Future Generali India Insurance Company Limited

Anti – Fraud Policy

(Version 6.0)

DOCUMENT SUMMARY

Title	Anti-Fraud Policy (hereinafter referred to as “the Policy”)
FGII Classification	Internal & External
Document code	FGII/FCU/20-21/26
Approved by	The Board of Directors
Effective date	February 9, 2021
Accountable Function	FCU
Key contact	Virendra Batra

CHANGE / HISTORY LOG

Version No.	Rollout Date	Changed by	Approved by	Purpose of revision
1	August 5, 2011			Revised
2.	May 31, 2013			Revised
3.	May 30, 2014			
4.	May 21, 2015			
5.	May 5, 2016			Reviewed No Changes
5.	August 11, 2017			
	12-May-2018			Reviewed No Changes
	14-May-2019			Reviewed No changes
	5-June-2020			Reviewed No Changes
6	9-Feb-2021			Reviewed changes

REGULATORY REFERENCES

Guidelines for Corporate Governance for Insurers in India read with applicable provisions of guidelines, notifications, advisories, if any, issued by Insurance Regulatory and Development Authority of India (IRDAI) and Companies Act, 2013

FUTURE GENERALI
TOTAL INSURANCE SOLUTIONS

INDEX

I. DEFINITIONS & ABBREVIATIONS:

a. "**Act**" means the Insurance Act, 1938 (4 of 1938) as amended from time to time;

b. "**Authority**" means the Insurance Regulatory and Development Authority of India established under the provisions of Section 3 of the Insurance Regulatory and Development Authority Act, 1999 (41 of 1999).

c. **"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.

Explanation

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 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:

Claims Fraud: Fraud against the insurer in the execution of an insurance product by obtaining wrongful payment;

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

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

- *Internal Fraud:* Fraud/ misappropriation against the insurer by its Director, Manager and/or any other officer or staff member (by whatever name called)

- *Third Party Fraud*: Fraud committed by third parties against the Insurer and the general public which primarily includes activities such as the issue of fake/forged policies and cover notes in the name of the Insurer.

- *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 –

    - *Buyer side frauds:* Where buyers file fraudulent claims, chargebacks or compromised payment cards.
    - *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.
    - *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 the Company systems
    - Other Frauds – Any other type of online fraud which does not fall under either of the above three sub-categories.

On the other hand, occupational fraud (a.k.a. internal fraud) is defined as the 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.

Fraud comes in all shapes and sizes. It may be a simple act involving one person or it may be a 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 report fraud (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;
- 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;
- Electronic Fraud and/or illegal hacking
- 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.

All occupational frauds fall into one of three major categories, according to the Uniform Occupational Fraud Classification System (commonly known as the "Fraud Tree"):

- Asset Misappropriation, which involves the theft or misuse of an organization's assets. Common examples include skimming revenues, stealing inventory and payroll fraud. The essential difference between fraud and theft is "deception". A theft does not necessarily involve deception, but fraud must involve deception in order to be termed as a fraud;

- Corruption, in which fraudsters wrongfully use their influence in a business transaction in order to procure some benefit for themselves or another person, contrary to their duty to their employer or the rights of another. Common examples include accepting kickbacks and engaging in conflicts of interest; and

- Fraudulent Statements, which generally involve falsification of an organization's financial statements. Common examples include overstating revenues and understating liabilities or expenses.

Please refer to *Attachment - I* and *Attachment - II* for the complete Fraud Tree and corresponding definitions. Occupational fraud is perpetrated by people who use their positions within the organization for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets.

The more reliance an organization places on an employee, the more autonomy and authority an employee receives, the greater the risk of fraud. Therefore, to strike the right balance between oversight and trust is the key in any effective anti-fraud program.

Fraud may be perpetrated to the detriment of the organization or be designed to benefit the organization itself. The latter generally produces such benefit by exploiting an unfair or dishonest advantage that may also deceive an outside third party.

Perpetrators of such acts usually accrue an indirect personal benefit, such as management bonus payments or promotions; improper payments, such as illegal political contributions, bribes and kickbacks, as well as payoffs to government officials, intermediaries of government officials, customers or suppliers; intentional and improper transfer pricing (e.g. valuation of goods exchanged between related organizations); intentional errors in tax compliance; prohibited business activities.

II. OBJECTIVE

The objective of this Policy is to lay down the framework for effective deterrence, prevention, detection and mitigation of frauds.

III. SCOPE

A. **Fundamental Elements of the Policy**:

This document identifies the measures that Future Generali India 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 via 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 the various types of fraud; and

(3) Develop an appropriate oversight process.

B. 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 by the Company including in case of e-commerce fraud;

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 any and all suspected 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.

C. **Applicability of the Policy**:

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.

IV. ADOPTABLE MEASURES

(a) 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/ pressures[1]; market pressures to meet financial targets or goals; etc.);

- Opportunity: circumstances exist that provide an opportunity to commit fraud, such as ineffective or absent 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[2].

In order for fraud to occur, all three elements of the triangle need to be present.

1 Such as a spouse who loses a job; living beyond one's means; high personal debt; gambling, drugs, affairs; undue pressure to succeed; etc. 2 Typical examples of rationalization include: "I am just borrowing this money"; "Everybody does it"; "I am not hurting anyone"; "The Company can afford it"; etc.

(b) 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 third parties without any assistance or collision 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.

Generally speaking, internal fraud (hereinafter referred to as "fraud") is defined as any intentional act or omission designed to deceive others performed by one or more staff

members directly or by way of third parties, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

External Fraud on the other hand includes fraudulent activities committed by third parties to defraud the Company by issuing fake/forged policies and cover notes in the name of the Company, selling such policies to the members of the general public and collecting money from them, eventually resulting in defrauding the Company as also the general public.

(c) ZERO TOLERANCE POLICY

The Company does not tolerate any unethical or dishonest behaviour, 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.

(d) FRAUD RISK GOVERNANCE - CREATING A CULTURE OF HONESTY AND HIGH ETHICS

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 behaviour by behaving ethically and openly communicating expectations for ethical behaviour to employees.

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

The Ethical Code and the Code of Business Conduct, as well as a 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 within senior management, claims and finance function, as well as other employees in areas that are exposed to the risks of unethical behavior (e.g. procurement, claims handling, sales and marketing) 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 Business Conduct and the Internal Fraud Policy Statement of the Company.

The confirmation statement shall include statements that the individual understands

the Company's expectations, has complied with the Code of Business Conduct and is not aware of any incidents of alleged or suspected fraud or violations of the Code of Business 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 behaviour to staff members.

Such training shall also include an element of "fraud awareness" and communication 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.

Directors, employees and contractors shall internally self-disclose potential or actual conflicts of interest, according to the procedures contained in the Code of Business Conduct.

As part of the Company's due diligence for fraud detection & mitigation, background checks on new employees and personnel (management and staff) / insurance agent / corporate agent / intermediaries etc (including the educational background, work experience, criminal records, etc.) shall be carried out in order to prevent fraud at the source. Background checks shall be duly formalized and documented in writing.

Exit interviews shall be conducted with terminated, resigning or retiring employees regardless of their position to identify potential fraud and vulnerabilities to fraud that may be taking place in the Company.

Furthermore, staff rotation and tying employee evaluations to ethics or compliance reviews and internal control reviews can also help to prevent fraud at the source.

(e) FRAUD RISK ASSESSMENT - EVALUATING THE RISKS OF FRAUD AND IMPLEMENTING ANTIFRAUD PROCESSES AND CONTROLS

The Company shall be proactive in reducing fraud opportunities by (1) identifying and measuring fraud risks, (2) taking steps to mitigate identified risks (including IT and cyber security risks), (3) implementing and monitoring appropriate preventive and detective internal controls and other deterrent measures and (4) coordinating with law enforcement agencies.

The Management has the primary responsibility for establishing and monitoring all aspects of the Company's fraud risk assessment and prevention activities and performing the fraud risk assessment.

Individuals from throughout the organization with different knowledge, skills and perspectives (e.g. accounting/finance, nonfinancial business units and operations

personnel, legal & compliance, risk management, internal audit, etc.) shall be involved in the fraud risk assessment.

Through the fraud risk assessment, the vulnerability of the Company to fraudulent activities (for example, misappropriation of assets, corruption, fraudulent financial reporting, etc.) is considered, as well as whether any of those exposures could result in a material misstatement of the financial statements or material loss to the Company. The fraud risk assessment shall identify where fraud may occur and who the perpetrators might be.

The nature and extent of the fraud risk assessment shall be commensurate with the size of the Company and the complexity of its operations.

It shall be performed, documented and updated periodically to identify potential fraud schemes, scenarios and events that need to be mitigated. Updates shall include considerations of changes in operations, new information systems, changes in job roles and responsibilities, internal audit findings, new or evolving industry trends, amongst others.

The fraud risk assessment shall be performed at all appropriate levels within the organization (i.e. entity level; significant account balance or business cycle/process level; and significant locations or business units) and shall be coordinated with the operational risk assessment.

The fraud risk assessment shall include fraud risk identification, fraud risk likelihood and significance and fraud risk response.

Although management has the primary responsibility for performing the fraud risk assessment, it is also critical that employees outside of management are involved in the fraud risk assessment. It is important that the business process owners or those who have significant knowledge, control or influence over the activities within a significant business process or cycle are involved in the fraud risk assessment exercise.

Once the fraud risk assessment has taken place, management shall reduce and eliminate identified fraud risks by making changes to the Company's activities and processes and identify the processes, controls and other procedures that are needed to mitigate the identified fraud risks.

Effective and appropriate internal controls, whether automated or manual, which include a well- developed control environment, an effective and secure information system and appropriate control and monitoring activities, are essential to reduce and eliminate identified fraud risks.

Risk Management Committee shall play an active role in the development, monitoring and ongoing assessment of the fraud risk management program of the

Company. Specifically, Internal Audit shall independently evaluate whether internal controls designed to reduce the risk of fraud are adequate and effective.

Chief Risk Officer shall assist management throughout the fraud risk assessment exercise, review the result of the assessment, independently assess the ability of existing controls to prevent the occurrence of fraud, propose corrective measures and present the outcome of the fraud risk assessment to the Risk Management Committee for their review and comments.

The Company shall implement such controls on its Insurance Self Network Platform (ISNP) that prevent and deter any online fraudulent transactions. In the case of the frauds identified on the ISNP, the assistance of the Chief Information and Security Officer shall be taken. Investigation process for frauds identified on the ISNP shall be as per the process implemented for investigation for any fraud detected in accordance with this Policy.

ISNP frauds which have been proven and action has been taken against the culprits, the Fraud Control Unit maintains a database of such cases and shall share such details with other Insurance

Companies (market participants) and the General Insurance Council and such other regulatory authorities/government bodies etc in order to make them aware of such fraudulent activities.

(f) FRAUD IDENTIFICATION, INVESTIGATION AND REPORTING

EXTERNAL FRAUD

I. Management shall identify and establish a Fraud Control Unit either as a stand-alone unit or as part of the operational units (e.g. claims, procurement, investments, etc.) with the objective of defining and implementing procedures and controls to prevent and detect external fraud.

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

III. Staff members are required to be alert and vigilant with respect to external frauds. If any external fraud comes to the attention of a staff member, he/she must immediately report the same to the department/branch manager. In the event of details received in respect of a fake/forged policy by the customer service department or by any other employee of the Company, they must immediately contact the concerned persons/complainant/aggrieved customer

and obtain in writing the complete facts and details in relation to such sale of fake/fraudulent policy to them and also obtain such person's personal contact details.

IV. As soon as practicable, the related department/branch manager shall report any suspected or alleged external fraud case to the Fraud Control Unit for arranging an investigation into the incident and to the Principal Compliance Officer if the suspicious incident may involve a breach of any relevant law or regulation or any investigation by a regulatory body.

INTERNAL FRAUD

Reporting Procedures - Communicating Concerns about Alleged or Suspected Fraud

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

II. 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 Principal Compliance Officer;
- The Head of Human Resources;
- The Head of Internal Audit;
- The Chief Information Security Officer (CISO)
- The Chief Executive Officer;
- The Head of Fraud Control Unit; and
- Chief Risk Officer
- Chief Operating Officer

III 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.

IV The manager or supervisor shall promptly escalate the concern to the Principal Compliance Officer, the Head of Human Resources, the Head of Internal Audit, the Chief Executive Officer; the Head of Fraud Control Unit or the Chief Risk officer, Chief Operating Officer .

V 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.

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

VII 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.

VIII As well as to employees, the internal reporting mechanism shall be made known and available to third parties such as customers, vendors and other third parties who conduct business with the Company through reference on the Company's website and other external communication materials.

IX 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.

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

Due Diligence

The Company will ensure that pre employment verification is done before appointing persons for every job. Similarly, steps will be taken to ascertain the antecedents of insurance agent/corporate agent/intermediary/TPAs before appointment/agreements with them. The respective function of the Company shall conduct proper due diligence for Vendor/insurance agent/corporate agent/intermediary/TPAs before appointment/agreement with the Company and FCU shall conduct a random base check of the same on quarterly basis.

Fraud Investigation, Fact Finding & Corrective Action

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.
- Communication and training shall occur to reinforce the Company's values, code of conduct and expectations.

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

Logging: The Fraud Control Unit 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, the Fraud Control Unit opens a case file, logs the case in the centralized internal fraud database and assigns a case number to the case. This enables the Company to track the resolution progress.

Preliminary Analysis: Then, the alleged internal fraud case is reviewed jointly by the Principal Compliance Officer, the Head of Human Resources, the Head of Fraud Control Unit and the Head of Internal Audit to determine:

- Whether the case should be investigated;
- Who should investigate the case;
- The types of resources needed to conduct the investigation;
- Who will be interviewed during the course of the investigation and how information will be gathered;
- The timeframe for completion; and
- How results will be reported and to whom.

The Principal Compliance Officer, the Head of Human Resources, the Head of Fraud Control Unit 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.

The Chief Risk Officer and the Chief Executive Officer shall be duly and promptly informed of the results of the preliminary analysis.

Fraud Control Unit: The Fraud Control Unit 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.

Investigations: Great care must be taken by the Fraud Control Unit 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 Control Unit 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 until the initial stages of the investigation have taken place.

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

The Fraud Control Unit 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 normally within forty-five (45) days from the disclosure or discovery of the fraud case, however based on the facts and circumstances of each case, the period may be extend beyond 45 days.

The conclusion and results of the investigations must be duly documented in writing. The fraud report regarding the results of the investigations and the corrective actions shall capture at least the fraud incident description, the fraud perpetrator details, the estimated fraud loss and recovery amounts, the controls implications and the resolution. Management is responsible for resolving fraud incidents.

The summary of fraud identified and action taken will be placed before Board through the Risk Management Committee

Once investigations are completed and risk findings are identified, thereafter the FCU team shall initiate and take necessary action by approaching Law Enforcement Agencies after approval from competent authority whenever appropriate.

Decision: Once the investigation is completed and if it substantiates that fraudulent activities have occurred, the Fraud Control Committee shall recommend to the Chief Executive Officer of the Company 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 Control Committee 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 Fraud Control Committee

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 Chief Executive Officer of the Company or by the Board of Directors of the Company (whenever they exceed the authority limits granted to him/her by the Board), as will final decisions on disposition of the case.

The Risk Management Committee will be informed at the subsequently scheduled meeting of the Committee.

The Fraud Control Unit will monitor the implementation of the resolution to ensure that proper corrective action was taken and report to the Risk Management Committee accordingly.

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

Reporting: The Head of Fraud Control Unit will keep track of all cases and timely and periodically submit a report to the Risk Management Committee about the status and results of the investigations and corrective actions taken, along with the report of the investigators.

CONFIDENTIALITY

The Fraud Control Unit shall treat all information received confidentially.

The detailed investigation results will 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.

PROTECTION

No unfair treatment will be reserved for 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 offense such as blackmail, he/she would not get any protection and his/her behavior would also constitute a disciplinary offense.

FRAUD CONTROL COMMITTEE

Under the supervision of the Chief Executive Officer of the Company, the Risk Management Function shall establish a Fraud Control Committee ('FCC') to ensure the effective implementation of this Policy or any amendments thereof.

The FCC shall be responsible for the following:

i. Laying down procedures for internal reporting from/and to various departments.
ii. Creating awareness among employees/intermediaries/policyholders to counter insurance frauds.
iii. Furnishing various reports on frauds to the Authority as stipulated in this regard.
iv. Furnish periodic reports to the Board of the Directors of the Company.

FRAUD COMMUNICATIONS (I.E. FRAUD INCIDENT REPORTING)

The Company shall formalize the information flow amongst the various operating departments as regards insurance frauds.

For this purpose, 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.

In addition, the fraud database information shall be shared with all other insurers through the General Insurance councils or any other common forum and a well-advised coordination platform shall be maintained.

Alleged, credible or proven fraud cases (either internal or external) may be reported to the following parties as per the table underneath:

Type of Fraud	**Fraud Incident Report Recipient**					
	Head of Fraud Control Unit	Head of Internal Audit	Principal Compliance Officer	Chief Risk Officer	Chief Executive Officer	COO
Internal Fraud (either alleged [3], credible [4] or proven [5])	All	All	All	All	All	All
External Fraud (either alleged, credible or proven	All	All	All	All	All	All
Any type of Online or Cyber fraud	All	All	All	All	All	All
Frequency of Fraud Incident Reporting	As soon as it occurs	Quarterly	Quarterly occurs	Quarterly	Quarterly	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.

At the meeting, the Risk Management Committee shall be provided with a condensed report for review of reported fraud cases [either internal (all cases) or external (above a defined threshold)], trends, early results from investigations underway and remediation taken by management to address any identified control weakness.

Any public communications and comments by management to the press, law enforcement. All public communication or other external parties in relation to incidents of fraud shall only be made

by authorized spokespersons and coordinated through legal counsel and corporate communications.

[3] Alleged Fraud = an act of fraud has been reported. [4] 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. [5] Proven Fraud = an act of fraud has been reported, thoroughly investigated and resolved.

REPORTS TO THE AUTHORITY

Based on the data received in the prescribed format from the Fraud Control Unit, the Legal & Compliance Function shall file a report on statistics on various fraudulent cases which come to light and action took thereon to the Insurance Regulatory and Development Authority ("IRDA") in forms FMR 1 and FMR 2 (as prescribed by IRDA vide it's Circular bearing ref. no. IRDA/SDD/MISC/CIR/009/01/2013, dated January 21, 2013) providing details of:

(i) Outstanding fraud cases; and

(ii) Closed fraud cases

every year within 30 days of the close of the financial year, i.e. on or before the 30th of April.

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 is also 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.

The Company shall also duly report any health claim fraud committed by any of the service providers empanelled by the Company to the Screening Committed appoint by the General Insurance Council (GIC) to investigate and decide whether fraud has been committed. The Company shall adhere to the procedures laid down under the Protocol for Action against Fraud issued by the General Insurance Council on July 12, 2017.

FUTURE GENERALI
TOTAL INSURANCE SOLUTIONS

Attachment II

DEFINITIONS:

- **Asset Misappropriation:** it involves the theft or misuse of an organization's assets. Common examples include skimming revenues, stealing inventory and payroll fraud.

  - **Cash Misappropriation** falls within one of three categories:

    - **Fraudulent Disbursements:** the perpetrator causes his/her organization to disburse funds through some trick or device. Common examples include submitting false invoices or forging company checks. Fraudulent Disbursements can generally be divided into five distinct categories:

      - **Billing Schemes:** a fraudster causes the victim organization to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.

      - **Payroll Schemes:** an employee causes the victim organization to issue a payment by making false claims for compensation.

      - **Expense Reimbursement Schemes:** an employee makes a claim for reimbursement of fictitious or inflated business expenses.

      - **Check Tampering:** the perpetrator converts an organization's funds by forging or altering a check on one of the organization's bank accounts, or steals a check the organization has legitimately issued to another payee.

      - **Register Disbursement Schemes:** an employee makes false entries on a cash register to conceal the fraudulent removal of currency.

  - **Skimming:** cash is stolen from an organization before it is recorded on the organization's books and records.

  - **Cash Larceny:** cash is stolen from an organization after it has been recorded on the organization's books and records.

- **Corruption:** fraudsters wrongfully use their influence in a business transaction in order to procure some benefit for themselves or another person, contrary to their duty to their employer

or the rights of another. Common examples include accepting kickbacks, and engaging in conflicts of interest.

- **Fraudulent Statements:** it generally involves the falsification of an organization's financial statements. Common examples include overstating revenues and understating liabilities or expenses.

V. IMPLEMENATION & COMMUNICATION

1. **Implementation of the Policy**:

Management is responsible for designing and implementing systems, procedures and internal controls for the prevention and detection of fraud commensurate with the nature and size of the organization and, along with the Board of Directors, for ensuring a culture and environment that promotes honesty and ethical behaviour.

It is the responsibility of the Chief Executive Officer of the Company to initiate and support such measures. The Chief Executive Officer shall, for effective implementation of the Policy, designate the officer of the Company as "Policy Owner" who shall as per the applicable provisions of the Regulations, Acts and this Policy take appropriate action for effective implementation of the Policy, with support of management team and as per guidance of the Chief Executive Officer, Board and Committees of the Board.

The Chief Executive Officer of the Company is responsible for the administration, revision, interpretation and application of this Policy, as well as of the related Internal Fraud Policy Statement.

Each member of the management team shall be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of irregularity.

Risk Management Committee:

Through the Risk Management Committee, the Board of Directors shall evaluate management identification of fraud risks, implementation of anti-fraud measures and creation of the appropriate "tone at the top".

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

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

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

Employees and Officers:

Employees and officers at every level, in every department and at every location have a responsibility to speak up when they believe that they have the knowledge or suspect that fraud is being committed. As soon as it is learned 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 current procedures in place.

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.

Internal Audit shall support and cooperate with the Fraud Control Unit, gathering information and making recommendations.

In addition, Internal Audit shall be responsible for uploading information in relation to incidents of internal fraud in the group fraud scheme database in order to support the development of fraud audit programs and facilitate audit planning.

Risk Management:

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

Legal & Compliance:

Legal & Compliance shall assist FCU in (a) drafting anti-fraud policies and procedures and (b) conducting fraud awareness training, thus helping in educating employees about fraud prevention and detection.

2. **Communication of the Policy**:

The Policy Owner / FCU has responsibility for the communication of the Policy to the employees and other stakeholders for its effective implementation

3. Overriding Effect:

a) The meaning of the words / terms used in this policy shall be in accordance with applicable IRDAI Regulations read with provisions of the Corporate Governance Guidelines for Insurers in India and other applicable Regulations, Guidelines and Notifications issued by Insurance Regulatory and Development Authority of India (IRDAI) from time to time and in force.

b) It is further clarified that in the event any further changes / amendments are made to the aforesaid said Regulations, the changes shall deem to be part of the Policy and be stand implemented from the date of effect of such changes / amendments in the Regulations and unless the Policy Owner has made the requisite change in the provisions of the Policy, this Policy shall in its next review cycle be duly amended and placed before the Board for its noting.

4. Custody of the Policy:

The Policy Owner shall keep the custody of the original copy of the Policy and shall provide to the Compliance Team a soft copy of the Policy.

VI. REVIEW PROCESS

Periodicity of Review:

The Policy Owner shall ensure that the Policy is reviewed and approved by the Board of Directors at least once annually, subject to it being first reviewed and recommended to the Board for approval by the Risk Management Committee and Legal & Compliance.