Reliance Nippon Life Insurance Company Limited

Fraud Prevention Policy

Table of Contents

Change History

Author	Reviewer/Approver	Version	Date of Release
Kapil Punwani	Kavita Maru	1.2	April - 2015
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.3	April - 2017
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.4	July 2018
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.5	July 2019
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.6	July 2020
	Sunder Krishnan		
Kapil Punwani	Kavita Maru	1.7	July 2021
	Sunder Krishnan		

1. Introduction and Objective

This policy is being formulated to establish an independent Fraud Risk Management framework across the Company, in line with IRDAI guidelines (IRDAI/ SDD/ MISC/ CIR/ 009/01/2013 dated 21st January 2013) 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. It is the intent of the Company to promote consistent organizational behavior by following guidelines and assigning responsibility for the development of controls and conduct of investigations.

This policy will cover the following aspects:

- Provide systems and adequate system-based controls to identify potential fraud areas, assess these and provide a framework of people, process, and technology-based controls of processes to prevent fraud.
- Ensure that management understands the risk of fraud to the organization and establish a sound control environment through policies, procedures and controls to detect, monitor and mitigate occurrences of frauds within various functions of the company that are vulnerable to the fraud risk.
- Create awareness among all stakeholders including employees, clients and other parties having business relation with the company to deter them from indulging in fraudulent activities and measures to be taken by them in case they suspect any fraudulent activities.
- Provide a set of measures and procedures to respond adequately and quickly to frauds.
- Lay down procedures to report frauds to board, senior management and regulator and exchange of information on frauds and framework for reviewing the procedures from time to time.

2. Scope

This policy applies to any fraud or suspected fraud involving distributors, vendors, customers, employees (all full time, part time or employees appointed on an ad-hoc / temporary /contract basis), Unknown/Third Party/s and representatives of vendors, suppliers, contractors, service providers or any outside agencies doing any type of business with the company.

3. Fraud Classification

Fraud in insurance is an act of omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties. It may be a simple act involving one person or it may be complex operation involving a large number of people from within and outside the company.

This may, for example, be achieved by means of:

(a) Misappropriating assets

(b) Deliberately misrepresenting, concealing, suppressing or not disclosing one or more material facts relevant to the financial decision, transaction or perception of insurer's status

(c) Abusing responsibility, a position of trust or a fiduciary relationship

The board categories of fraud are:

a) **Policy holder fraud and or claims fraud:** Fraud against the company in the purchase and or execution of an insurance product, including fraud at the time of making a claim.

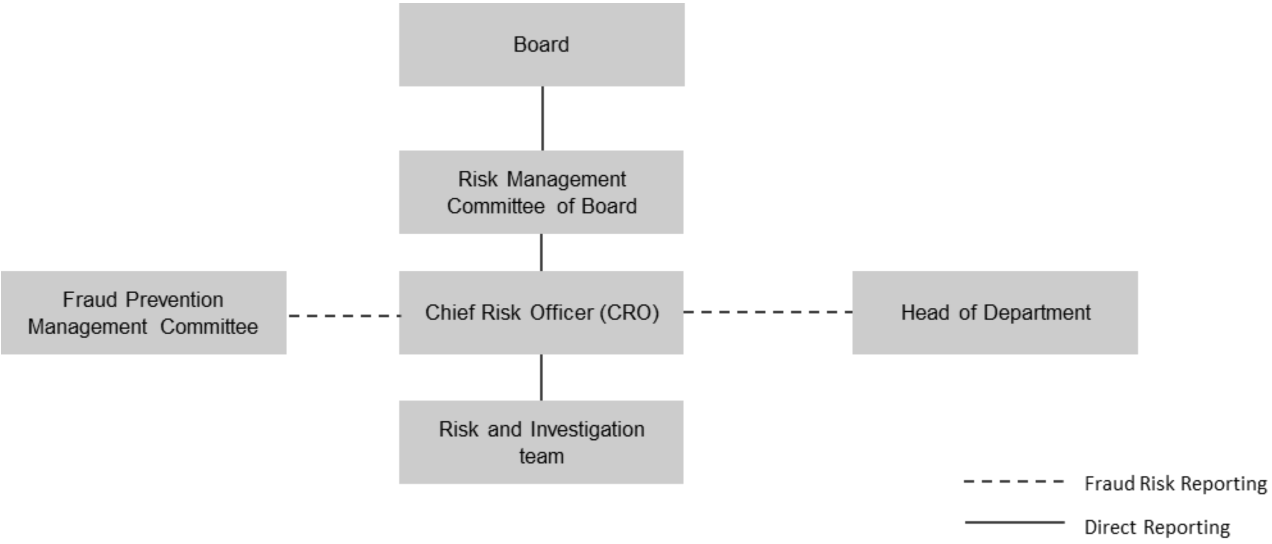
b) **Internal fraud:** Fraud against the company by a board member, director, manager or any other staff member or office.

c) Intermediary fraud: Fraud perpetrated by an insurance agent/Corporate agent/TPA against the company or policy holders.

An illustrative list of Insurance Frauds is given as **Appendix – A**. These instances include frauds perpetrated internally, by insurance agent/Corporate Agent/intermediary/TPAs and instances of claims/policyholder frauds

4. Fraud Risk Management structure

The Fraud Risk Management structure is given below:



The Board of Directors provide the overall guidance on Fraud Risk Management and has delegated the responsibilities relating to Fraud Risk Management activities to Risk Management Committee of the Board (RMCB). The Chief Risk Officer independently reports to the Risk Management Committee of Board. The Chief Risk Officer is supported by the Risk and Investigation team for performing the Fraud Risk Management activities of the organization. All investigations are handled by Risk team.

Other business leaders such as functional heads (E.g. Product development, marketing, human resources etc.) should also participate in responsibilities under the organization's antifraud strategy; they oversee areas of daily operations in which risk arises. Such functional heads can serve as subject matter experts to assist the Chief Risk Officer with respect to their particular areas of expertise or responsibility.

The roles and responsibilities for Fraud Risk Management are defined below:

4.1 Risk Management Committee of Board (RMCB)

The Risk management committee is responsible for this policy and will remain, interpret and communicate the policy in company. The committee is responsible for the following activities:

- Creation of anti-fraud culture across the Organization
- To initiate and oversee a prompt investigation of any suspected fraudulent act or omission or non-compliance with the policy's requirement
- Review the issues identified during entity's fraud risk assessment as well as during internal and external audit.
- To ensure that this policy and related guidelines are communicated, updated and made available to all employees and representatives within the company.
- To ensure that Board of Directors are informed of fraud on occurrence of any fraud incident through periodical reporting process

(For further details, please refer Risk Management Committee Charter)

4.2 Fraud Prevention Management Committee

For Fraud Prevention Management, RMCB has appointed Fraud Prevention Management Committee (which is part of Control Committee) at company level. The Committee consists of senior officials like Chief Executive Officer, Chief Risk Officer, Appointed Actuary, Chief Operating Officer, Chief Financial Officer, Chief Distribution Officer, Chief Investment Officer, Chief Human Resource Officer, Chief Marketing Officer and Head-Nippon Best Practices. Other Head of Departments can be invited as special invitees. The decision of the committee will be taken on majority basis. Fraud Prevention Management Committee will meet at least monthly or as and when need arises.

The scope of roles and responsibilities of the Fraud Prevention Management Committee is briefly mentioned as under:

a) Review the Fraud Prevention Policy and recommend any revisions in Fraud Prevention policy to RMCB on an annual basis.
b) Monitor and review Fraud Risk Management framework
c) Monitor and review frauds reported (actual as well as attempted)
d) Review actions taken and proactive fraud prevention activities
e) Monitor fraud prevention action plans
f) Review information for Fraud Risk Management purpose (such as Fraud events analysis, Fraud trends, and results of Fraud assessments) provided by Risk and Investigation team.

(For further details, please refer Fraud Prevention Management Committee Charter)

4.3 Chief Risk Officer

The Chief Risk Officer reports to the Risk Management Committee of the Board. The Chief Risk Officer is supported by the Risk and Investigation team for performing the Fraud Risk Management activities of the organization.

The CRO acts as the custodian of Fraud Risk Management framework and guides the implementation of the Fraud Risk Management framework across the organization. Recommendations of the Fraud Prevention

Management Committee reported to RMCB by the CRO with support from the Risk and Investigation team.

a) Responsible for the functioning of Risk and Investigation team and for escalating all reported cases of suspected fraud / misconduct, as appropriate within the organisation

b) Review the fraud risk assessments to identify areas prone to fraud and suggest anti-fraud controls

c) For external fraud, review the investigation report provided by investigation agencies so that necessary steps can be undertaken to recover losses and misappropriated assets

d) Review the identified fraud data obtained from Head of Departments and submit the fraud monitoring reports to the Chief Compliance Officer for reporting to regulatory authority

e) Report the fraud cases and results of other fraud monitoring activities conducted to the Risk Management Committee of Board

4.4 Head of Department

All functional heads shall share the responsibility of prevention and detection of fraud and for implementing Fraud Prevention policy of the company. It is the responsibility of all functional heads to ensure that there are mechanisms in place within their area of control to:

a) Implement adequate controls and measures for prevention and timely detection of fraud incidents
b) Spread awareness to all employees within the department about possible fraud scenarios
c) Familiarize each employee with the types of improprieties that might occur in their area.
d) Educate employees about fraud prevention and detection
e) Create a culture whereby employees are encouraged to report any or suspected fraud which comes to their knowledge, without any fear of victimization.
f) Record all reports received from employees on suspected incidents of fraud/misconduct
g) Inform reports received from employees on suspected incidents of fraud/misconduct to Risk and Investigation team within 48 hours from the detection of any confirmed, attempted or suspected fraud.

The Head of Department may delegate the above responsibilities to a defined SPOC within the department.

4.5 Risk and Investigation team

The function of Fraud Monitoring and investigations is handled by Risk and Investigation team which is part of the Enterprise Risk Management department. Risk and Investigation team is headed by Chief Risk Officer (CRO) of the Company. The Risk and Investigation team under the guidance of the CRO is responsible to develop, implement and maintain a Fraud Risk Management (FRM) Framework, to achieve their objective of being a fraud resilient organisation that is committed to preventing, detecting and responding to fraud.

The key roles and responsibilities of Risk and Investigation team are mentioned below:

(a) Develop and implement a Fraud Risk Management (FRM) Framework

(b) Identification of areas prone to fraud by carrying out periodic fraud risk assessments and pro-active detection through alerts built in system. Suggest suitable anti-fraud controls for risks identified in the Fraud risk assessment review

(c) Develop fraud prevention mechanism fraud response mechanism

(d) 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 and Internal Audit. Based on the observations noted in the review, the Risk and Investigation team will put in place controls for prevention, detection, mitigation of fraud or get investigations / special review carried out by investigation agencies in case these observations point to a suspected case of fraud

(e) For external fraud, appoint investigation agencies to investigate reported fraud or complaint with suspicion of fraudulent activity and identify the perpetrator. Take necessary steps to recover losses and misappropriated assets

(f) Perform analysis of relevant data to identify potential fraud trends and fraud areas

(g) Collate identified fraud data obtained from various Head of Departments and submit to CRO for review

(h) Create awareness among the employees to counter insurance frauds

(i) Organize and collect management information with respect to fraud in the company, make it available in a timely manner for the Board and senior management to monitor development and take appropriate action

4.7 Employees, Vendors, Service providers

Every employee (Full time, part time, ad-hoc, temporary, contract), representative of vendors, suppliers, contractors, consultants, service providers or any other agencies doing any type of business with the company is expected and shall be responsible to ensure that there is no fraudulent act being committed in their areas of responsibility/control.

As soon as it is learnt that a fraud or suspected fraud has taken or is likely to take place, they should immediately apprise the same to the concerned person as per the procedure.
They should take necessary steps for prevention of fraud and appropriate actions in case of suspicion of commission of a fraud or detection of an actual fraud.

5. Identify Potential areas of fraud within the organization

The following areas of business and departments of the organization are potentially prone to fraud.
A detailed department wise anti-fraud procedure will need to be laid down to address the risk from fraud.

- Product development function
- Branch operations
- New business and underwriting-Accepting clients
- Human Resource department- Hiring and firing of management and staff
- Claims-Claims handling process
- Agency/CDATPD and other sales functions-Recruitment/management of intermediaries
- IT-Information security and IT assets
- Customer service-Outsourced activities
- Finance- Pay-out handling
- Investment
- Administration-Procurement of materials

6. Fraud Prevention

Preventive controls are designed to help to reduce the risk of fraud and misconduct from occurring in the first place. These controls can be categorized based on:

- Governance
- Roles and Responsibilities
- Internal audit function
- Fraud risk assessment

6.1 Governance based fraud prevention controls

6.1.1 Code of Conduct

An organization's code of conduct is one of the most important communications that management should use to communicate to employees on key standards that define acceptable business conduct. \
The code of conduct should be in place based on below key attributes:

- High-level endorsement from the organization's leadership, underscoring a commitment to integrity.
- Simple, concise and positive language that can be readily understood by employees
- Guidelines on each of the company's major policies or compliance risk areas
- Ethical decision-making tools to assist employees in making right choices
- A designation of reporting channels and viable mechanisms that employee can use to report concerns or seek advice without fear of retaliation.

6.1.2 Continuous policy and procedure review covering (but not limited to) financial procedures, tendering, gifts and hospitality expenses.

6.1.3 Due Diligence

<u>Employee and Third Party</u>

- An important part of an effective fraud prevention strategy is the use of due diligence in the hiring, retention, and promotion of employees, agents, vendors, and other third parties.
- The scope and depth of the due diligence process typically varies based on the organization's identified risks, the individual's job function and or level of authority and the specific laws applicable to organization.
- Due diligence begins at the start of the employment or business relationship and continues through out. For instance, considering behavioural considerations such as adherence to the organization's core value (DNA) in performance evaluations provides a powerful signal that management cares about not only what employees achieve but also that those achievements were made in a manner consistent with the company's values and standards. Further, vendor and third-party appraisals need to be carried out at defined intervals as per the agreement entered with them.
- The initial and on-going assessment of the fitness and property of management and staff should include the verification of identity, personal information and background.

- Personal records should be complete and contain all information on the recruitment of Board members, senior managers and other staff. Records should be retained for an adequate period after the person in question has left the company.
- Periodical job rotation and mandatory vacations for management and staff in fraud sensitive positions.
- Observing maker checker concept (involvement of more than one person in decision making or other material activities for reasons.)
- Eliminating potential conflict of interest between the board members, senior management and other staff.

<u>Policyholder</u>

- Policy holder fraud and claims fraud deterring and prevention starts with adequate product development. When designing a new product, risk enhancing factors need to be considered.
- Establish an adequate client acceptance policy.
- Client should be identified, and the identity verified
- Approaches used for client acceptance include
    - Using professional judgment based on experience
    - Checking internal or external databases and red flag lists
- Draw the attention of the policyholders to their duties and responsibilities when taking out insurance. The company should include several provisions on policy documents and other relevant documents which make the policy holder, claimant and beneficiary aware of submitting a false statement or incomplete statement.

6.1.4 Communication and Training

Making employees aware of their obligations concerning fraud prevention controls begins with practical communication and training.
In formulating training and communications plan, management should consider developing fraud initiatives that are:

- Comprehensive and based upon job functions and risk areas
- Integrated with other training efforts, whenever possible
- Regular and frequent, covering the relevant employee population

In particular, the functions identified as potential business areas of fraud (refer section 5) should get initial and ongoing training on fraud matters. Training can help to raise staff awareness of the risks of fraud and the importance of compliance with internal control procedures and security checks to prevent such frauds. Additionally, close monitoring of staff compliance with these controls helps ensure their consistent application.
There should be communication to both potential clients and existing clients about the company's anti-fraud policies. Proposal form/ Policy document will need to be included with cautionary statements highlighting the consequences of submitting a false statement.

6.2 Roles and Responsibilities

Please refer section 4 for detailed roles and responsibilities.

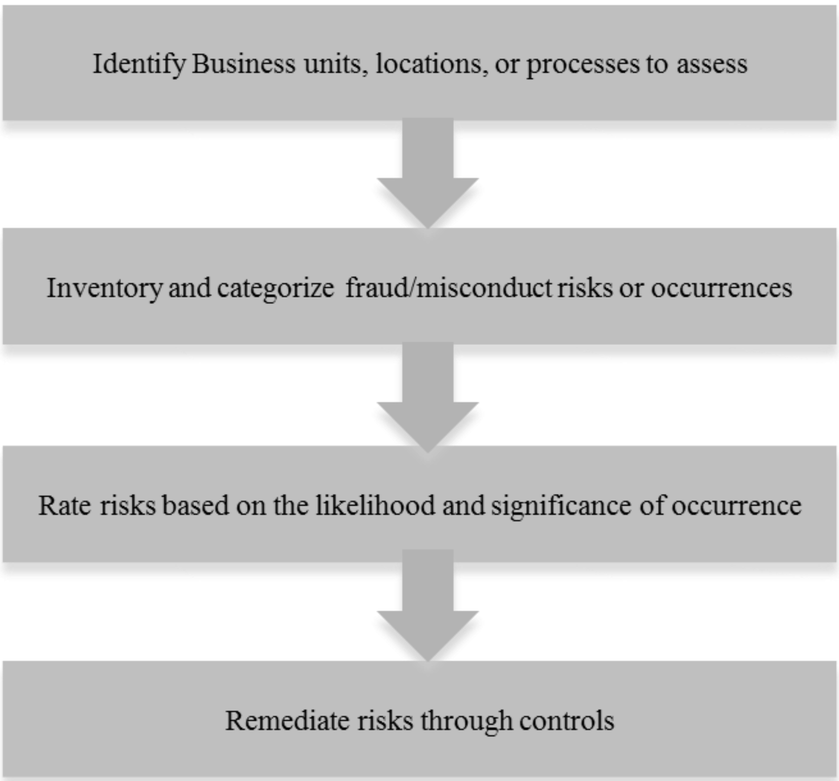
6.3 Internal Audit function

Internal audit should be responsible for:

a) Planning and conducting the evaluation of design and operating effectiveness of antifraud controls
b) Suggesting remediation action plans and monitor whether mitigation actions are being implemented on timely basis
c) Verifying compliance with the Fraud Prevention policy and identify cases of non-adherence to policy
d) Reporting to the Fraud Prevention Management Committee on internal control assessments, audits, investigations and related activities

6.4 Fraud Risk assessment

Fraud Risk assessment helps management understand the risks that are unique to its business, identify gaps or weaknesses in control to mitigate those risks and develop a practical plan for targeting the right resources and controls to reduce risk.
Management should ensure that such as an assessment is conducted across the organization, taking into consideration the entity's significant business units, processes and functions.
With input from process owners as to the relevant risks to achieving organizational objectives, a fraud risk assessment includes the steps listed in below diagram:



7. Fraud Detection

Detective controls are designed to uncover fraud when it occurs. Fraud can be detected by various below methods among others:

- Whistle blower policy
- Internal or external tip off
- Audit: Internal/External
- Customer complaints
- Negative customer data
- Investigation based on regulatory requirements
- Periodical evaluation of external vendor both pre and post empanelment
- Document/Asset verification
- Risk Reviews
- Risk logs and alerts
- Process reviews
- Key Fraud Risk Indicators
- Pre/Post Issuance verification of policies based on predictive fraud analytics

Auditing and monitoring

Auditing and monitoring systems that are reasonably designed to detect fraud are important tools that management should use to determine whether organization’s controls are working as intended. Management should develop a comprehensive auditing and monitoring plan that is based on risks identified through the organization’s fraud risk assessment process.
An auditing and monitoring plan should thus encompass activities that are tailored in depth to the nature and degree of the risk involved, with higher risk issues receiving priority treatment.
Auditing activities (evaluation of past events) should be performed in, but are not limited to areas where:

- There are specific concerns about a key process or function.
- The company has a history of occurring fraud in respective area.
- There is high employee turnover or organizational changes.
- Laws and regulations have changed significantly.

Proactive Data Analysis

Many of the indicators of fraud, both actual and potential reside within an organization’s financial, operational and transactional data and can be identified using data analysis tools and techniques. Such proactive data analysis requires sophisticated analytical tests, computer based cross-matching, and non-obvious relationship identification to highlight the potential fraud.
The benefits of such an analysis includes among others:

- Identification of hidden relationships between people, organizations and events
- A means to analyse suspicious transactions
- An ability to assess the effectiveness of internal controls intended to prevent or detect fraudulent activities.
- The potential to continually monitor fraud threats and vulnerabilities
- Pre/Post Issuance verification of policies based on predictive fraud analytics

Techniques such as data matching and data mining can be used for analysing the data. Data matching involves computerized scanning of data held in different databases in organization. Data mining involves

selecting and exploring large amount of data to reveal previously unknown patterns, behaviours, trends or relationships which may help to identify cases of fraud.
Focus on specific areas of fraud risk and preventative controls for the below mentioned areas

- Fraudulent death claims
- Expenses layering
- Contract Monitoring
- Pay-out frauds – Surrenders, refunds, redemption
- Payroll and expenses
- Branch relocations and refurbishments

8. Fraud Response

Response controls are designed to investigate and take corrective action to remedy the harm caused by fraud.

8.1 Investigation

When information relating to actual or potential fraud is uncovered, management should conduct a comprehensive investigation with the objective to:

- Assess and document the facts of case, prevent the fraud from continuing and to protect the innocent
- Provide basics for appropriate consequences, up to and including the termination of employment or contract and taking legal action where appropriate
- Taking legal actions against the culprits if necessary
- Recovery of loss if any suffered for fraudulent act
- Improve the controls to prevent the future fraudulent acts
- Publishing X files (Live case studies) covering all types of frauds done by internal or external customers.
- Publishing risk-based advisories as part of an awareness campaign covering key do's & don'ts for critical/emerging risks

Investigation is highly sensitive, and it is therefore critical that it should be conducted in a prescribed manner involving only those people who require the information to conduct a proper investigation. Further, it should be conducted in accordance with applicable laws and rights as well as privacy of all parties involved should be respected to the extent required.

The investigating team can either be in-house or outsourced third party fraud investigating agencies provided that the quality of fraud investigations and the confidentiality of information are not compromised by the outsourcing.

A well-designed investigation process should typically include following attributes among others:

- Risk officer should be consulted before any investigative action is taken to determine the course of action. Other departments should be consulted on need to know basis only.
- The means to carry out the investigation should be within the bounds established by law.
- All investigations should be carried out in an independent manner with due regard for the individual's rights but without regard to length of services, position held or relationship with the company
- All investigations must be kept confidential. Information related to a suspected fraud may not be revealed other than to the functional heads of the finance team, human resource team, and legal team and senior management and or others on a need to know basis.

- Care must be taken in an investigation of suspected fraud to avoid mistaken accusations or alerting suspected individuals that an investigation is underway.
- The result of investigations should be disclosed by the Risk officer to only those individuals who require the information to perform their roles, at Risk officer's discretion.
- Incidents of fraudulent acts or omissions should be reported to appropriate regulatory and or law enforcement agencies if the same is warranted.

Further, once the case has been reported/is being investigated by Risk and Investigation team or relevant departments, the reporting individual should not:

- Try to contact the suspected individual in an effort to determine facts or demand restitution
- Attempt to personally conduct investigations or interviews/interrogations related to any suspected fraudulent act
- Discuss the case, facts, suspicions, or allegations with anyone unless specifically asked to do so by the Risk and Investigation team or relevant department

8.2 Corrective Action

A consistent and credible disciplinary system is a key control for deterring fraud. Well-designed disciplinary process should be communicated to all employees and external parties to ensure that all concerned are aware about consequences in terms of verbal warning, written warning, suspension, pay reduction, location transfer, demotion, termination, taking legal action or imposing financial penalty.

Once fraud has occurred, management should consider taking action to remedy the harm caused. Company considers fraudulent activity to be a serious offence. A disciplinary action matrix has been defined covering all types of frauds. Actions up to and including termination of employment or contract for just cause should be pursued when warranted.
In addition, Company:

- May take action to recover losses incurred as a result of fraudulent acts or omissions; and
- May refer the matter to law enforcement, regulatory agencies or external organizations for the purpose of further investigation or prosecution

In no circumstance will any decision to be taken to discipline, suspend or terminate an individual's employment or contract without notification to, and approval of head of human resource function. Furthermore, no matter will be referred to law enforcement, regulatory agency or external organization for the purpose of further investigation or prosecution without the approval of Chief Executive Officer, Chief Financial Officer, Head Human Resources and Compliance / Risk officer. Action should be taken with the approval of any one of the above

8.3 Co-ordination with Law enforcement Agencies

If warranted by the nature, scale and complexity of the incident all consequential fraudulent activities may be reported to law enforcement agencies through the legal team of the organization with the explicit approval of the relevant authorities mentioned above. Legal team will be responsible for any further co-ordination and follow-up with law enforcement agencies.
Internal, policy holder, claims and intermediary fraud generate illegal proceeds. If there are reasonable grounds to suspect that the proceeds of the fraud are being laundered or are related to terrorist financing, the matter should be reported to the financial intelligence unit or relevant law authorities.

Employees/ intermediaries shall cooperate with any law enforcement agency in order to facilitate the expeditious completion of investigation.

9. Reports and exchange of information

Fraudsters may target different insurers simultaneously or consecutively. Therefore, there should be a continuous exchange or sharing of information about fraudsters with each other. This needs to be achieved within the limits of the privacy law and the data protection law of the company's jurisdiction by timely communication between them and setting up shared databases.

A shared database may contain Root Cause Analysis (RCA) of fraud cases and information about internal fraudsters and fraudulent policy holders, claimants, beneficiaries, intermediaries and other third parties. In addition to the exchange of specific information about fraudsters need to explore sharing knowledge about risks, trends, policy issues, prevention and detection.

All such exchange of information should be made through life insurance council subject to enough data protection mechanisms. The statistics on various fraudulent cases and action taken thereon should be filed with the regulator by providing the following details within 30 days of the close of the financial year.

- Outstanding fraud cases; and
- Closed fraud cases

Additionally, investigation reports of all suspected/actual fraudulent acts will be discussed in Fraud Prevention Management Committee on a monthly basis. Identified frauds will be reported to Risk Management Committee of Board, along with actions devised/taken.

Claim fraud that impinge on the border of innocent "non-disclosure" by the customer would not be construed as a fraud that needs to go through all the above stages of identification up to the stage of reporting to the Board and Authority. Similarly, customer complaints settled by an insurer but not involving a per-se fraudulent activity such as document tampering or deceit with malefic intention need not be construed as a reportable fraud.

A Fraud Monitoring Report (FMR) is also shared with the regulator once a year as per format designed by IRDAI.

10. Review of policy

This policy would be reviewed annually to keep it current with regulatory and business requirements and changes, if any, will be approved by the board.

11. Appendix A - Illustrative List of Insurance Frauds

Broadly, the potential areas of fraud include those committed by the officials of the insurance company, insurance agent/corporate agent/intermediary of TPAs and the policyholders/ their nominees. Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

11.1 Internal Fraud: Fraud/ Mis-appropriation against the insurer by its Director (excluding independent directors), Manager and/or any other officer or staff member (by whatever name called)

(a) Misappropriating funds
(b) Fraudulent financial reporting (Improper revenue recognition, overstatement of assets, and understatement of liabilities)
(c) Stealing cheques
(d) Overriding decline decisions to open accounts for family and friends
(e) Inflating expenses claims/over billing
(f) Paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
(g) Permitting special prices or privileges to customers, or granting business to favoured suppliers, for kickbacks/favours
(h) Forging signatures
(i) Fraudulent Surrenders
(j) Misrepresentation of Customer Details
(k) Utilising Customer's premium amount for personal use and/or delay in deposit
(l) Business login of a Dead Person and/or adverse health life
(m) Removing money from customer accounts
(n) Falsifying documents
(o) Selling insurer's assets at below their true value in return for payment.

11.2 Policyholder Fraud and Claims Fraud: Fraud against the Insurer in the purchase and/or execution of an insurance product, including fraud at the time of making a claim

(a) Customer applying fake documents
(b) Staging the occurrence of incidents
(c) Reporting and claiming of fictitious loss
(d) Medical claims fraud
(e) Fraudulent Death Claims

11.3 Intermediary fraud: Fraud perpetuated by an insurance agent/Corporate Agent/Intermediary/Third Party Administrators (TPAs) against the insurer and/ or policy holder

(a) Premium diversion-intermediary takes the premium from the purchaser and does not pass it to the insurer
(b) Inflates the premium, passing on the correct amount to the insurer and keeping the difference
(c) Non-disclosure or misrepresentation of the risk to reduce premiums
(d) Misrepresentation of Customer Details
(e) Utilising Customer's premium amount for personal use and/or delay in deposit
(f) Business logion of a Dead Person and/or adverse health life