employees/representatives
d. Vendors, suppliers of any goods or services to the Company (including IT hardware/software suppliers and support and maintenance providers).
e. Third Party Administrators (TPAs) and/or their individual employees/representatives' Customers/clients of the Company and/or their individual employees/representatives
f. Agents and/or their individual employees/representatives
g. Brokers and/or their individual employees/representatives
h. Shareholders etc.

### Examples of Insurance Frauds:

The following are some typical examples of internal, policyholder, intermediary and claims frauds that are likely to appear in course of transaction. It is equally pertinent to point that below listed frauds are only illustrative/ indicative and does not intend to be exhaustive for the purpose of this Policy:

i. Wilful suppression of facts /deception in matters of appointment, in submission of reports of any nature to the Company, in any recommendations or making such recommendations because of which a wrongful gain is made to any person/organization/entity and/or a wrongful loss is caused to the Company or the Public exchequer.
ii. Forgery or unauthorized alteration of any document (including Certificate of Insurance, Insurance Policy /Endorsement/Cover note/Declaration etc.) or correspondence or account belonging to the Company.
iii. Forgery or unauthorized alteration of cheques, bank drafts or any other financial instruments
iv. Misappropriation of funds, securities, supplies or other assets by fraudulent means.
v. Selling insurer's assets at below their true value in return for payment.
vi. Making fraudulent/false noting in official records of the Company.

vii. Utilizing Company funds for purposes for which the said funds are not intended. ix. Effecting major material departures from standard laid down Tendering procedures or norms without clear written authorizations and "speaking orders".
viii. Unauthorized or illegal use of confidential information (e.g. profiteering as a result of insider knowledge of company activities).
ix. Frauds perpetuated by intermediaries may include non-disclosure or misrepresentation of the risk resultantly rendering coverage other than assured to the client. An agent might collect the premium from a customer without passing it to the company leading to non-issuance or renewal of a policy. Fake insurance documents carrying the façade of Company's document.
x. On the claims and underwriting side frauds may include close proximity cases related, staging of occurrences, damages to vehicles shown exaggerated, non-existent and preexisting. Multiple claims under the same policy or successive policies. Alteration made in the policy without sufficient/proper authorization, misrepresentation of material facts to make the claim payable.
xi. Loss of intellectual property (e.g. disclosing confidential and proprietary information to the outside parties).
xii. Conflict of interest resulting in actual or exposure to financial loss.
xiii. Vendor related frauds.
xiv. Where a policyholder or applicant either deliberately misrepresents or deliberately fails to disclose material facts at policy inception (that would materially impact either the terms & conditions applied to a policy of insurance, or the issue/renewal decision itself) for financial gain.
xv. Creating dummy policyholders, paying the initial premium to the company, collecting the commission, and then annulling the insurance by stopping further premium payments.
xvi. Any other act that falls under description of 'fraudulent activity'.

## 5] Fraud Risk Management Framework (Evaluation of Risks, Implementing Anti-Fraud Processes and Controls)

5.1 The Company follows a zero-tolerance approach to fraud and maintains a fraud risk management framework to deter, prevent, detect, report, and address insurance frauds. The Company shall establish and maintain a robust framework to identify, assess, mitigate, monitor, and report fraud risks across all lines of business and operations.

5.2 The Risk Management Committee (RMC) shall be responsible for effective implementation and oversight of the fraud risk management framework.

5.3.1 Fraud Monitoring Committee

A Fraud Monitoring Committee (FMC) which 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

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

5.3.2

Composition of the FMC: The FMC:

a) shall be headed by a KMP and include senior representatives from relevant departments, such as underwriting, claims, legal or any other department as deemed necessary.

b) May form subcommittees, as required, for its effective functioning.

c) Shall avoid conflicts of interest in its composition and functioning.

5.3.3

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.

5.3.4
Reporting Requirements: The FMC shall:
a) submit quarterly reports to the RMC on its activities, findings, and recommendations including the financial impact of fraud on the company.
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.

5.4 Fraud Risk Identification, Mitigation and Monitoring

The Company shall establish and maintain a robust framework to identify, assess, mitigate, monitor, and report fraud risks across all lines of business and operations.
The Company has detailed Fraud Response and Monitoring Procedures outlining the approach to handle confirmed or suspected frauds involving employees, intermediaries, vendors, policyholders, or any other stakeholders, whether internal or external.

a. Fraud risks shall be identified and assessed based on business lines, activities, past experience, emerging trends and applicable regulatory guidance. Appropriate preventive, detective and corrective controls shall be implemented to mitigate identified fraud risks across all processes.
b. The Company shall clearly define responsibilities and establish a delegation of authority for all relevant functions, including identified sensitive posts, to ensure accountability and effective control over fraud risk management.
c. Functional Heads shall be responsible for maintaining, implementing, and strengthening systems, processes, and controls within their respective areas, as well as for conducting due diligence on the various entities or individuals such as personnel, distribution channels, TPAs, vendors, and consultants with whom the Company engages, before entering into agreements or appointments, to minimize the occurrence of fraud and mitigate its impact in a timely manner.
d. Red Flag Indicator (RFI) shall mean a warning sign that may indicate potential fraud. The Company shall define, embed RFIs within relevant operational and analytical processes which will be periodically reviewed for continued relevance and effectiveness. (Refer Annexure B for the illustrative list of RFIs)
e. Employees and other stakeholders shall report suspected or detected frauds promptly through the incident reporting mechanism..
f. The Company shall maintain effective monitoring and review mechanisms, including fraud incident databases, fraud sensitive audits, trend analysis of distribution channels, continuous vendor monitoring and review of customer grievances to detect and prevent fraud.
g. The company shall monitor recovery of fraud related losses and undertake continuous improvement initiatives, including review of missed detection opportunities and fraud awareness programs, to promote a culture of zero tolerance to fraud.
h. The Company shall ensure confidentiality of fraud investigations, provide protection to individuals who report fraud in good faith, and take appropriate action in cases of non-reporting or malicious complaints and against the fraudsters.
i. The Company also has an established Whistle-blower Policy to safeguard individuals reporting fraudulent activity while protecting the interests of the organization.
j. The Company shall coordinate with law enforcement agencies for timely fraud reporting and follow-up. Reporting to relevant agencies will be done on a case-to case basis

### 5.5 Cyber or New Age Fraud

The Company shall prevent such frauds by implementing a robust cybersecurity framework, continuously monitoring and strengthening systems and processes for Fraud Risk Management across all functions

### 5.6 Insurance Information Bureau (IIB)

The Company shall participate in the IIB Fraud Monitoring Technology Framework, share required fraud related data including blacklisted distribution channels, hospitals, vendors and fraud perpetrators, as appropriate. The Company shall report as per the prescribed format within timelines prescribed by IIB and utilize industry wide threat intelligence to prevent fraud.

### 5.7 Framework for Reinsurance business

The company shall manage fraud risk in reinsurance business by conducting due diligence on reinsurers, monitoring their fraud controls, and ensuring compliance with applicable regulatory requirements and our internal fraud risk framework, wherever relevant, thereby maintaining governance and integrity standards

Although Management has the prime responsibility for performing the Fraud Risk Management function it is also critical that employees at each level are involved in the fraud risk management process having knowledge, influence and control over significant business processes. Individuals from throughout the organization with knowledge, different skills and perspectives (e.g. accounting/finance/claims/underwriting/ vigilance/internal audit/legal/HR/compliance etc.) are to be involved in the fraud risk management process. Key pillars of the process are:

The Enterprise risk management framework of the company encompasses the processes in respect of risk management of frauds and the same framework is to be considered as Fraud Risk Management framework of our company. Company will strive to remain proactive in reducing the fraud opportunities by:

a. Identifying and measuring fraud risks
b. Taking up steps to mitigate the identified risks
c. Implementing and monitoring appropriate preventive and detective internal controls along with adopting deterrent measures.

## 6] Roles and responsibilities:

### 6.1 Fraud Monitoring Unit (FMU):

Fraud is a critical risk facing an enterprise that needs to be managed/ controlled/mitigated by the Company in an organized way. To achieve this end, a dedicated Fraud Monitoring Unit as a part of Enterprise Risk Management (ERM) department has been set up in the Company. Chief Risk Officer shall steer the Fraud Monitoring function, will develop, implement and maintain a Fraud Risk Management framework to achieve their objective of being a fraud resilient organization that is committed to preventing, detecting and responding to fraud and report at regular intervals to the Risk Management Committee as well as the Board.

The key roles and responsibilities of FMU are mentioned below:

i. To formulate the Corporate Anti-Fraud Policy and review it periodically.
ii. Develop and implement a Fraud Risk Management (FRM) framework.
iii. Carry out periodic fraud risk assessments to identify departments/areas prone to fraud.
iv. Suggest suitable anti-fraud controls for risks identified in the Fraud risk assessment review.
v. Carry out procedures to test the effectiveness of the FRM framework as part of a review Program. The review program and procedures will be developed/modified in consultation with the CRO. Based on the observation noted in the review, the FMU will put in place controls for prevention, detection and mitigation of fraud.
vi. To design the modules for creating fraud awareness amongst the employees and public.

vii. Obtain half yearly declaration from the head of departments/operating offices regarding identification and reporting of fraud, if any, in their functional/geographical jurisdiction.

viii. Co-ordination with the Internal Audit and Vigilance Departments in the Company to report to Board about the matters related to the Department.

ix. Perform analysis of relevant data to identify potential fraud trends/areas and build fraud triggers.

x. Collate the fraud data from various departments/operating offices in the specified format and submit to CRO for reporting to the appropriate authority on yearly basis.

xi. Nodal Officer: The ERM SPOCS who are the Nodal Officers posted at various Offices; Operating units will function as extended arm of the FMU.

FMU department will undertake activities from time to time to create awareness about the frauds by issuing the Advisories', having brief Workshops, Wallpapers, Mailers. The Primary aim of this activity is prevention and mitigation of frauds.

### 6.2 Chief Risk Officer:

i. To review the Anti-Fraud policy periodically.

ii. Responsible for the functioning of Fraud Monitoring Unit and for escalating all reported cases of suspected fraud / misconduct, as appropriate within the organisation.

iii. Review the fraud risk assessments to identify areas prone to fraud and suggest anti-fraud controls.

iv. Review the identified fraud data obtained from Head of Departments/Operating offices and submit the fraud monitoring reports in the specified format to regulatory authority.

v. Report the fraud cases and results of other fraud monitoring activities conducted to the Risk Management Committee.

### Alignment of Functions of Vigilance, IAD & Operational Units vis-a-vis FMU:

i. The Company already has a well-defined system and procedure for tackling internally originated frauds, i.e. Frauds committed by Company's own employees by means of Vigilance Department. Vigilance Department itself has the avowed intent to be proactive in implementing "Preventive Vigilance" by means of making system-studies, anticipating fraud-prone areas, spreading awareness and sensitizing drives, conducting surprise checks and so on. It is also expressly tasked with investigating of suspected frauds by own employees acting by themselves or in concert with outside elements and with bringing established cases of fraud (with evidence) to suitable conclusion – whether disciplinary proceedings or any other appropriate punitive measure. The Department functions in the light of the Conduct Discipline and Appeal Rules (CDA Rules).

ii. The Company also has an Internal Audit Department (IAD) that audits transactions and accounts which on occasion reveal commission of frauds.

iii. All operational units (RO's/CBO's/KBO's/BO's/Hubs) as well as HO Departments, apart from preventing frauds emanating internally and referring such instances detected to the appropriate authority, are expressly responsible for being vigilant against potential frauds by intermediaries, policyholders and other outsiders, being aptly placed for this role and responsibility by virtue of their day-to-day work. The latter responsibility is to be exercised by means of adherence to laid down norms and best practices and exercise of due diligence.

iv. Suitable action (including prosecution of any civil or criminal proceedings as per law) following suspicion of or detection of fraud by such outside entities /persons shall be the domain of the operational units/ departments The function or intent of the Fraud Monitoring Unit (FMU) is naturally not to take over or even overlap the functions of these departments, but to act in coordination with them.

## 7] Fraud Incident Reporting:

### 7.1 Internal Reporting

i. Company shall formalize the information flow amongst the various operating offices/employees as regards insurance frauds.

ii. Any outsider(s) or employees(s) who is in the knowledge or come across any fraud/irregular fraudulent practices being committed by an intermediary or policyholder will notify the same through any operating office (s) to the Fraud Monitoring Unit (Email id fmc@newindia.co.in) at Head Office. It is the bounden duty of every officer/employee of the Company to provide to the management information which is within his/ her knowledge about any fraud or potential fraud.

iii. Every instance of attempted or detected actual fraud (regardless of whether it has caused actual financial loss to the Company, at that juncture or not) shall be reported by the affected department /operational units to the overseeing office /department /executive. Where the fraud involves or is reasonably suspected to involve an employee of the Company, it shall be reported to Vigilance Department at RO or HO as applicable. Every such instance of fraud shall also be reported to the FMU email id fmc@newindia.co.in by the department/Operational unit.

iv. Fraud Incident Reporting shall capture crucial information regarding each fraud incident, including description, fraud perpetrator details, loss and recovery estimates, control implications and already action taken. **Annexure A** is attached with the policy for reporting frauds.

v. Vigilance Department and IAD shall share with the FMU, details of frauds detected after sensitive /confidential investigation processes are over.

vi. The FMC shall, through the ERM Department, report periodically to the Risk Management Committee of the Board.

### 7.2 External Reporting

i. Company shall file annual returns with Authority (IRDAI) in forms FMR-1 placed in Annexure I within 30 days of close of financial year.

ii. 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.

## 8] Investigation:

i. No employee or third party is permitted to independently conduct investigations, interviews, or interrogations related to any actual or suspected fraudulent activity, unless explicitly instructed by the FMC.

ii. Depending on the case's sensitivities (as determined by the FMC), the Committee may choose to appoint an independent investigation agency to handle the case comprehensively.

iii. FMC will keep Internal Audit informed about all cases referred to FMC for investigation and take their inputs during investigations as required.

iv. FMC shall present its findings to Risk Management Committee.

v. The fraud investigation shall consist of gathering sufficient information about specific details.

## 9] Compliance:

Each employee working in the company and every individual/organisation/entity dealing with the Company shall endeavour in every possible manner to 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.

## 10] Recovery of Fraud Loss:

Upon detection of a fraud, the Operating Units or Departments concerned should make vigorous effort possible to recover the loss amount involved. Loss mitigation action will include systematic action which includes recovery from concerned customer /outsider and would include initiating legal action including filing of recovery suits wherever feasible.

## 11] Creation of data bank of frauds repository:

Another area is to create a data bank on frauds and take steps to avoid occurrences of the same fraud in future. This data bank/pool shall be analysed periodically which will act as knowledge repository of policy responses.

## 12] Creating Awareness- Among employees, customers & public:

i. The Policy recognizes that proper awareness is the pivot of fraud prevention measures and efforts. The Company should aim at continuously educating its employees, customers and the general public on fraud prevention and enlist support and participation in fraud prevention.

ii. This Corporate Anti-Fraud policy document shall be published on the website of the Company.

iii. Customers and the Public should be sensitized by means of advertisements, detailed do's and don'ts published on website or in posters and flyers or other communications sent along with policies /renewal notices etc.

Employees will be equipped with adequate tools to combat frauds by means of training programs (either special training sessions or by inclusion in induction training or sectorial training modules), regular communication through circulars, newsletters etc. is also to be resorted to.

## 13] Co-ordination with Law Enforcement Agencies:

i. Perpetration of a Fraud or an attempt to commit a fraud is a serious issue, which will be dealt with swiftly by the company.

ii. Instances where sufficient evidence of fraud is obtained post conduct of internal investigations / review would be reported to the relevant law enforcement agencies in consultation with the appropriate authority.

iii. Employees / Intermediaries shall cooperate with any law enforcement agency to facilitate the expeditious completion of investigation.

## 14] Framework for Exchange of Information:

i. Relevant information collected by the FMU and Vigilance department from its review and monitoring activities would be disseminated within the organisation as deemed necessary.

ii. This information would be shared on a common platform with other insurance companies to increase the knowledge repository. The information would be shared in a manner that no personal information about the individuals involved would be disclosed.

iii. Similarly information received from others in a common forum would be shared with the relevant department so that existing Fraud Risk Management Framework may be tested for resilience to these risks and additional controls may be put in place in case required.

## 15] Due Diligence:

FMC will ensure that there are adequate procedures in place at various departments for carrying out due diligence on the various entities/ people with whom the Company carries out its business before entering into agreement/ or their appointment, for e.g. staff recruitment, insurance agents, corporate agents, intermediaries, TPA, vendor engagement etc.

## 16] Whistle Blower Policy:

The company has a well-defined Whistle Blower policy and mechanism in place as one of the measures of mitigation of Fraud Risk.

## 17] Custodian of the Policy:

The Chief Risk Officer of the Company will be the custodian of the Policy.

## 18] Review of the Policy:

This Policy will be reviewed annually and approved by the Risk Management Committee. The final approval will be provided by the Board of Directors. The Committee may, if feel necessary, direct the FMC to modify any portion of the Policy suitably or consider the suggestion(s) submitted by the FMC for modifications to the Policy during such annual reviews.

## Annexure A

Report on Actual/Suspected Frauds:

| | |
|---|---|
| FROM: | TO: |
| Name of RO/LCBO/TP HUB: | Deputy General Manager |
| Office In charge: | Fraud Monitoring Cell |
| Code No: | The New India Assurance Co. Ltd |
| Address: | 87, MG Road |
| | Head Office-400001 |
| Date: | Tel: 022-22708523, IP: 100422 |

| | | |
|---|---|---|
| 1 | Details of the RO/LCBO/DO/BO/MO (where fraud was committed):<br>a) Name of in charge<br>b) Code no.<br>c) Address<br>d) Contact details | |
| 2 | a) Name of insured (on whom fraud was committed)<br>b) Line of activity (individual/corporate/dealer/financier) | |
| | Fraud committed by:<br>a) Employees of the company<br>b) Intermediaries (surveyors/investigators/agents/brokers/TPAs/doctors/advocates/financiers/other third parties, etc.)<br>c) Fraud committed by employees in collusion with outside parties/intermediaries, etc. | |
| 3 | a) Area of operation where the fraud has occurred<br>b) Whether fraud has occurred within the office/outside the office | |
| 4 | a) Nature of fraud (like fake policy/policy alterations/bogus claims/exaggerated claims/misuse of APD accounts/misappropriation of cash/bogus hotel/ITS bills/misuse of passwords, etc.)<br>b) Series of events (one event leading to multiple events)<br>c) Whether computer used in committing the fraud; if yes, furnish details | |
| 5 | a) Date of occurrence<br>b) Date of detection<br>c) How the fraud came to light<br>d) Reasons for delay, if any, in detecting the fraud<br>e) Date on which reported to next higher authority<br>f) Reasons for delay, if any, in reporting to next higher authority, after detection | |
| 6 | Any event that may lead to fraud, though suspected but not reported | |

| | | |
|---|---|---|
| 7 | Brief history/modus operandi | |
| 8 | If fraud committed by staff/intermediaries/any other outsiders:<br>a) Policy number/claim no/license no/case no<br>b) Whether reported to higher authority/vigilance authority<br>c) Whether any investigation has been carried out<br>d) Whether any complaint has been lodged with the police/CBI<br>i. If yes, branch of police station<br>ii. FIR no<br>iii. Present position of the case<br>iv. If not reported to police, reasons thereof | |
| 9 | Action taken/status of the case | |
| 10 | Steps taken/proposed to be taken to avoid such incidents | |
| 11 | a) Total amount involved<br>b) Total amount recovered<br>c) Extent of loss to the company<br>d) Provision to be provided, if any | |
| 12 | Suggestions, if any for action | |

Date:

Place:

Signature OF BO/DO/RO-
In charge with
Name & Designation

## Annexure B - Illustrative list of RFIs at various stages

**1. Proposal Stage RFIs**

- Proposal form submitted with incomplete, inconsistent, or altered information.
- Discrepancies between customer declarations and supporting documents.
- Frequent changes requested by the proposer before policy issuance.
- High-value proposals submitted at the end of business hours or with urgency for immediate issuance.
- Proposals submitted by intermediaries with past instances of irregularities.

**2. KYC & Customer Verification RFIs**

- Identity documents that appear forged, mismatched, or tampered.
- Address proof inconsistent with customer statements or occupation.
- Multiple policies using the same address, phone number, or bank account.

**3. Premium Payment RFIs**

- Premiums paid in cash for high-value policies where digital payment is expected.
- Premiums paid by third parties not connected to the insured or proposer.
- Multiple premium payments from unrelated bank accounts.
- Frequent dishonor of cheques or reversals of payments.

**4. Claims Stage RFIs**

- Claim reported immediately after policy inception or reinstatement.
- Delay in submission of claim documents without reasonable cause.
- Hospital, garage, or service provider suspected or known for fraudulent practices.
- Original bills/documents unavailable or only photocopies provided.
- Sudden increase in claim value after initial intimation.
- Claim linked to multiple past claims of similar nature.

**5. Agent / Intermediary-Related RFIs**

- Intermediaries submitting unusually high volume of claims or early claims.
- Pattern of business from high-risk geographic areas with poor historical experience.
- Same intermediary associated with multiple suspicious or fraudulent claims.

**6. System & Technology RFIs**

- Multiple login attempts or irregular system access outside normal work hours.
- Alteration or deletion of system records without proper authorization.
- Data inconsistencies between core systems and supporting systems.
- Unauthorized changes in customer or policy data.

**7. Vendor / Partner RFIs**

- Vendor invoices with identical patterns, dates, or rounding-off issues.
- Complaints from customers regarding vendor practices or quality of service.

**8. Financial / Accounting RFIs**

- Unusual reconciliations or unexplained variances in financial records.
- Repeated adjustments, reversals, or manual entries in ledgers.
- Vendors or employees sharing common bank accounts or addresses.
- Duplicate payments or suspicious refund transactions.

## Annexure 1: Fraud Monitoring Report

**FMR – 1**

**Fraud Monitoring Report**

Name of the Insurer: New India Assurance Company Ltd.

**Part I -Frauds Outstanding- Business segment wise:**

| Sl. No. | Category 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 fraud, details of Cyber/New Age Fraud shall be reported separated 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 |
|---|---|---|---|
| | | | |

**Part II – Age-wise analysis of unresolved cases**

| Sl. No. | Unresolved Cases at the end of the year (age-wise) | No. | 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** | | | | | | | | |

**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