ANTI FRAUD POLICY

Version 1.4

Future Generali India Life Insurance Co. Ltd.

6th Floor, Tower 3, Indiabulls Finance Centre,

Elphinstone, Mumbai – 400 013

Document Version Control

DOCUMENT	Anti-Fraud Policy
VERSION	1.4
PREPARED BY	Piyush Singh (Enterprise Risk Management)
REVIEWED BY	Madangopal Jalan (Executive VP - Company Secretary & Legal) Bikash Choudhary (AA & CRO) Amol Apte (Associate Vice President – Legal) Pushkar Mahadik (Sr. Manager - Sales Compliance)
APPROVED BY	The Board of Directors (BOD)
OWNERSHIP OF POLICY	Legal & Compliance

Change History

VERSION	ISSUE DATE	REASON FOR CHANGE
1.0	April 01, 2013	First Version
1.1	May 29, 2014	Yearly review, there is no change in policy
1.2	May 21, 2015	Yearly review, there is no change in policy
1.3	April 12, 2016	Yearly review, Added Ownership details of Compliance Head in Introduction
1.4	June 19, 2017	Added E-commerce fraud Management Framework, Roles & Responsibility amended.

Contents

This page is left intentionally blank

1. Introduction

Financial Fraud poses a serious risk to all segments of the financial sector. Fraud in insurance reduces consumer and shareholder confidence; and can affect the reputation of individual insurers and the insurance sector as a whole. It also has the potential to impact economic stability. It is, therefore, required to understand the nature of fraud and take steps to minimize the vulnerability of operations to fraud.

Under the Regulatory Framework put in place for insurance companies, the Insurance Regulatory Development Authority of India (IRDAI) has stipulated a number of measures to be taken to address the various risks faced. Some of these include:

- The Corporate Governance guidelines mandate insurance companies to set up a Risk Management Committee (RMC). The RMC is required to lay down the company-wide Risk Management Strategy.

- As part of the Responsibility Statement which forms part of the Management Report filed with the Authority under the IRDA (Preparation of Financial Statements and Auditors' Report of Insurance Companies) Regulations, 2002, the management of an insurance company is required to disclose the adequacy of systems in place to safeguard the assets for preventing and detecting fraud and other irregularities, on an annual basis.

- IRDAI circular dated January 21, 2013 mandated insurers to put in place Board Approved Anti-Fraud Policy to define holistic approach to adequately identify, measure, control and monitor fraud risk and accordingly lay down appropriate risk management policies and procedures across the organisation.

Future Generali India Life Insurance Company Limited (hereinafter referred to as the "Company") values integrity, honesty and fairness in everyone from the top to the bottom. The Company encourages openness to prevent malpractice or any cover-up of malpractice and create a positive workplace environment where employees have positive feelings about the Company itself and the Group and do not feel abused, threatened or ignored.

The Company has adopted this policy to ensure consistent and effective investigation, reporting and disclosure of fraud occurrences and to provide a clear guidance to the employees and others dealing with the Company, forbidding them from involvement in any fraudulent activity and the action to be taken by them when they suspect any fraudulent activity.

This policy is owned by the Compliance Head of the company and it should be reviewed at least once annually by the members of RMC (Risk Management Committee).

2. Scope and Classification of Insurance Frauds

This document identifies the measures that Future Generali India Life Insurance Company Limited (hereinafter referred to as the "Company") shall implement to prevent, deter and detect fraud in the context of three fundamental elements:

(1) Create and maintain a culture of honesty and high ethics, including the understanding and awareness of risks and controls;

(2) Identify and assess the risks of fraud and implement the processes, procedures and controls needed to mitigate the risks and reduce the opportunities for fraud; and

(3) Develop an appropriate oversight and governance process.

Specifically, this document aims at:

i. Ensuring that management is aware of its responsibilities for the detection and prevention of fraud and for establishing procedures to prevent fraud and/or detect fraud on its occurrence;

ii. Providing a clear guidance to employees and others dealing with the Company, forbidding them from involvement in any fraudulent activity and the action to be taken by them when they suspect any fraudulent activity;

iii. Providing a mechanism for employees and officers of the Company to report any incident of fraud or alleged incident of fraud and protect the employees and officers of the Company who make a disclosure against their managers and/or fellow employees in certain defined circumstances from harassment and/or dismissal;

iv. Providing a clear guidance on how investigations into fraudulent activities will be conducted;

v. Providing assurance that any and all suspected fraudulent activities will be fully investigated and dealt with;

vi. Providing assurance to one and all that fraudulent activities will not be allowed or tolerated; and

vii. Ensuring preventive measures and internal control procedure enhancement, subsequent to any fraud being identified, are strengthened in a speedy manner.

This document applies to all employees and officers of the Company at whatever level, at every location and whatever the terms of employment, hours of work or length of service, including contractual staff and directors in the employment of the Company, as well as shareholders, agents and other insurance intermediaries, service providers, consultants, vendors, contractors and subcontractors, prospective and existing customers and/or other parties with a business relationship with the Company.

Any required investigative activity will be conducted without regard to the suspected wrongdoer's length of service, position/title or relationship to the Company.

What is Fraud?

Fraud is an operational risk. Generally speaking, it is defined as any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

Fraud encompasses a range of irregularities and illegal acts characterized by intentional deception or misrepresentation, which an individual knows to be false or does not believe to be true. Fraud is perpetrated by a person knowing that it could result in some unauthorized benefit to him/her or to another person or undue loss to the Company and can be perpetrated by persons outside and inside the organization.

Specifically, fraud in insurance is defined as an act or omission to gain dishonest or unlawful advantage for a party committing the fraud (hereinafter referred to as the "fraudster") or for other parties.

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 a financial decision, transaction or perception of the insurer's status; and
c) abusing responsibility, a position of trust or a fiduciary relationship.

Fraud in insurance falls into one of the following categories:

- **Intermediary Fraud:** Fraud by intermediaries such as Agents, Corporate Agents, Third Party Administrators (TPAs) against the insurer or policyholders;

- **Policyholder Fraud and / or Claims Fraud :** Fraud against the insurer in the purchase or in the execution of an insurance product by obtaining wrongful coverage or payment under the contract of insurance

- **Internal Fraud:** Fraud/ mis-appropriation against the insurer by its Director, Manager and / or any other officer or staff member (by whatever name called)
- **Occupational Fraud:** Use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. *(This definition encompasses a wide range of misconduct by employees, managers and executives, from pilferage of company supplies to financial statement frauds.)*
- **Ecommerce Fraud:** This fraud is separately covered in detail under section **5** of this document

Fraud may occur in many forms. 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. Common examples of fraud include:

- Kickbacks (including the receipt of excessive gifts or accepting or seeking anything of material value from contractors, vendors or persons providing services/materials to the Company);
- Diversion to an employee or outsider of a potentially profitable transaction;
- Forgery or alteration of documents or accounts belonging to the Company;
- Concealment or misrepresentation of transactions, assets or liabilities;
- Expense related frauds (e.g. claims for services or goods not actually provided);
- Loss of intellectual property (e.g. disclosing confidential and proprietary information to outside parties);
- Conflicts of Interest resulting in actual or exposure to financial loss;
- Vendor fraud;
- Reimbursement fraud;
- Embezzlement (i.e. misappropriation of money, securities, supplies, property or other assets);
- Cheque fraud (i.e. forgery or alteration of cheques, bank drafts or any other financial instrument);
- Payroll fraud;

- Bribery & corruption;
- Fraudulent financial reporting (e.g. forging or alteration of accounting documents or records; intentional concealment or misstatement of transactions resulting in false records or misleading statements; intentional failure to record or disclose significant information accurately or completely);
- Improper pricing activity;
- Unauthorized or illegal use of confidential information (e.g. profiteering as a result of insider knowledge of company activities);
- Unauthorized or illegal manipulation of information technology networks or operating systems;
- Tax evasion;
- Destruction, removal or inappropriate use of records, furniture, fixtures and equipment of the Company;
- Sales or assignment of fictitious or misrepresented assets;
- Utilizing company funds for personal purposes.

The above list is indicative only and does not intend to be exhaustive.

An illustrative list of Insurance Frauds as published in the IRDAI circular is given at Appendix – 1.

The above mentioned instances include frauds perpetuated internally; by insurance agent/Corporate Agent/intermediary/TPAs; and instances of claims/policyholder frauds.

3. The Fraud Triangle

There are three basic conditions that contribute to the occurrence of fraud:

- **Incentive/ Motive/ Pressure:** Management or other employees have an incentive/ motive or are under pressure to commit fraud (e.g. personal financial needs; market pressures to meet financial targets or goals; etc.);
- **Opportunity:** Circumstances exist that provide opportunity to commit fraud, such as ineffective or absence of controls, poor oversight or management ability to override controls. Opportunities to commit fraud exist throughout the organization and are greatest in areas with weak internal controls and a lack of segregation of duties; and

- **Rationalization/ Attitude:** the culture or the environment enables management or other employees to rationalize committing fraud, i.e. legitimize or justify the crime – attitude or values of those involved, or pressure that enables them to rationalize committing a dishonest act.

In order to commit a fraud, all three elements of the triangle need to be present.

4. Internal Fraud vs. External Fraud

Fraud can be further distinguished between internal fraud and external fraud, whereby internal fraud involves at least one internal party, whereas external fraud is committed solely by external party without any assistance or collusion of an internal party.

All employees and people who are part of the Company and/or the Group, including associated companies, tied sales networks, etc., are considered "internal parties". Such definition also includes the employees of outsourcers belonging to the group, tied agents and their employees and members of corporate bodies. It excludes other outsourcers and suppliers, consultants, brokers and independent intermediaries like Corporate Agent, Insurance Marketing Firms, Web Aggregators.

Generally speaking, internal fraud is defined as any intentional act or omission designed to deceive others, performed by one or more staff members directly or in collusion with external parties, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

5. E- Commerce Fraud

E-commerce is being seen as an effective medium to increase insurance penetration and enhance financial inclusion in a cost-efficient manner. The Insurance Regulatory and Development Authority of India (IRDAI) (hereinafter referred to as the "Regulator") as part of its developmental mandate, issued guidelines under CIRCULAR NO.IRDA/INT/GDL/ECM/055/03/2017, DATED 9-3-2017; to promote e-commerce in insurance space which is expected to lower the cost of transactions in insurance business and bring higher efficiencies and greater reach. The Guidelines also make it mandatory for the insurers to have a robust fraud detection policy which is duly approved by its board.

i. Types of E-Commerce Frauds

Identity Fraud

The deliberate use of someone else's identity, is a common method to make undue financial gain.

Card Testing

Card testing fraud is the practice of creating and testing the validity of a card number, in order to use it on another website to commit fraud. Fraudster target websites which give a different response for each type of decline: for example, when a card is declined due to an incorrect expiration date, a different response is given, so they know they just need to find the expiration date.

External Fraud

A. **Eavesdropping –** This way an attacker gets access to data paths in the network to "listen in" or interpret (read) the network traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping.

B. **Data Modification -** An attacker modifying the data in the packet without the knowledge of the sender or receiver.

C. **Identity Spoofing (IP Address Spoofing) -** An attacker using special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

D. **Denial-of-Service Attack -** The denial-of-service attack prevents normal use of computer or network by valid users.

E. **Sniffer Attack -** A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer gets full view of the data inside the packet.

F. **Application-Layer Attack -** An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls.

Phishing

In this case an email asks for user ID, passwords, credit card details and other personal information. The sender seems to be a credit institution that needs a confirmation of some information due to a change in the system. Phishing allows criminals to get access to bank or other accounts and it can be used for identity theft.

Others

Payment Fraud

Fraud that involves falsely creating and / or diverting payments from intended result. Payment fraud can include: creating bogus customer records and bank accounts so that false payments can be generated. Intercepting and altering payee details and amounts on cheques and Payable Orders, then attempting to cash them.

Intermediary Fraud

Fraud perpetuated by an Insurance agent / Corporate Agent / Intermediary/ Third Party Administrators (TPAs) against the insurer and / or policyholders.

ii. Manner of detecting and identifying frauds

Company has implemented various measures to deter possible e-commerce fraud -

Sr No	Type of Fraud	Fraud Indicator	Mitigation Strategies
1	Identity Fraud/Payment Fraud	Multiple policies logged from single IP	To detect fraud, Logging is enabled. Logs need to be checked & reviewed based on fraud incidents.
2	Intermediary Fraud	Premium amount collected is not deposited with FGIL	Managed by reconciliation process
3	Intermediary Fraud	Incorrect premium amount other than actual premium amount collected from policyholder/prospect customer	Managed by reconciliation process
4	Intermediary Fraud	Transaction has declined due to any reason such as server issue etc , however debited money is not returned/credited in customer account	Managed by reconciliation process
5	External Fraud	Hacker attacks on e-commerce platform and stealing customer data.	1) Ecommerce setup is protected with WAF, IPS, Malware services. 2) Systems are also protected from Botnet attacks. 3) Servers are deployed post verifications of hardening parameters & vulnerability assessments. Yearly vulnerability

			assessments are also performed.
			4) Access to the systems are controlled & provided to specific individuals based on needs.
			5) Access are reviewed on half yearly basis.
			6) Changes are governed & controlled by change management process.
			7) Backup is taken on regular basis which can be used to recover data in case of system failure.
6	Phishing	Manipulated browsers direct unsuspecting customers to fraudulent websites.	Customer Education through emailers
7	Payment Fraud	Premium paid by non-related entity to policyholder and/or proposer	Managed by reconciliation process
8	Payment Fraud	Usage of multiple transactions/medium for payment of premium for a single premium transaction. (Premium being received in split payments)	Managed by reconciliation process
9	Card Testing	Multiple failed transactions from a single card to validate card details such as card validity period, CVV number and pin	This aspect has to be managed by payment gateway partners as we re-direct the payment transactions to payment gateway partners.

- Note : Above list is not exhaustive

iii. Cooperation amongst market participants to identify frauds, building database and sharing

Based on the fraud incidents being observed, a reporting would be submitted to Regulator and other relevant repository such as Experian in the stipulated format on a timely basis.

Based on the arrangement as developed by the Company's Management, database with either/or both Regulator and Repository Service Providers would be maintained. Frequent data would be exchanged to further enhance the fraud identification, detection and management process.

6. Zero Tolerance Policy

The Company does not tolerate any unethical or dishonest behavior, even if the result of the action benefits the Company itself.

Violators will be prosecuted and may be terminated and referred to the appropriate authorities.

7. Roles and Responsibilities

7.1 Board of Directors

The Board of Directors to ensure that Senior Management lays down and implements the Fraud Management Policy.

7.2 Chief Compliance Officer

Chief Compliance Officer is entrusted with the responsibility to ensure that the monitoring of the Fraud and forgery cases across the organization and report their progress to the GC, Audit Committee and the Board at a, not later than, Quarterly frequency.

It is the responsibility of the Chief Compliance Officer to ensure that the responsible functions are aware of their duties and responsibilities in identification, monitoring and reporting of fraud along with procedure for Governance Action.

Chief Compliance Officer shall be placed at a senior management level and shall operate independently and report to Board of Directors.

7.3 Governance Committee (GC)

Governance Committee has been constituted of Senior Management Level employees. GC will comprise of Senior Representatives / Function Heads typically from Risk, Human Resource along with Chief Compliance Officer.

- GC is entrusted with the responsibility to review the volume of fraud events, facilitate to arrive at a judgment in reported / investigated cases based on the case facts and recommendations provided by the Fraud Investigating team.

- GC shall take a stock of the movement of fraud events and related action.

- GC shall meet in a period of every three months or earlier if the need arises.

7.4 Fraud Investigation Team

During the preliminary analysis, the types of resources needed to conduct the investigation are duly determined (e.g. internal audit, human resources, legal & compliance, risk management, external legal counsel, forensic auditors, technical experts, etc.). This is the so called Fraud Investigation Team.

The Fraud Investigation Team has the primary responsibility for the investigation of all suspected or alleged internal fraudulent acts as defined in this document.

Technical resources may be drawn upon as necessary to augment the investigation (e.g. Information Technology, Claims, Underwriting, etc.), provided that they are independent from the case and unbiased.

7.5 Legal & Compliance

Legal & Compliance along with Risk Management shall assist management in drafting anti fraud policies and procedures and conducting fraud awareness training, thus helping in educating employees about fraud prevention and detection.

Legal & Compliance function is in charge of implementation of the anti-fraud policy of the Company.

Legal & Compliance has to ensure that the procedures for internal reporting from / and to the various departments across the organization is laid down.

Function shall be responsible for maintaining a centralized fraud database where incidents of fraud are duly and timely recorded, capturing information such as fraud incident description, fraud perpetrator details, estimated fraud loss and recovery amounts (if any), control implications and resolution.

Legal & Compliance function co-ordinates with law enforcement agencies, for reporting frauds on timely and expeditious basis and follow-up processes thereon.

Legal & Compliance function has to ensure awareness among the employees, intermediaries and policy holders to counter insurance frauds.

Generation of meaningful reports from the fraud data for internal and external reporting as defined by Chief Compliance Officer, Governance Committee, Board of Directors, IRDAI and any other Regulatory Authority.

It is the responsibility of Legal & Compliance function to inform service providers / vendors / third parties / customers (existing and new both) about the anti-fraud policy of the Company

and also ensure that regular caution /alert messages / clauses are included in the insurance contracts/ contracts with service provides / third parties and in other relevant documents, duly highlighting the consequences of submitting a false statement and/or incomplete statement, for the benefit of the policyholders, claimants, the beneficiaries and the Company.

Legal & Compliance function shall also proactively sketch possible areas of frauds and identify and implement controls and measures to mitigate them.

7.6 Risk Management

Risk Management shall assist in identifying and assessing fraud risks and help management to design specific controls to mitigate fraud risks.

7.7 Internal Audit

Internal Audit shall assist in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness of the system of internal controls and by conducting proactive auditing to search for fraud.

In addition, by carrying out fraud audits, Internal Audit shall proactively detect indications of fraud in those processes or transactions where analysis indicates the risk of fraud to be significant or high.

On request from Management Internal Audit may support and cooperate with the Fraud Investigation Team, gathering information and making recommendations.

7.8 Audit Committee

The Audit Committee shall also ensure that senior management implements appropriate fraud deterrence and prevention measures.

The Audit Committee shall receive periodic reports describing the nature, status and disposition of any fraud or unethical conduct.

The Audit Committee shall establish an open line of communication with members of management one or two levels below senior management to assist in identifying fraud at the highest levels of the organization or investigating any fraudulent activity that might occur.

Through the Audit Committee, the Board of Directors shall be timely informed of any fraud or alleged fraud involving any member of senior management.

7.9 Employees

Employees and officers at every level, in every department, at all offices of the Company and at all the locations have a responsibility to speak up when they believe that they have knowledge or suspect that fraud is being committed. 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 party as per the laid down procedures in place.

8. Fraud Monitoring

Identification, detection and reporting of fraud are the responsibility of all employees and officers of the Company.

8.1 Probable Indicators for Fraud Detection

Following are the indicators of fraud detection which could indicate probability of occurrence of frauds; however the list is not exhaustive.

Internal Fraud	**Intermediary Fraud**	**Policyholder and/or Claims Fraud**
Unexplained wealth or living beyond apparent means, sudden change of lifestyle	Intermediary often changes address or name.	To deal with the claim quickly, the claimant is willing to accept an inexplicably low settlement.
Customer complaints and/or missing statements, unrecognized transactions	Exceptional increase of production and/or increase of production without apparent reason.	The claimant gives inconsistent statements to the police, experts and third parties.
Key managers or employees having too much control and/or authority without oversight or audit by another person	Portfolio of the broker/agent has (relatively) a lot of insurances with special characteristics*	The insured has detailed knowledge about insurance terms and the claim process.
Rising costs with no explanation	A lot of policy substitutions with complete commission.	The insured has checked the insurance coverage shortly before the claimed event.
Manager or employees with close or long–standing relationships with contractors	Insured and broker/agent are represented by the same person or have the same zip code;	The policyholder has several policies with the same insured object and coverage.
Manager or employees with external business interests	Policyholder/insured lives beyond the region were the broker/agent operates. High	The insured requests that payment is made into different accounts.

Internal Fraud	Intermediary Fraud	Policyholder and/or Claims Fraud
	insured amount by a broker/agent with a small portfolio.	
Marked personality changes of managers or employees	Broker/agent asks for payment of all commissions at once or for payment of commissions in advance.	The insured changes address, bank or telephone details shortly before a claim is made.
Fast increasing sales or change in product mix	Request for payments to be made via the broker/agent	The claimant request payment to be made to a third party.
Managers or employees who consistently work late, who are reluctant to take vacations and who seem to be under permanent stress		The claimant insists without proper reason on using certain contractors, engineers or medical practitioners or wants to use relatives.
New managers or employees who resign quickly		The way a claim is filed is remarkable (for example, the claimant used a lawyer or sought professional advice in claims reporting).
		The policyholder has been denied insurance before and has not mentioned this when applying for insurance.
		The policyholder insists on changing terms and conditions.
		Irregularity in the documentation provided during Claims or during policy request

8.2 Procedures for Reporting of Fraud

Employees shall promptly communicate any concerns about unethical behavior and report any actual or suspected incident of fraud or violations of the code of conduct or ethics policy on a confidential basis.

The Company offers several channels for reporting any actual or suspected incident of fraud. Employees and officers are encouraged to use the channel with which they are most comfortable, starting with their manager or supervisor. Other reporting channels include:

- Another Manager or Supervisor;
- The Chief Compliance Officer;
- The Chief Risk Officer;
- The Chief Human Resources Officer;
- The Head of Internal Audit;
- The Chief Executive Officer; and
- The Chairperson of the Audit Committee.

Every manager or supervisor who receives a report shall treat the concern or allegation with discretion and treat the employee who brought the concern forward with respect.

The manager or supervisor shall promptly escalate the concern to the appropriate authority i.e. Chief Compliance Officer, the Chief Human Resources Officer, the Head of Internal Audit, the Chief Executive Officer or the Chairperson of the Audit Committee, as deemed suitable. The concern can be raised with any one or more or with all the authorities.

Any concern or allegation involving senior management shall be directed directly to the Chairperson of the Audit Committee to avoid filtering by management or other internal personnel.

Any employee who suspects dishonest or fraudulent activity shall notify the abovementioned parties immediately, and should not attempt to personally conduct investigations or interviews/ interrogations related to any suspected fraudulent act.

It is the responsibility of the Authorities to ensure that concern is duly investigated in fair and transparent manner and the concern is duly addressed.

Any alleged or suspected incident of fraud shall be reported in writing so as to ensure a clear understanding of the issues raised. Anonymous disclosures or disclosures containing general, non detailed or offensive information will not be entertained.

Legal & Compliance function shall ensure that the internal reporting mechanism shall be made known and available to all the employees and third parties such as customers, vendors and other third parties who conduct business with the Company through reference in the Company's website and other external communication materials.

In addition, in order to facilitate the reporting of alleged or suspected incidents of fraud, management may set up opinion boxes and/or telephone hotlines and/or dedicated email addresses and clearly communicate their existence.

Management shall lay down an appropriate framework for a strong whistle blower policy.

8.3 Procedure for Fraud Investigation

The following actions shall be taken in response to an alleged or suspected incident of fraud:

- A thorough investigation of the incident shall be conducted.
- Appropriate and consistent actions shall be taken against violators.
- Relevant controls shall be assessed and improved.

All employees shall cooperate fully with an investigation into any alleged or suspected fraud. Details of the investigation process are as follows:

- **Logging:** The Chief Compliance Officer maintains a centralized internal fraud database where all internal fraud data losses and recoveries are logged.

  Upon discovery or reporting of an internal fraud case (by the said Authorities or by the employees or any other external party), the Chief Compliance Officer will opens a case file and log the case in the centralized internal fraud database and assigns a unique case number to the case. This enables the Company to track the resolution progress. The case must be logged within 1 working day of the discovery or reporting, as the case may be.

- **Preliminary Analysis:**
  Then, the alleged internal fraud case may be reviewed by the Chief Compliance Officer,and/or the Chief Human Resources Officerand/or the Head of Internal Audit to determine further action plan with reference to following parameters:

  a) Whether the case should be investigated;
  b) Who should investigate the case and the types of resources needed to conduct the investigation;
  c) Who will be interviewed during the course of the investigation and how information will be gathered; *(it is mandated that interview of any female person must be in the presence of another female person)*
  d) The timeframe for completion; and
  e) How results will be reported and to whom.

  The Chief Compliance Officer, the Chief Human Resources Officer and/or the Head of Internal Audit shall be excluded from the preliminary analysis or the subsequent investigations if the alleged or suspected internal fraud case involves him/her.

- **Investigations:**

  Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

The fraud investigation shall consist of gathering sufficient information about specific details and performing those procedures that are necessary to determine whether fraud has occurred, the loss or exposures associated with the fraud, who was involved in it and the fraud scheme (how it happened).

The members of the Fraud Investigation Team will have free and unrestricted access to all Company records and premises, whether owned or rented, and the authority to examine, copy and/or remove all or any portion of the contents of files, desks, cabinets and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

The alleged fraudster will be informed of the allegations as soon as reasonably practicable. This may not be done until the initial stages of the investigation have taken place.

The investigations shall take place on legal restrictions to ensure that findings and evidences are admissible in court. Investigatory or disciplinary hearings and evidence gathering will always be carried out with the assistance and under the supervision of legal counsel (either internal and/or external).

The Fraud Investigation Team shall take into custody all relevant records, documents and other evidence to protect them from being tampered with, destroyed or removed by the suspected perpetrators of fraud or by any other party under his/her influence. The full records of the investigation, including interview notes, shall be kept secure.

The investigations shall be kept as confidential and private as possible to ensure the least amount of disruption to the Company and maintain the process integrity at all times.

Confidential information will be shared only on a "need-to-know" basis.

The investigations shall be completed within forty-five (45) days from the disclosure or discovery of the fraud case. Any further extension for time line for investigation must be reviewed and approved by the Group of Authorities.

The conclusion and results of the investigations must be duly documented in writing in the form of Fraud Investigation Report (FIR). The FIR to include following

- Fraud incident description
- Results of the investigations
- Details of the corrective actions,
- The fraud perpetrator details,
- The estimated fraud loss and recovery amounts,
- The controls implications and the resolution.

Management is responsible for resolving fraud incidents are resolved completely.

The summary of FIR will be presented to the Board of Directors through the Audit Committee and the Chief Executive Officer of the Company.

Post completion of the Investigations and identification of the risk findings thereafter the Legal & Compliance function and / or Human Resource shall initiate and take necessary action by approaching Law Enforcement Agencies or any other authority, whenever and wherever appropriate.

- **Decision:**

Once the investigation is completed and if it substantiates that fraudulent activities have occurred, the Fraud Investigation Team shall recommend to the Governance Committee to take such disciplinary or corrective actions (e.g. employee discipline, any referral to the applicable law enforcement agency, changes to processes or internal controls, etc.), as the Fraud Investigation Team may deem fit.

Disciplinary or corrective actions may include: employee dismissal; business process remediation and/or internal control remediation (i.e. determine whether internal procedures or controls need to be changed); termination of a contract; restitution agreement with the perpetrator; criminal prosecution, i.e. referral of the case to law enforcement authorities; civil lawsuits against the perpetrator to recover stolen funds; internal disciplinary action such as termination, suspension with or without pay, demotion or warnings; etc.

All actions taken in response to an established act of fraud must be approved by the Chief Executive Officer of the Company or Chairman of the Audit Committee or by the Board of Directors of the Company (whenever an authority exceed the limits granted to him/her by the Board).

Any decisions to prosecute by way of civil proceedings or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be taken in conjunction with legal counsel by the Governance Committee or Chairman of the Audit Committee or by the Board of Directors of the Company (whenever the Authority exceed the limits granted to him/her by the Board), as will finalize the decisions on disposition of the case.

The Audit Committee will be timely informed of such decisions either through its Chairperson (in case of urgency) or at the subsequent scheduled meeting of the Committee.

The Fraud Investigation Team will monitor the implementation of the resolution to ensure that proper corrective action was taken and report to the Audit Committee accordingly.

Only after the resolution has been verified, the case can be closed.

- **Reporting:**

The Chief Compliance Officer will keep track of all cases and timely and periodically submit a report to the Audit Committee about the status and results of the investigations and corrective actions taken, along with the report of the investigators.u

8.4 Fraud Prevention & Control

The Company values integrity, honesty and fairness in everyone from the top to the bottom. It encourages openness to prevent malpractice or any cover-up of malpractice and create a positive workplace environment where employees have positive feelings about the Company and the Group and do not feel abused, threatened or ignored;

The Board of Directors, managers and officers set the "tone at the top" for ethical behavior by behaving ethically and openly communicating expectations for ethical behavior to employees;

Integrity is a requirement of anyone within the Company, as reflected in the Code of Conduct and Governance Policy of the Company, which guide employees in making appropriate decisions during their workday;

The Code of Conduct and Governance Policy of the Company, as well as the measures take towards commitment to fraud risk management, are communicated to all personnel in an understandable fashion. They are clearly communicated to all officers and staff members of the Company through several means (including but not limited to the employee manual, the company website, intranet, training courses, etc.).;

All employees including senior management employees are required to sign (either electronically or manually) a confirmation statement at least annually, acknowledging that they have read, understood and complied with the Code of Conduct, Governance Policy Statement of the Company and the Anti-Fraud Policy Statement of the Company;

The confirmation statement shall include statements that the individual understands the Company's expectations and has complied with the Code of Conduct and is not aware of any incidents of alleged or suspected fraud or violations of the Code of Conduct other than those the individual lists in his/her response. Any non replies shall be followed up thoroughly by Human Resources;

Regular and periodic training (including new-hire orientation and refresher training) shall be provided to all personnel, upon joining the organization and throughout their association with the Company, in order to clearly communicate expectations for ethical behavior to staff members;

Such training shall also include an element of "fraud awareness" and communication of responsibilities. As far as possible, training should be specific to the employee's level within the Company, geographic location and assigned responsibilities. Examples of the types of fraud that could occur and the potential perpetrators shall be provided in the course of the training;

Realistic business objectives and targets and sufficient resources are allocated to the Board of Directors, Senior Management and other staff to meet them;

Processes within the Company which are highly vulnerable to internal frauds shall be identified by all the control functions (Underwriting, Risk Management, Internal Audit and Legal & Compliance) and possible controls instituted for each of the fraud areas;

Personnel records are kept complete and contain all information on the recruitment of Board members, senior managers and other staff. Records are retained for an adequate period of time after the person in question has left the insurer.

In addition following activities will be undertaken to prevent and control fraud instances:

- During recruitment background checks are performed to check whether any false information, such as false employment history, false references and certificates or false identity is provided by the applicant;
- Pre-employment and in-employment screening of permanent or temporary employees and staff shall be performed.
- Preventive policies, procedures and controls are drafted and implemented;
- Issuance of office manual and internal guideline on ethical behavior for management and staff;
- Maintaining adequate supervision of management and other staff;
- Eliminating potential areas of conflicts of interest between the insurer, Board members, senior managers and other staff;
- Dividing the function that may cause or be susceptible to conflicts of interest;
- Four eyes principle is followed (involvement of maker-checker in decision making or other material activities for reasons e.g., of validation, proper governance, transparency and control);
- Adequate Segregation of functions establishing efficient physical and procedural safeguards over the use, handling and availability of cash, other assets and transactions as well as of information systems;
- Cash and Money flows are dealt by more than one person so as to establish clear reporting lines and communication procedures;
- Common mail ids / contact nos. for reporting of frauds being published on Company intranet sites;
- No concession KYC and related documentation prior to issuance of policy;
- Clearly drafted guidelines and policies for Client identification, verification and risk assessment with periodic reviews;
- Maker –Checker concept for high profile cases;
- Reporting of suspected fraudulent cases to FIU;
- Complaints management team is established to record and act on the Mis-selling cases;
- Claims Committee is established to review the Claims cases to arrive at an appropriate decision for acceptance and rejection of Claims cases;
- Operating Limits Handbook in place which defines the delegation of powers is appropriately distributed and the document is reviewed at a yearly frequency;

- Quarterly Compliance Certification from the Function heads with regards to conformation of no fraudulent transactions within the function and / or with other related stake holders;
- Terms of business agreements that have to be completed are signed by the intermediaries;
- Periodic review of policies and procedures by the Control functions and findings presented to the Board level Committee.

9. Confidentiality

The Fraud Investigation Team shall treat all information received confidentially.

The detailed investigation results shall not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct.

10. Protection

No unfair treatment will be reserved to the person who has reported in good faith a suspected or alleged incident of fraud.

As a policy, the Company condemns any kind of discrimination, retaliation, harassment, victimization or any other unfair employment practices being adopted against the person who has reported in good faith a suspected or alleged incident of fraud.

Complete protection will be given to the person who has reported in good faith a suspected or alleged incident of fraud against any unfair practice like retaliation, threat or intimidation of termination/ suspension of service, disciplinary action, transfer, demotion, refusal of promotion, etc.

The identity of the person who has reported the suspected or alleged incident of fraud shall be kept confidential to the extent possible and permitted under the law.
However, any abuse of this protection (for example, any false or bogus allegations made by a person knowing them to be false or bogus or with a mala fide intention) will warrant disciplinary action.

If an employee or an officer reports a suspected or alleged incident of fraud for personal gain or to disrupt the working environment or, by making the disclosure, would be committing a criminal offence such as blackmail, he/she would not get any protection and his/her behavior would also constitute a disciplinary offence.

11. Fraud Communications

Fraud investigations shall be communicated on a strictly no-name basis and without any references or evidence through intranet messages, specific messages, newsletters and/or other regular communication to business managers.

Sharing fraud knowledge across the Company allows business managers to learn from past incidences in other parts of the business, quickly improve internal control deficiencies in their purview, minimize repeat incidences of fraud and detect fraud by assessing if fraud schemes identified in other areas have also manifested themselves in their area.

Furthermore, alleged, credible or proven fraud cases (either internal or external) shall be reported to the following parties as per the table below:

Type of Fraud	Fraud Incident Reporting				
	Principal Compliance Officer	Head of Internal Audit	Chief Risk Officer	Chief Executive Officer	Audit Committee
Internal Fraud (either alleged, credible or proven)	All	All	All	All	All
External Fraud (either alleged, credible or proven)	All	All	All	Above a defined Threshold	Above a defined Threshold
Frequency of Fraud Incident Reporting	As soon as it occurs	As soon as it occurs	As soon as it occurs	As soon as it occurs	Quarterly

The Fraud Incident Reporting shall capture crucial information regarding each fraud incident, including description, fraud perpetrator details, loss and recovery estimates, control implications and proposed or completed actions taken.

The Chief Financial Officer shall be provided with a summary of internal fraud cases (either alleged, credible or proven) that may jeopardize financial reporting.

(Alleged Fraud = an act of fraud has been reported.
Credible Fraud = an allegation of fraud has been reported and appears reasonably likely that the allegation will be substantiated as fraud in whole or in part. The case has not been fully resolved.
Proven Fraud = an act of fraud has been reported, thoroughly investigated and resolved)

12. Reporting

The Chief Compliance Officer maintains the data and prepares relevant reports to be presented to the Senior Management and Board of Directors at not later than a period of 3 months.

Legal & Compliance function will ensure that the reports as prescribed by IRDAI will be updated and submitted to the authority within the specified timelines.

The current format for internal and external reporting is attached as Appendix – 2 *.

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; and
(ii) closed fraud cases

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

* This format may subject to change. Legal & Compliance to ensure use of current format as per Company and/or IRDAI guidelines.

13. Review

The Legal & Compliance along with Enterprise Risk Management team shall be responsible to review and update the Anti-fraud policy at yearly basis or earlier if the need arises. The Chief Compliance Officer shall submit the revised/updated policy to the Board of Directors for review and approval.

14. Approval

Board of Directors authorizes any change in the Anti-Fraud Policy upon having heard due recommendations from the Chief Compliance Officer.

15. Audit

In the event that the Internal Audit function were to deem appropriate, Fraud Management process may be subject to audit activities including adequateness of human resources, capacity to handle the size and complexity of data of the systems, timeliness and usefulness of reports, decision making and sign-off procedures, adequateness of the organizational structure, amongst others.

16. Annexure

Appendix – 1

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/TPAs and the policyholders/ their nominees. Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

1. Internal Fraud:

a) misappropriating funds
b) fraudulent financial reporting
c) stealing cheques
d) overriding decline decisions so as 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 favored suppliers, for kickbacks/favors
h) forging signatures
i) removing money from customer accounts
j) falsifying documents
k) selling insurer's assets at below their true value in return for payment.

2. Policyholder Fraud and Claims Fraud:

a) Exaggerating damages/loss
b) Staging the occurrence of incidents
c) Reporting and claiming of fictitious damage/loss
d) Medical claims fraud
e) Fraudulent Death Claims

3. Intermediary fraud:

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) Commission fraud - insuring non-existent policyholders while paying a first premium to the insurer, collecting commission and annulling the insurance by ceasing further premium payments.

Appendix – 2

FMR – 1

Fraud Monitoring Report

Name of the Insurer:

Part I

Frauds Outstanding- Business segment wise *:

Sl. No.	Description 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)
	Total								

Part II

Statistical details: (unresolved cases as at end of the year) –Business segment wise*

Sl. No.	Description of Fraud	No. of Cases	Amount Involved (` lakh)

	Total		

Part III

Preventive and Corrective steps taken during the year- Business segment wise*

Sl.No.	Description of the fraud	Preventive/Corrective action taken

Part IV

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								

* Business segments shall be as indicated under IRDA (Preparation of Financial Statements and Auditor's Report of Insurance Companies) Regulations, 2002

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

FMR – 2

Fraud Cases closed during the year

Name of the Insurer:

Sl. No.	Basis of closing a case	Number of cases closed
i.	The fraud cases pending with CBI/Police/Court were finally disposed off	
ii.	The examination of staff accountability has been completed	
iii.	The amount involved in the fraud has been recovered or written off	
iv.	The insurer has reviewed the systems and procedures; identified the causative factors; has plugged the lacunae; and the portion taken note of by appropriate authority of the insurer (Board, Committee thereof)	
v.	Insurer is pursuing vigorously with CBI for final disposal of pending fraud cases, staff side action completed. Insurer is vigorously following up with the police authorities and/or court for final disposal of fraud cases	
vi.	Fraud cases where: The investigation is on or challan/ charge sheet not filed in the Court for more than three years from the date of filing of First Information Report (FIR) by the CBI/Police; or Trial in the courts, after filing of charge sheet / challan by CBI / Police has not started, or is in progress.	

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:

For reporting purposes, only in the following instances of fraud cases can be considered as closed:

1. The fraud cases pending with CBI/Police/Court are finally disposed of.
2. The examination of staff accountability has been completed
3. The amount of fraud has been recovered or written off.
4. The insurer has reviewed the systems and procedures, identified the causative factors and plugged the lacunae and the fact of which has been taken note of by the appropriate authority of the insurer (Board / Audit Committee of the Board)
5. Insurers are allowed, for limited statistical / reporting purposes, to close those fraud cases, where:

    1. The investigation is on or challan/ charge sheet not filed in the Court for more than three years from the date of filing of First Information Report (FIR) by the CBI/Police, or
    2. The trial in the courts, after filing of charge sheet / challan by CBI / Police, has not started, or is in progress.

Insurers should also pursue vigorously with CBI for final disposal of pending fraud cases especially where the insurers have completed the staff side action. Similarly, insurers may vigorously follow up with the police authorities and/or court for final disposal of fraud cases and / or court for final disposal of fraud cases.

*****End****