



Leadership and beyond

दि न्यू इन्डिया एश्योरन्स कंपनी लिमिटेड
The New India Assurance Co. Ltd

India's Premier Multinational General Insurance Company

CORPORATE ANTI-FRAUD POLICY and Standard Operating Procedure 2019 Version 1.3

**Corporate Anti Fraud Policy 2013 Version 1.1
Corporate Anti Fraud Policy 2018 Version 1.2**

Table of Contents:

1.	Preamble.....	3
2.	Objective and Scope of the Policy.....	3
3.	Definition and common types of Fraud.....	4
4.	Classification of Insurance Frauds.....	5
5.	Fraud Risk Management Framework.....	6
6.	Roles and Responsibilities.....	7
(I).	Fraud Monitoring Cell.....	7
(II).	Chief Risk Officer.....	8
7.	Alignment of Functions of Vigilance, IAD & Operational Units vis-a-vis FMC.....	8
8.	Fraud Incident Reporting.....	9
9.	Compliance.....	10
10.	Recovery of Fraud Loss.....	10
11.	Creation of Data Bank of Fraud repository.....	10
12.	Creating awareness – Among Employees, Customers & Public	10
13.	Co-ordination with Law Enforcement agencies.....	11
14.	Framework for exchange of information.....	11
15.	Due Diligence.....	11
16.	Reporting to the Authority	11
17.	Whistleblower Policy.....	12
18.	Custodian of the Policy.....	12
19.	Review of the Policy.....	12
20.	Annexure A - Report on Actual/ Suspected Fraud.....	13

1. 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 Para C of IRDA Circular ref: IRDA/SDD/MISC/CIR/009/01/2013 dated Jan 21, 2013.

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 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.

2. 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 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.

3. Definition and common types of Fraud:

Fraud Defined

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.

The IRDAI Circular referred at the outset above recognizes that insurers typically face prospects of fraud into broadly six main categories:-

- i. **Policyholder Fraud** - Fraud against the insurer in the purchase or in the execution of an insurance product by obtaining wrongful coverage or payment.
- ii. **Intermediary Fraud** - Fraud perpetrated by an insurance agent/Corporate Agent/Intermediary/Third Party Administrators (TPAs) against the insurer and/or policyholders.
- iii. **Internal Fraud** - Fraud/misappropriation against the insurer by its Director, Manager and/or any other officer or staff member (by whatever name called).
- iv. **Claims Fraud**: Fraud against the insurer in the execution of an insurance product at the time of making a claim and in settlement of claims.
- v. **Third Party Fraud**: Fraud committed by third parties against the insurer and the general public which primarily includes activities such as issue of fake/forged policies and cover notes in the name of the insurer.
- vi. **Online Fraud**: This type of fraud is typically a third party fraud, however, this could inter- alia involve any of the following types of frauds-
 - a) Buyer side frauds: where buyers file fraudulent claims, chargebacks or compromised payment cards.
 - b) Merchant side frauds: Frauds committed by any of the merchant partners of the Company which would include non-remittance of premium collected on behalf of the Company and/or incorrect charge backs etc.

- c) Cyber security fraud: Transactions effected through fake or stolen credit card/ bank accounts to carry out a transaction in the web portal of the Company. Threat of confidential data of the Company being comprised due to any cyber-attack/hacking of Company systems.
- d) Other Frauds- Any other type of online fraud which does not fall under either of the above three sub-categories.

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:-

- i. Employee(s), ex-employee(s)
- ii. Persons engaged for work or assignment on temporary/ad-hoc/contract/daily-wage basis and/or their individual employees/representatives
- iii. Advisor(s), consultants and similar providers of professional expertise including Surveyors/Valuers/Loss Adjusters, Lawyers, Investigators and/or their individual employees/representatives
- iv. Vendors, suppliers of any goods or services to the Company (including IT hardware/software suppliers and support and maintenance providers).
- v. Third Party Administrators (TPAs) and/or their individual employees/representatives
- vi. Customers/clients of the Company and/or their individual employees/representatives
- vii. Agents and/or their individual employees/representatives
- viii. Brokers and/or their individual employees/representatives
- ix. Shareholders etc.

4. Classification 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 as a result 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. Falsifying records, removing the documents/papers/noting from files and/or replacing them.
- vii. Making fraudulent/false noting in official records of the Company.
- viii. 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”.

- x. Unauthorized or illegal use of confidential information (e.g. profiteering as a result of insider knowledge of company activities).
- xi. 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 insurer leading to non-issuance or renewal of a policy. Fake insurance documents carrying the façade of Company’s document.
- xii. On the claims and underwriting side frauds may include close proximity cases related, staging of occurrences, damages to vehicles shown exaggerated, non-existent and pre-existing. 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.
- xiii. Loss of intellectual property (e.g. disclosing confidential and proprietary information to the outside parties).
- xiv. Conflict of interest resulting in actual or exposure to financial loss.
- xv. Vendor related frauds.
- 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) :

- i. 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.
- ii. 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.
- iii. 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 :

I) Fraud Monitoring Cell (FMC) :

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 Cell** 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 FMC 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 FMC 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 FMC.

xii. Constitution of Committee :

CMD to constitute a Committee consisting of two General Managers, GM Internal Audit & CRO to examine the fraud incidents reported and initiate remedial measures. FMC will report to this Committee.

The Committee to meet atleast once a quarter and the required quorum will be three members.

The Committee is also empowered to decide whether the incident falls within the definition of fraud.

FMC 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.

II) Chief Risk Officer (CRO) :

- i. To review the Anti-Fraud policy periodically.
- ii. Responsible for the functioning of Fraud Monitoring Cell 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.

7. Alignment of Functions of Vigilance, IAD & Operational Units vis-a-vis FMC :

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/LCBOs/DO's/BO's/MO's) 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, policy-holders 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.

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 Cell (FMC) is naturally not to take over or even overlap the functions of these departments, but to act in coordination with them.

8. Fraud Incident 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 Cell (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 FMC email id fmc@newindia.co.in by the department/Operational unit.
- iii) 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.

- iv) Vigilance Department and IAD shall share with the FMC, details of frauds detected after sensitive /confidential investigation processes are over.
- v) The FMC shall, through the ERM Department, report periodically to the Risk Management Committee of the Board.

9 Compliance :

- i. 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.
- iv. 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 in order to facilitate the expeditious completion of investigation.

14. Framework for Exchange of Information :

- i. Relevant information collected by the FMC 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 FRM 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. insurance agents, corporate agents, intermediaries, TPA etc.

16. Reporting to the Authority :

The statistics on various fraudulent cases which come to light and action taken thereon shall be filed with the authority in forms FMR 1 and FMR 2 providing details of:

- i. Outstanding fraud cases
- ii. Closed fraud cases

every year within 30 days of the close of financial year.

17 Whistle Blower Policy:

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

18. Custodian of the policy :

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

19. 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.

-----x-----

Corporate Anti-Fraud Policy and SOP 2019 (Version 1.3) – Policy has been revised and adopted in Board Meeting held on 9th August 2019.

ANNEXURE A

REPORT ON ACTUAL / SUSPECTED FRAUDS

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

1.	DETAILS OF THE RO/LCBO/DO/BO/MO (where fraud was committed) A) NAME OF INCHARGE B) CODE NO. C) ADDRESS D) CONTACT DETAILS	
2.	A) NAME OF INSURED (On Whom fraud was committed) B) LINE OF ACTIVITY (Individual/corporate/dealer/financier)	
	<u>FRAUD COMMITTED BY :</u> A)EMPLOYEES OF THE COMPANY: B)INTERMEDIARIES: (Surveyors/Investigators/Agents/Brokers/TPAs/Doctors/Advocates /financiers/ Other third Party etc.) C) FRAUD COMMITTED BY EMPLOYEES IN COLLUSION WITH OUTSIDE PARTIES/ INTERMEDIARIES ETC.	
3.	A) AREA OF OPERATION WHERE THE FRAUD HAS OCCURRED 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/LTs bills/ Misuse of passwords etc.) B) SERIES OF EVENTS: (One event leading to multiple events) C) WHETHER COMPUTER USED IN COMMITTING THE FRAUD IF YES, FURNISH DETAILS	
5.	A) DATE OF OCCURRENCE B) DATE OF DETECTION C) HOW THE FRAUD CAME TO LIGHT	

	D) REASONS FOR DELAY, IF ANY, IN DETECTING THE FRAUD: E) DATE ON WHICH REPORTED TO NEXT HIGHER AUTHORITY 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: A)POLICY NUMBER/ CLAIM NO / LICENSE NO/ CASE NO: B) WHETHER REPORTED TO HIGHER AUTHORITY / VIGILANCE AUTHORITY C) WHETHER ANY INVESTIGATION HAS BEEN CARRIED OUT D) WHETHER ANY COMPLAINT HAS BEEN LODGED WITH THE POLICE/CBI (i) IF YES, BRANCH OF POLICE STATION (ii) FIR NO (iii)PRESENT POSITION OF THE CASE (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 B)TOTAL AMOUNT RECOVERED B) EXTENT OF LOSS TO THE COMPANY C) PROVISION TO BE PROVIDED, IF ANY	
12.	SUGGESTIONS, IF ANY FOR ACTION	

Date:

**SIGNATURE OF BO/DO/RO-
INCHARGEWITH
NAME & DESIGNATION**

Place: