Generali Central Insurance Company Limited

Anti - Fraud Policy (2026)
(under Insurance Fraud Monitoring Framework)

Version 8.0

GCI Fraud Risk and Surveillance

GCI POLICY
For internal purposes only

Document summary

Title	-	Anti - Fraud Policy (2026)
GCI Classification	-	Policy
Document code	-	GCI/FR&S/20-21/26
Approved by	-	Board of Directors of GCI
Effective date	-	01-Apr-2026
Accountable Function	-	Fraud Risk & Surveillance
Key contact	-	Arshad Naseer

Versioning and Ownership

Version	Date of issuance	Document code	Reason for and Extent of Changes
1	August 5, 2011		
2	May 31, 2013		Revised
3	May 30, 2014		Reviewed (no change)
4	May 21, 2015		Reviewed (no change)
5	May 5, 2016		Reviewed (no change)
	August 11, 2017		Reviewed (no change)
	May 12, 2018		Reviewed (no change)
	May 14, 2019		Reviewed (no change)
	June 5, 2020	FGII/FCU/20-21/26	Reviewed (no change)
6	February 9, 2021	FGII/FCU/20-21/26	Revised
7	February 7, 2022	FGII/FCU/20-21/26	Reviewed (no change)
	November 7, 2023	FGII/FCU/20-21/26	Revised
	November 11, 2025	GCI/FR&S/20-21/26	Revised
8	April 1, 2026	GCI/FR&S/20- 21/26	Revised (for alignment with IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025)

Main related internal regulatory references

- GCI Code of Conduct
- Reporting Concern and Anti - Retaliation Guideline
- Whistle Blower Policy

Any substituted/abrogated internal regulation

- N/A

Main related external regulatory references

Regulatory	• IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025 • Master Circular on Corporate Governance for Insurers, 2024

Annexes

- Red Flag Indicators – Annexure I

Note: Circulation or dissemination of abridged, modified, or any different version of this Policy will be de facto unauthorized.

EXECUTIVE SUMMARY

This Anti - Fraud Policy provides the framework for anti-fraud practices across GCI, including its committees, functions and employees. It is meant to lay down their responsibilities in prevention, detection and reporting of fraud or financial irregularities.
In particular, the document regulates:

- Objective of the Policy
- Scope of the Policy
- Fraud Risk Management Framework
- Fraud Identification and investigation
- Reporting to the Authority

The Board and senior leadership shall foster a strong ethical culture with zero tolerance for fraud by promoting integrity, transparency and compliance. Clear expectations on ethical conduct and fraud reporting shall be communicated across the organization. Mandatory training shall be provided to employees and distribution partners to enhance fraud awareness. All relevant persons shall disclose conflicts of interest, and background verification shall be carried out prior to onboarding in line with due diligence requirements.

INDEX

1 Glossary and Definitions

Acronym / Term	Explanation / Definition
Act	The Insurance Act, 1938 (4 of 1938) as amended from time to time
Authority	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).
Board	"Board" means the Board of Directors of Generali Central Insurance Company Limited.
Date of approval	Date on which GCI Anti – Fraud Policy (2026) is approved by the Board of Directors.
Distribution Channels	"Distribution Channels" include insurance agents, intermediaries, corporate agents, insurance intermediaries, or any individuals or entities authorized by the Authority to solicit, procure, sell, or service insurance policies on behalf of the Company.
Effective Date	The date from which this Policy becomes operational and enforceable within the Company.
Fraud / Insurance Fraud	"Insurance Fraud" (hereinafter referred to as 'Fraud') shall mean an act or omission intended to gain advantage through dishonest or unlawful means, for a party committing the fraud or for other related parties; including but not limited to: • Misappropriating funds; Deliberately misrepresenting/concealing/not disclosing one or more material facts relevant to any decision / transaction, financial or otherwise • Abusing responsibility, position of trust or a fiduciary relationship.
Fraud Risk and Surveillance (FR&S)	"Fraud Risk and Surveillance" or "FR&S" refers to the designated independent function of the Company responsible for implementing, managing, and monitoring all activities related to fraud prevention, detection, investigation, and reporting under this Policy.
Cyber or New Age Fraud	"Cyber or New-Age Fraud" refers to any fraud committed using digital, electronic, cyber, or new-age technological means, including but not limited to identity theft, phishing, system manipulation, or unauthorised access.
Third-Party Fraud	"Third-Party Fraud" refers to fraud perpetrated by persons who are not employees or representatives of the Company, including customers, external parties, forged policy issuance agents, or other individuals unaffiliated with the Company.
GCI / Company	Generali Central Insurance Company Limited
Stakeholders	"Stakeholders" include all employees, directors, officers, contractual workers, distribution partners, intermediaries, vendors, service providers, consultants, agents, contractors, customers, and any other persons having a business relationship with the Company.
GCI Accountable Function	Fraud Risk and Surveillance/Department
Red Flag Indicator or RFI	"Red Flag Indicator" or "RFI" means any fact, event, statement of claim, circumstance, transaction pattern, behavior, or documentation irregularity that may indicate or suggest the possibility or potential of fraud, whether taken individually or in conjunction with other indicators.

2 Introduction & Objective

This Anti-Fraud Policy ("Policy") establishes the framework adopted by GCI for the prevention, detection, investigation, reporting, and mitigation of fraud. The Company is committed to conducting its business with integrity, transparency, and accountability and to maintaining an organizational culture that actively deters fraudulent activities. This Policy lays down the principles, governance structure, responsibilities, and procedures necessary to safeguard the interests of the Company, its policyholders, stakeholders, and the insurance ecosystem.

2.1 Objectives

The objectives of this Policy are to:

a. **Deter, Prevent, detect, monitor, mitigate, report and remedy** the occurrence of insurance fraud across all operations of the Company.
b. Establish and implement robust processes, controls, and oversight mechanisms to manage fraud risk effectively.
c. Promote an ethical organizational environment characterized by fairness, integrity, and zero tolerance for fraudulent behavior.
d. Define clear responsibilities for all stakeholders in identifying and reporting suspected or actual fraudulent activities.
e. Provide a consistent framework for the investigation and resolution of fraud incidents.
f. Ensure compliance with applicable laws, regulations, and guidelines issued by the Insurance Regulatory and Development Authority of India (IRDAI), including the Insurance Fraud Monitoring Framework Guidelines, 2025.

2.2 Approval and Review

a. This Policy is approved by the Board of Directors of the Company
b. This Policy shall be reviewed at an annual frequency. Additional review will be undertaken in case of:
- change in applicable laws or regulations,
- emerging fraud risks or industry practices,
- organizational changes or internal process enhancements.

c. Amendment to this Policy shall only be effected upon grant of approval of the Board.

2.3 Effective Date and Implementation Deadline

a. This Policy shall be effective from Board approval date or April 1, 2026, whichever is earlier.
b. The Policy shall be implemented immediately upon coming into effect, and all internal functions shall ensure prompt operationalization of the requirements herein.

2.4 Scope of Application

This Policy is applicable to the following stakeholders:

1. **Internal Stakeholders:**
   All employees, officers, senior leadership, Key Managerial Personnel (KMPs), directors, trainees, temporary staff, and contracted resources of the Company.

2. **External Stakeholders:**
   Shareholders, intermediaries, agents, corporate agents, insurance intermediaries, Third-Party Administrators (TPAs), service providers, vendors, contractors, outsourcing partners, consultants, distribution channels, prospective and existing customers, and any person or entity engaged in business with the Company.

This Policy applies irrespective of location, designation, employment status, business relationship, or contractual arrangement.

All employees are required to annually confirm that they have read, understood, and complied with the provisions of this Policy.

Illustratively, this Policy shall apply to all employees and officers of GCI at whatever level, at every location and whatever the terms of employment, hours of work or length of service, including contractual staff and directors of GCI, 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 GCI.

2.5 Waivers and Dispensations

a. No waiver, dispensation, relaxation, or exception to any provision of this Policy shall be valid unless expressly approved in writing by the Board of Directors.

b. Any request for deviation must be supported by appropriate justification and evaluated for legal, regulatory, and operational implications.

2.6 Implementation, Monitoring, and Information Flows

a. The Company shall ensure that infrastructure, systems, processes, and resources necessary for effective implementation of this Policy are established and maintained.

b. The **Fraud Risk and Surveillance (FR&S) Function** shall be responsible for coordinating the implementation and ongoing monitoring of this Policy across all internal and external functions.

c. All departments shall ensure timely, accurate, and complete flow of fraud-related information to FR&S in accordance with the reporting procedures prescribed herein.

d. The Company shall conduct periodic training and awareness sessions to ensure stakeholders understand their obligations under this Policy.

3 Scope of the Policy

This Policy establishes the framework and requirements for preventing, detecting, deterring, and investigating fraud across all functions, processes, and operations of Generali Central Insurance Company Limited ("GCI" or "the Company"). It outlines the fundamental elements of the Company's fraud risk management approach and applies to all stakeholders as defined under this Policy.

3.1 Fundamental Elements of the Policy:

The Company shall adopt a structured and comprehensive fraud risk management approach built upon the following three fundamental pillars:

a. Ethical Culture and Integrity Framework
Establishing and maintaining a culture of honesty, ethical conduct, and transparency across the organisation. This includes:

- Communicating expectations relating to ethical behaviour and fraud prevention.
- Conducting regular, structured training for employees and distribution partners.
- Reinforcing the "tone at the top" through ethical leadership and accountability.

b. Fraud Risk Identification, Assessment, and Control Measures
Identifying, assessing, and evaluating fraud risks across all business functions and implementing appropriate controls, processes, and systems to mitigate such risks. This includes:

- Periodic Fraud Risk and Control Assessments (FRCA).
- Identification and monitoring of Red Flag Indicators (RFIs).
- Strengthening internal policies, procedures, documentation standards, and system controls.

c. Oversight, Monitoring, and Governance Mechanism
Developing robust oversight and governance structures to ensure effective implementation of fraud risk management. This includes:

- Risk Management Committee (RMC)
- Fraud Monitoring Committee (FMC)
- Fraud Risk and Surveillance (FR&S) Function
- Control functions
- Mechanisms for escalation, reporting, and review of fraud incidents

3.2 Applicability of the Policy:

a. This Policy is effective from the date of its approval by the Board and shall remain in force until superseded or amended.

b. This Policy shall be read in conjunction with:

- The Company's Code of Conduct;
- The Reporting Concern and Anti-Retaliation Guideline;
- The Whistle Blower Policy;
- Applicable internal controls frameworks; and
- All relevant laws, rules, and regulations issued by IRDAI and other competent authorities.

c. In case of conflict between this Policy and any applicable law or regulatory guideline, the latter shall prevail.

d. All employees and relevant stakeholders shall annually confirm compliance with this Policy through a

declaration process administered by the Human Resources Department.

e. All new joiners shall confirm having read and understood this Policy at the time of onboarding.

4 Types of Fraud

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.
The categories described below are illustrative and not exhaustive. New or emerging fraud patterns, including those arising from technological advancements, shall also fall within the ambit of this Policy.

4.1 Internal Fraud:

Internal Fraud refers to fraudulent acts committed by the Company's employees, officers, directors, contractual staff, or any individual acting in a capacity on behalf of the Company. Examples include, but are not limited to:

- Misappropriation or unauthorised diversion of Company funds or assets.
- Fraudulent or manipulated financial reporting.
- Theft of cheques, cash, or negotiable instruments.
- Inflated or falsified expense claims.
- Overbilling or processing false invoices, whether individually or through collusion with vendors.
- Granting unauthorised concessions, benefits, or preferential treatment in exchange for kickbacks or personal favours.
- Forgery, falsification, or alteration of documents, signatures, or records.
- Undervaluing or misappropriating Company assets for personal gain.

4.2 Distribution Channel Fraud:

Fraud perpetuated by an Insurance agent /Intermediaries/Third Party Administrators (TPAs) and service providers against GCI and/or policyholders. Few illustrations of fraud:

- Premium diversion-intermediary takes the premium from the purchaser and does not pass it on to GCI.
- Inflates the premium, passing on the actual amount to GCI and keeping the difference.
- Non-disclosure or misrepresentation of the insurance risk to reduce premiums.
- Commission fraud - Insuring non-existent lives while paying the first premiums to GCI, collecting commission and annulling the insurance by ceasing further premium payments.

4.3 Policyholder Fraud and/or Claims Fraud:

Fraud against GCI in the purchase and/or execution of an insurance product, including fraud at any time during the term of the policy and at the time of making a claim. Few illustrations of fraud:

- Staged or fabricated incidents or losses.
- Submission of false, altered, or exaggerated documents or claims.
- Medical fraud, including fabricated diagnoses, inflated bills, and collusive healthcare provider practices.
- Fraudulent death, disability, or loss claims.
- Misrepresentation or non-disclosure of material information at the time of proposal.

4.4 Third Party Fraud / External Faud:

External Fraud refers to fraudulent acts committed by individuals or entities who are not directly associated with the Company. Examples include:Issuance or circulation of fake, forged, or counterfeit insurance policies or cover notes in the name of the Company.

- Identity theft, impersonation of customers or employees, or unauthorized access to systems.
- Fraudulent claims or attempts to deceive the Company using fabricated evidence.

4.5 Online Fraud, Cyber Fraud and New Age Fraud:

Cyber or online fraud includes any fraudulent act executed using digital, electronic, or cyber-based means or new age technologies. Illustrative examples include:

a. Buyer-Side Online Fraud
Fraudulent claims raised by customers or digital users through online platforms, portals, or mobile applications.

b. Merchant-Side Online Fraud
Fraud committed by merchant partners or digital payment entities, including:

- Non-remittance of collected premiums,

- Manipulation of chargebacks or payment reversals,
- Digital transaction irregularities.

c. Cybersecurity Fraud
Acts intended to compromise Company systems or sensitive data, including:
- Unauthorised access or hacking of Company systems,
- Use of stolen or fake credit cards or bank accounts,
- Malware attacks, phishing, ransomware, or intrusion into Company digital infrastructure.

d. Any Other Digital Fraud
Any other cyber-enabled fraud not covered above

4.6 Affinity Fraud or Complex Fraud:

Fraud involving collusion between two or more internal or external parties. These schemes are typically sophisticated and may involve multiple actors across the insurance value chain. Examples include:

a. Collusion in Motor Insurance Claims
Collusion among policyholders, authorised repairers, surveyors, assessors, lawyers, intermediaries, or internal employees, including:
- Fabricated accident scenarios,
- Inflated repair estimates,
- Falsified survey reports,
- Override or bypass of system-generated alerts.

b. Collusion to Issue Fake Policies and Facilitate Fraudulent Third-Party Claims
- Coordinated issuance of backdated or fabricated policies to assist fraudulent third-party claims or to avoid regulatory penalties.
- Customers, intermediaries, and employees may collaborate to issue fake policies to avoid police action in accidents, implant vehicles/drivers, and encourage fraudulent TP claims. This misuse of system workflows and public funds often involves backdated entries and fabricated documents.

c. Misuse of Banker Receipts
Fraud committed by banking personnel, employees, or intermediaries using banker receipts improperly to compel policy issuance or facilitate illegal transactions.
Indicators may include irregular receipt usage, unexplained policy issuance, or patterns suggesting coercion or collusion.

The above list is only illustrative and not exhaustive. GCI would also ensure deployment of proactive fraud detection measures to protect its e-commerce activities.

4.7 Other Forms of Fraud

Any fraudulent act, scheme, coercion, deception, or manipulation not expressly listed above but which results in wrongful or unlawful gain, or causes loss, damage, or risk to the Company, stakeholders, or policyholders.
The Company shall continue to identify and mitigate emerging fraud risks as part of its ongoing fraud prevention and detection programme.

5 Fraud Risk Management Framework

The Company shall maintain a robust Fraud Risk Management Framework to prevent, detect, investigate, and mitigate fraud. This Framework is built on the principles of ethical leadership, strong internal controls, effective oversight, and timely reporting. It also reinforces the Company's commitment to compliance with the Insurance Fraud Monitoring Framework Guidelines, 2025 issued by IRDAI. The Risk Management Committee (RMC) of the Company is responsible for effective implementation and oversight of the Fraud Risk Management Framework. This Framework has been designed to accommodate several factors including nature of business, size, risk profile, overall business strategy, products, distributions channels and technology infrastructure.

5.1 Fraud Prevention Measures

The Company shall implement preventive measures including:
- Establishment of comprehensive and robust procedures to **deter, prevent, identify, detect, report and remediate frauds** across all categories of fraud and across various insurance operations, including underwriting, claims, investments, procurement, distribution and IT systems.
- Clearly defined **roles, responsibilities and delegation of authority** for the Board of Directors, RMC, FMC, FR&S and all relevant functions, including specific controls and oversight mechanisms for **identified sensitive and vulnerable positions**, to ensure effective implementation of the fraud risk management framework.

- A well-defined and transparent **mechanism for taking appropriate disciplinary, corrective, legal and regulatory actions** in cases of non-compliance with the fraud risk management framework, as well as against individuals or entities involved in fraudulent activities.
- A structured **periodic review process** to identify and analyze **missed or undetected insurance fraud instances**, with the objective of strengthening controls, improving detection systems and enhancing the overall effectiveness of fraud risk management measures.
- establish and implement robust cybersecurity framework to protect against evolving cyber frauds or threats.
- continuously monitor and strengthen systems and processes for fraud risk management, such as incident databases, customer verification, and access control
- utilize a team with relevant risk and technological expertise to manage cyber fraud risks across various insurance business lines.
- Designate "sensitive posts" based on elevated fraud exposure arising from access to funds, systems, data or high risk decisions. For these posts, the Company shall enforce enhanced vetting, role rotation/cooling off, mandatory leave, periodic access reviews, strengthened maker–checker, activity logging, and restricted override privileges.

e. Proactive Prevention Activities

Including but not limited to:

- Data analytics for early detection of fraud patterns.
- Document review and verification mechanisms.
- Customer awareness initiatives on fraud risks and reporting practices.
- Investigating whistleblower complaints as per the Whistleblower Policy.
- Identifying and addressing control weaknesses.
- Maintaining and updating Red Flag Indicators (RFIs) for each functional area as specified in Annexure-I.

5.2 Fraud Detection Processes

a) All employees are responsible for identifying and escalating suspicious activity.
b) Employees shall remain vigilant regarding RFIs and take reasonable steps to prevent fraud.
c) Any suspected fraud must be immediately reported to the employee's supervisor/manager or directly to the Fraud Risk and Surveillance (FR&S) Function.
d) No employee, other than an authorized FR&S member or designated investigator, shall independently investigate a suspected fraud.
e) Fraud detection shall be supported through:
    - Predictive analytics
    - System-generated alerts
    - Trend analysis
    - Interviews and due diligence
    - Review of customer and intermediary patterns
f) FMC shall oversee the Missed Fraud Detection Review Process to identify instances where fraud risks, red flag indicators, or control weaknesses existed, but fraud was not detected in a timely manner.
g) The Missed Fraud Detection Review shall be conducted at least annually and also on an event-driven basis, wherever warranted.
h) Outcomes of such reviews shall be documented, corrective and preventive actions identified, and findings shall be presented to the FMC and escalated to the RMC, as applicable.

5.3 Constitution of the Fraud Monitoring Committee (FMC)

The Company has constituted an internal Fraud Monitoring Committee (FMC), which shall be responsible for operationalizing the Fraud risk management framework within the Company and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.

5.4 Constitution of the Fraud Risk and Surveillance (FR&S) Function

a) The Company has established the Fraud Risk and Surveillance (FR&S) Function to support FMC in discharging its functions and effective implementation of measures suggested by FMC.
b) FR&S shall operate independently under a designated KMP.
c) FR&S shall perform the following functions:

- Receive, consolidate, and track all fraud-related cases across the Company.
- Conduct investigations or coordinate with authorised investigators.
- Submit investigation reports to FMC, highlighting system/process breaches and financial impact.
- Maintain a centralized fraud database with details of reported and investigated fraud incidents.
- The FR&S Function shall maintain and periodically update a centralized Incident Database capturing details of:
    - Persons or entities convicted of insurance fraud; and

- Persons or entities identified as attempting insurance fraud, whether internal or external to the Company.
- The database shall include details of employees, intermediaries, distribution channels, vendors, service providers, healthcare providers, surveyors, and external third parties involved in fraud.

- Track implementation of corrective actions recommended by FMC through Action Taken Reports (ATR).
- Examine claim referral cases from Claims departments.
- Conduct data analysis to identify fraud patterns and potential fraud .
- Organize/conduct FMC meetings and present findings for case-by-case review.
- Ensure appropriate background verification (in coordination with HR and other functions).
- Establish procedures for reporting within the Company and to external authorities when required.
- conduct Missed Opportunity Reviews for (i) frauds detected late, (ii) externally discovered cases (e.g., law enforcement/IIB alerts), (iii) high loss events, and (iv) repeat patterns.

Integrity Obligation for FRS

- FRS shall ensure impartiality and transparency in all fraud investigations.
- Evidence must be handled securely and preserved in its original form until case closure or authorized disposal.
- FRS must not influence outcomes for personal or organizational bias and shall maintain confidentiality of all investigation details.
- Any breach of integrity will be treated as a serious violation and subject to disciplinary action.

5.5 Oversight and Internal Control Mechanisms

a. The Company shall implement internal controls designed to prevent, detect, and mitigate fraud risk.
b. Control weaknesses identified shall be addressed promptly through corrective and preventive actions.
c. The Company shall ensure segregation of duties, system access controls, and transactional oversight in high-risk processes.

6 Reporting of Fraud

The Company is committed to ensuring that all suspected or actual incidents of fraud are reported promptly, investigated thoroughly, and addressed appropriately. Every employee, intermediary, service provider, and stakeholder has a duty to report fraud in accordance with this Policy.

6.1 Mandatory Reporting of Suspected or Actual Fraud

a) Any employee or stakeholder who becomes aware of, or has reason to suspect, a potential or actual fraud must immediately report such incident.
b) Reports may be made to:
   - The employee's immediate supervisor or manager;
   - The Head of the concerned department; or
   - Directly to the Fraud Risk and Surveillance (FR&S) Function
c) Employees may also use the whistleblowing channel prescribed under the Company's **Whistle Blower Policy** to report fraud anonymously or confidentially.

6.2 Reporting Channels

The Company shall maintain the following channels for reporting fraud:

- Direct reporting to reporting managers, or functional heads (unless the incident involves such person/s)
- Email to the FR&S Function at **alert@generalicentral.com**
- Whistleblowing email ID at whistleblowercomplaints@generalicentral.com

6.3 Form and Content of Fraud Reports

a) A report of suspected or actual fraud should, to the extent possible, include:
   - Name and details of the person(s) involved;
   - Description of the incident or suspicious activity including modus operandi and extent of financial loss;
   - Date, time, and location of the occurrence;
   - Documents, communication, or evidence available; and
   - Names of potential witnesses, if any.

b) Absence of detailed information shall not be grounds for withholding a report.
c) Reports must be factual; frivolous, malicious, or knowingly false allegations may result in disciplinary action.

6.4 Prohibition Against Retaliation

a) No adverse action, retaliation, discrimination, or harassment shall be taken against any person who reports a suspected or actual fraud **in good faith**.
b) Retaliation constitutes a violation of Company policy and will result in disciplinary consequences.
c) The Company shall adhere to its **Reporting Concern and Anti – Retaliation Guideline**, ensuring the protection of whistleblowers and complainants.

6.5 Confidentiality of Reports and Investigations

a) All fraud-related reports, complaints, and investigations shall be treated as strictly confidential.
b) Information shall be shared only with individuals who have an authorized need to know, including investigators, FMC members, FR&S, and regulatory authorities as applicable.
c) Unauthorized disclosure of information relating to fraud reports or investigations may result in disciplinary action.

6.6 Escalation Requirements

a) All suspected frauds shall be immediately escalated to the FR&S for evaluation and further action.
b) Material or significant fraud cases, as defined under this Policy or through the regulatory framework, shall be escalated to:
   - Fraud Monitoring Committee (FMC);
   - Chief Executive Officer;
   - Risk Management Committee (RMC); and
   - Board of Directors (if and when required)
c) Cases requiring external reporting shall be escalated to FR&S for regulatory submission as per Section 9 of this Policy.

6.7 Obligation to Preserve Evidence

a) Employees shall not conceal, destroy, or alter evidence or documentation relating to any suspected or actual fraud.
b) Attempting to influence witnesses or investigators is strictly prohibited.

6.8 Rights of the Accused

a) The Company shall ensure that individuals accused of fraud are treated fairly and provided with a fair and equal opportunity to respond to the allegations during the investigation process.
b) The presumption of innocence shall be respected until the investigation is concluded and allegations are proved.

7 Fraud Identification, Mitigation and Monitoring

The Company shall conduct timely, impartial, and comprehensive investigations into all suspected or actual cases of fraud. The investigation process shall be handled by authorised personnel only and shall adhere to applicable legal requirements, regulatory expectations, and internal governance standards.

7.1 Principles Governing Investigations

All investigations under this Policy shall be conducted in accordance with the following principles:
a. **Objectivity:** Investigations shall be conducted impartially and without preconceived conclusions.
b. **Confidentiality:** All information, evidence, and findings shall be kept confidential and disclosed strictly on a need-to-know basis.
c. **Timelines:** Investigations shall be initiated promptly upon receipt of a fraud report and concluded within prescribed / reasonable timelines.
d. **Fairness:** All parties involved shall be treated fairly, and the principles of natural justice shall be observed.
e. **Compliance:** Investigations shall be carried out in accordance with applicable laws, regulatory guidelines, and the Company's internal policies.

7.2 Authority to Investigate

a. **Fraud Risk and Surveillance (FR&S)** is the nodal function responsible for evaluating fraud reports and initiating investigations.
b. FR&S may conduct investigations directly or appoint internal or external investigators based on the nature, complexity, and sensitivity of the case.
c. No employee other than those authorised by FR&S shall conduct or participate in fraud investigations.
d. FR&S shall keep the RMC / Chief Executive Officer and the Fraud Monitoring Committee (FMC) informed of all material fraud investigation cases as and when required.

7.3 Investigation Procedures

All fraud investigations shall follow a structured, documented procedure that generally includes the following steps:

a. Preliminary Assessment

- FR&S shall conduct an initial assessment of the allegation or suspicion.
- The purpose of this assessment is to determine whether a formal investigation is warranted.

b. Formal Investigation Initiation

If the preliminary assessment warrants a full investigation, FR&S shall:

- Formally initiate the investigation;
- Designate investigators;
- Define the scope and objectives; and
- Establish timelines.

c. Evidence Collection

Investigators shall collect relevant documentary, digital, physical, and testimonial evidence, which may include:

- Internal records and system logs;
- Email and communication archives;
- Transaction documents;
- Third-party information;
- Interviews and statements.

d. Witness and Subject Interviews

- Interviews shall be conducted in a professional, respectful, and non-coercive manner.
- The subject of the investigation ("accused") shall be given an opportunity to present their explanation.

e. Forensic Review

- Forensic techniques, data analytics, and expert resources may be used where necessary to validate evidence or identify patterns indicative of fraud.

f. Documentation and Record-Keeping

- All steps taken, evidence reviewed, and conclusions drawn shall be thoroughly documented.
- Investigation files shall be maintained in a secure repository by FR&S.
- Period of retention of identified records shall be as per the regulatory mandate and the Company's policy for record retention.

7.4 Investigation Findings and Reporting

a) Upon completion of the investigation, the report shall comprehensively contain:

- Facts and evidence
- Analysis of findings
- Root cause assessment
- Modus operandi
- Financial impact (if applicable)
- Parties involved
- Breach of internal controls or procedures
- Conclusion on whether fraud is substantiated or unsubstantiated

b) FR&S shall present all investigation reports to the Fraud Monitoring Committee (FMC) for case-by-case review.

c) FR&S shall issue an **Action Taken Report (ATR)** after FMC acceptance of investigation findings, detailing:

- Actions implemented;
- Recovery efforts;
- Disciplinary measures;
- Control enhancements / system improvement; and
- Regulatory reporting status.

7.5 Cooperation with Investigations

a) All employees, intermediaries, vendors, service providers, and stakeholders shall cooperate fully with investigations.

b) Failure to cooperate or attempts to obstruct an investigation may result in disciplinary or contractual action.

7.6 Protection of Evidence

a) All relevant records, documents, systems, and data relating to a suspected or actual fraud must be secured immediately upon initiation of an investigation.

b) Employees shall not alter, conceal, or destroy any evidence.

c) FR&S shall ensure appropriate steps are taken to preserve electronic data, including system logs, emails, and digital files.

7.7 Disciplinary and Remedial Actions

a) If fraud is substantiated, the Company may take appropriate disciplinary action against employees, intermediaries, or third parties involved, including termination of employment or contract.
b) The Company may pursue civil or criminal proceedings to recover losses or prosecute offenders, as appropriate.
c) Control and process deficiencies identified during the investigation shall be rectified promptly.

7.8 External Reporting and Law Enforcement Involvement

a) Where required under law or regulation, FR&S shall initiate reporting to IRDAI.
b) Investigators may seek assistance from external experts, forensic specialists, legal counsel, law enforcement agencies, or regulators.

8 FRAUD MONITORING COMMITTEE (FMC)

The Fraud Monitoring Committee ("FMC") is the apex internal governance body which shall be responsible for operationalizing the Fraud risk management framework within the Company and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.

8.1 Objectives of the FMC

The FMC shall be responsible for:
a. Providing strategic direction and oversight for the operationalizing of this Policy.
b. Reviewing all reported fraud cases, investigation findings, and action taken reports.
c. Assessing fraud trends, emerging risks, and pattern developments.
d. Ensuring that appropriate preventive and corrective measures are implemented.
e. Recommending enhancements to processes, systems, and controls to strengthen fraud resilience.
f. Reporting significant fraud-related matters to the Risk Management Committee (RMC) and the Board, as applicable.

8.2 Composition of the FMC

a. The (being a KMP) shall be the Chairperson of the FMC. Other members shall be the following senior representatives:

- Chairperson: General Counsel, Chief - Regulatory Affairs and Company Secretary
- Claims & Underwriting: Chief Insurance Officer
- Risk Management: Head – Risk Management
- Finance: Chief Financial Officer
- Fraud Risk & Surveillance: Head – FR&S (as permanent invitee)

b. FMC shall avoid conflicts of interest in its composition and functioning.

8.3 Roles and Responsibilities of the FMC

The FMC shall perform the following functions:

a. Oversight and Review

1. Oversee prompt responses to instances or suspicion of fraud.
2. Review investigation reports submitted by FR&S for each fraud case.
3. Evaluate root causes, control weaknesses, and systemic failures contributing to fraud.
4. Review and approve Action Taken Reports (ATR) and monitor progress on remedial actions.
5. Oversee financial and operational impacts of fraud incidents.

b. Monitoring and Analytics

1. Review periodic fraud analytics, dashboards, red flag trends / indicators, and data analyses.
2. Identify areas of heightened fraud risk.
3. Recommend improvements in fraud detection systems, data analytics tools, and technology.

c. Policy and Framework Review

1. Review the effectiveness of the Fraud Monitoring Framework
2. Recommend changes to the Anti-Fraud Policy, FRCA methodology, RFIs, and internal guidelines.
3. Ensure alignment with IRDAI guidelines and industry best practices.

d. Reporting and Escalation

1. Report significant fraud matters and material cases to the RMC and Board.
2. Ensure timely reporting to the Authority (IRDAI) through FR&S.
3. Oversee regulatory compliance relating to fraud risk management.

e. Capacity Building

1. Promote fraud awareness and training across functions.
2. Recommend specialised training for high-risk functional teams.

f. recommends and regularly updates, based on experiences, appropriate measures on fraud risk management to various functions.
g. oversees prompt responses to instances or suspicions of fraud
h. maintains database of all relevant details pertaining to each instance of fraud
i. facilitates collaboration with industry peers / bodies, law enforcement agencies and regulatory bodies to pursue cases of fraud and share information / intelligence on known fraud schemes and perpetrators.
j. conducts an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines and activities for fraud, using past experiences, emerging trends & Red Flag Indicators (RFIs), etc.
k. identifies areas for improvement and adaptation of the Fraud Risk Management Framework

8.4 Meetings of the FMC

a. FMC shall meet **at least once every quarter**.
b. Additional meetings may be convened based on urgency, complexity, or sensitivity of fraud cases.
c. The quorum for FMC meetings shall consist of the Chairperson and at least half of the Committee members.
d. Attendance may be physical or virtual, subject to proper documentation and participant verification.
e. FR&S shall circulate the agenda and supporting documents in advance of each meeting.

8.5 Minutes and Documentation

a) Minutes of each FMC meeting shall be recorded and maintained by FR&S.
b) The minutes shall document:

- Cases reviewed
- Findings
- Decisions taken
- Action items assigned
- Timeline commitments

c) FMC Minutes shall be shared with the RMC and presented to the Board, where required.

8.6 Follow-Up and Action Tracking

a) FR&S shall track the implementation of FMC decisions through Action Taken Reports (ATR).
b) All functions shall ensure timely implementation of corrective and preventive actions assigned to them.
c) Delays or non-compliance shall be escalated to FMC and, if applicable, to the RMC.

8.7 Independence and Authority

a) FMC has the authority to access all information, documents, systems, and resources necessary for fulfilling its mandate.
b) FMC may invite external experts, auditors, investigators, or consultants to provide support or independent insights.
c) FMC functions independently and without influence from business functions or individuals.

8.8 Reporting Requirements

The FMC shall:

a. Submit quarterly reports to the RMC on its activities, findings, and recommendations, including the financial impact of fraud on the Company.
b. Submit report of the annual comprehensive fraud risk assessment before the board of directors through RMC.
c. Report to the Audit Committee, in addition to the RMC, in case of all internal frauds.

8.9 Participation in Insurance Information Bureau (IIB) Framework

The Company shall participate in the Fraud Monitoring Technology Framework made available by the Insurance Information Bureau of India (IIB), relating to general and health insurance business, to support industry-wide fraud prevention and detection.

8.10 Information Sharing with Insurance Information Bureau (IIB)

The Company shall share with the IIB, the following information:

(i) Details of blacklisted distribution channels;
(ii) Details of hospitals and third party vendors blacklisted for fraud or misconduct; and
(iii) Details of confirmed fraud perpetrators, as permitted under applicable laws.

9. REPORTING TO THE AUTHORITY

The Company shall comply with all regulatory reporting requirements relating to fraud as prescribed under the Insurance Fraud Monitoring Framework Guidelines, 2025 and any amendments issued thereafter. All reports to the Insurance Regulatory and Development Authority of India ("the Authority") shall be accurate, complete, and submitted within prescribed timelines.

9.1 Responsibility for Regulatory Reporting

a. The **Fraud Monitoring Committee (FMC)** shall be the designated function responsible for all fraud-related regulatory submissions. The execution arm shall be the FR&S function. Filing of all reports shall be preceded by an express approval of the FMC.

b. FMC shall ensure that:

- All reportable frauds are identified promptly;
- Required information is compiled from relevant functions;

- Reports are reviewed for accuracy and completeness; and
- Submissions to the Authority are made in a timely manner.

c. Once identified and approved by the FMC, FR&S shall conduct reporting in the following manner:
- Incidents of fraud will be reported to law enforcement agencies and, as per applicable laws, to relevant agencies;
- Incidents of fraud will be reported to IRDAI as per the method and timeline prescribed in the Guidelines;
- Events of fraud committed by distribution channels will be reported to IRDAI through prompt escalation.

9.2 Authentication and Record Maintenance

a. All submissions to the Authority shall be authenticated by authorised officials in accordance with regulatory requirements.

b. FR&S shall maintain centralized records of:
- All frauds reported to the Authority
- Supporting evidence
- Communications exchanged
- Acknowledgements received

c. Records shall be retained for the period stipulated under applicable laws or internal policies, whichever is longer.

9.3 Communication with Law Enforcement and Other External Agencies
Reporting to external agencies and authorities shall be conducted by FR&S, in consultation with the Legal and Compliance functions.

10. Confidentiality and Non-Retaliation
The Company is committed to maintaining the confidentiality and security of all information accessed, processed, or generated during the prevention, detection, reporting, and investigation of fraud. All employees, intermediaries, vendors, consultants, and stakeholders are required to adhere strictly to the confidentiality obligations set out in this Policy and all other applicable Company policies.

10.1 Confidentiality of Fraud-Related Information
a. All information relating to suspected, alleged, or confirmed fraud—including reports, documents, evidence, investigation findings, and internal communications—shall be treated as **confidential and sensitive**.
b. Such information shall be disclosed strictly on a **need-to-know basis** and only to persons authorised to access or handle fraud-related information, including FMC members, FR&S, Legal, Compliance, or external authorities, where required.
c. Any unauthorised disclosure, dissemination, or misuse of fraud-related information is strictly prohibited and may result in disciplinary, contractual, or legal action.

10.2 Protection of Personal Data and Sensitive Information

a. All personal data and sensitive personal information obtained during fraud detection, investigation, or reporting activities shall be processed in accordance with:
- Applicable data protection laws,
- Regulatory requirements, and
- The Company's Privacy Policy.

b. Access to personal data shall be limited to authorised individuals and used solely for the legitimate purpose of fraud management.

c. The Company shall implement appropriate technical and organisational controls to safeguard data against:
- unauthorised access,
- alteration,
- disclosure,
- destruction, or
- cyber incidents.

10.3 Secure Handling and Storage of Records
a. All fraud-related records—including physical files, digital documents, emails, audio/video recordings, and investigation notes—shall be stored securely using approved Company systems and repositories.
b. FR&S shall maintain a centralised repository of fraud cases with restricted access controls.
c. Data retention periods shall be aligned with applicable laws, regulatory expectations, and internal record-retention

policies.
d. No employee shall store fraud-related information on personal devices, unapproved platforms, or external storage media.

10.4 Confidentiality Obligations During and After Employment

a. Employees and other stakeholders who participate in investigations or have access to fraud-related information are bound by confidentiality obligations during the course of their engagement with the Company and **even after cessation of employment or contract**.
b. Breach of confidentiality obligations may result in:

- disciplinary action,
- termination of employment or engagement,
- contractual remedies, and
- legal proceedings, as applicable.

10.5 External Disclosure and Communication Controls

a. No employee or stakeholder shall communicate or disclose fraud-related information to any external party—including media, customers, lawyers, third parties, or any unauthorised person unless expressly approved.
b. External disclosures shall be made **only** through FR&S in consultation with Legal and Compliance functions and, where necessary, FMC.
c. Any request for information from law enforcement, regulatory bodies, or statutory authorities shall be handled strictly through authorised channels.

10.6 Protection of Whistleblowers and Informants

a. The identity of employees, whistleblowers, informants, witnesses, or complaint filers shall be kept strictly confidential in accordance with the Company's Whistle Blower and Anti-Retaliation Policies.
b. No adverse or retaliatory action shall be taken against any individual who, in good faith, reports a suspected or actual fraud.

10.7 Use of Information for Legitimate Business Purpose Only

a. Information obtained during any fraud investigation shall be used exclusively for the legitimate business purpose of fraud detection, prevention, investigation, regulatory reporting, or disciplinary action.
b. Using fraud-related information for personal gain, manipulation, or unauthorised purposes shall constitute misconduct and may lead to disciplinary and legal consequences.

11. ROLES AND RESPONSIBILITIES

Effective fraud risk management requires coordinated efforts across all levels of the organisation. The roles and responsibilities set out below establish accountability for fraud prevention, detection, reporting, investigation, and monitoring across the Company.

11.1 Board of Directors

a. Approve the Anti-Fraud Policy and ensure that an effective Fraud Risk Management Framework is established.
b. Provide oversight to ensure that fraud risks are identified, assessed, monitored, and managed effectively.
c. Review significant fraud cases and corrective actions through updates from the RMC and FMC.
d. Ensure adequate resources, systems, and controls are in place to support fraud risk management.

11.2 Risk Management Committee (RMC)

The RMC shall:
a. Assist the Board in implementing and overseeing the Company's Fraud Risk Management Framework.
b. Review periodic fraud reports, emerging fraud risks, and control deficiencies.
c. Inform significant or systemic fraud matters to the Board.
d. Provide IIB with the details of distribution channels, hospitals, third party vendors and fraud perpetrators blacklisted.

11.3 Fraud Monitoring Committee (FMC)

Obligations of FR&S Function are specified in clause 8.3 above.

11.5 Fraud Risk and Surveillance (FR&S) Function

Obligations of FR&S Function are specified in clause 5.4 above.

11.6 Training Function

a) Design and deliver mandatory fraud awareness and ethics training at the induction programme for new joiners and periodically thereafter.
b) Update training content based on the revisions to this Policy.
c) Maintain training records and report completion status to FR&S.

d) Shall conduct awareness programmes for educating policyholders and general public about risk of fraud and mitigation measures.

e) Shall conduct periodic training programmes for employees, higher officials, and for distribution channels associated with the Company.

Generali Central India Insurance Company Limited

Anti - Fraud Policy

GCI Fraud Risk and Surveillance

GCI POLICY

For internal purposes only

Document summary

Title	Anti - Fraud Policy
GCI Classification	Policy
Document code	GCI/FR&S/20-21/26
Approved by	Board of Directors of GCI
Effective date	2025-11-11
Accountable Function	Fraud Risk & Surveillance
Key contact	Arshad.Naseer2@generalicentral.com

Versioning and Ownership

Version	Date of issuance	Document code	Reason for and Extent of Changes	Owner
7.0	2025-11-11	GCI/FR&S/20-21/26	Revision and Updation	FR&S

Main related internal regulatory references

- GCI Code of Conduct
- Reporting Concern and Anti – Retaliation Guideline
- Whistle Blower Policy

Any substituted/abrogated internal regulations

- -n/a

Main related external regulatory references

Regulatory [X] Yes [ ] No

- IRDAI Insurance fraud Monitoring Framework (Ref. IRDA/SDD/MISC/CIR/009/01/2013), dated January 21, 2013
- IRDAI Guidelines for Corporate Governance for insurers in India (Ref. IRDA/F&A/GDL/CG/100/05/2016), dated May 18, 2016

Relevant for the purposes of Legislative Decree 231/2001 [ ] Yes [X] No

Annexes

- -n/a

EXECUTIVE SUMMARY

Anti - Fraud Policy provides guidelines to employees to understand their responsibilities in prevention, detection and reporting of fraud or financial irregularities.

In particular, the document regulates:

- Objective of the Policy
- Scope of the Policy
- Fraud Risk Governance Framework
- Fraud Identification and investigation
- Reporting to the Authority

INDEX

1 Glossary and Definitions

Acronym/Term	Explanation/Definition
GCI	Generali Central India Insurance Company Limited
Fraud Risk and Surveillance (FR&S)	The function that, is accountable to manage the Anti - Fraud Policy relevant activities at GCI.
Date of approval	Date on which GCI Anti – Fraud Policy is approved by the Board of Directors.
Effective Date	Date of the Implementation of Anti – Fraud Policy.
GCI Accountable Function	Fraud Risk and Surveillance/Department
Fraud	Fraud is a term which generally refers to any act committed intentionally to secure an unfair or unlawful gain.
Insurance Fraud	Insurance Fraud is an act or omission related to the conclusion of an insurance contract or to a claim; meant to gain unjustified enrichment for the fraudster or another party or meant to cause a loss to another party.
Act	The Insurance Act, 1938 (4 of 1938) as amended from time to time
Authority	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).

2 Introduction

2.1 Objectives

The Policy is established to detect, monitor and mitigate occurrence of insurance fraud in GCI. It would facilitate development of processes to prevent, detect and manage frauds. It will also ensure development of control measures at an organizational level. GCI is committed to conducting business in an environment of fairness and integrity and will strive to eliminate fraud from all operations.

2.2 Approval and Review

The GCI Policy was approved by Board of Directors of GCI, upon proposal of the GCI CEO.

It shall be promptly reviewed, and in any case atleast on an annual basis, to include developments in legislation, market and/or best practices, Group strategy and organization.

2.3 Effective Date and Implementation Deadline

The GCI Policy is effective as of 08 November 2023 and shall be immediately implemented.

2.4 Scope of Application

The Policy applies to:

- Internal Stakeholders
- External Stakeholders
- Intermediaries

Illustratively, this Policy shall apply to all employees and officers of GCI at whatever level, at every location and whatever the terms of employment, hours of work or length of service, including contractual staff and directors of GCI, 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 GCI.

3 Scope of the Policy

3.1 Fundamental Elements of the Policy:

This document identifies the measures that GCI 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 the various types of fraud; and

(3) Develop an appropriate oversight process.

3.2 Applicability of the Policy

The Policy shall be effective from the date of its approval by the Board. The Policy is to be read in conjunction with the Code of Conduct and Anti – retaliation and Reporting Concern Guideline and is intended to supplement / compliment all applicable laws, rules and regulations and other corporate policies.
All employees shall confirm to having read and understood this Policy and not violated any of its provision, on an annual basis, in the form as may be advised by the HR Department. All new joiners shall adhere to this requirement also at the time of joining to the HR department.

4 Types of Fraud

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 mostly falls into one of the following categories. However, this list is only illustrative and not exhaustive.

4.1.1 Internal Fraud:

Fraud/mis - appropriation against GCI by its Director, employee and/or anyone else associated with GCI (by whatever name called). Few illustrations of Internal fraud:

- Misappropriating funds.
- Fraudulent financial reporting.
- Stealing cheques.
- Inflating expenses claims/over billing.
- Paying false (or inflated) invoices, either self-prepared or obtained through collusion with vendors.
- Permitting special prices or privileges to customers or granting business to favoured vendors, for kickbacks/ personal favours.
- Forging signatures.
- Falsifying documents.
- Selling Company assets at below their true value in return for personal benefit.

4.1.2 Policyholder Fraud and Claims Fraud:

Fraud against GCI in the purchase and/or execution of an insurance product, including fraud at any time during the term of the policy and at the time of making a claim. Few illustrations of fraud:

- Staging the occurrence of incidents.
- Reporting and claiming of fictitious damage/loss.
- Medical claims fraud.
- Fraudulent Death Claims.

4.1.3 Intermediary fraud:

Fraud perpetuated by an Insurance agent /Intermediaries/Third Party Administrators (TPAs) and service providers against GCI and/or policyholders. Few illustrations of fraud:-

- Premium diversion-intermediary takes the premium from the purchaser and does not pass it to GCI.
- Inflates the premium, passing on the actual amount to GCI and keeping the difference.
- Non-disclosure or misrepresentation of the insurance risk to reduce premiums.
- Commission fraud - Insuring non-existent lives while paying the first premiums to GCI, collecting commission and annulling the insurance by ceasing further premium payments.

4.1.4 Third Party Fraud:

Fraud committed by third parties against GCI and the general public which primarily includes activities such as the issue of fake/forged policies and cover notes in the name of GCI.

4.1.5 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 such as–

- *Buyer side frauds:* Where buyers file fraudulent claims using online medium.
- *Merchant side frauds:* Frauds committed by any of the merchant partners of GCI which would include non-remittance of premium collected on behalf of GCI 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 GCI. Threat of confidential data of GCI being comprised due to any cyberattack/hacking of GCI systems.
- *Other Frauds* – Any other type of online fraud which does not fall under either of the above three sub-categories.

The above list is only illustrative and not exhaustive. GCI would also ensure deployment of proactive fraud detection measures to protect its e-commerce activities.

5 Fraud Risk Governance Framework – Creating a Culture of Honesty and High Ethics

The Board of Directors and Senior Management at GCI set the “tone at the top” for ethical behaviour by behaving ethically and openly communicating expectations for ethical behaviour to the Employees. The Anti - Fraud Policy is clearly communicated to all employees of the company in an understandable fashion. 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 employees.

Directors, employees and contractors shall internally self - disclose potential or actual conflicts of interest to appropriate functional head in the organisation as part of the company’s due diligence for fraud detection and mitigation, background checks on new employees and personnel (management and staff) / insurance agent / corporate agent / intermediary shall be carried out in order to prevent fraud at the source. Background checks shall be duly formalized and documented in writing.

GCI seeks to establish and maintain a robust framework to provide reasonable assurance that dishonest acts are prevented or promptly detected and actioned upon, which have been reinforced through this Policy, which outlines the procedures in relation to the following:

i. **Oversight** – GCI has built adequate procedures and policies to oversee that the Fraud Risk Governance Framework is established, implemented and adequate internal controls exist to prevent, identify, detect, investigate, deter fraud and report frauds.

ii. **Prevention** – GCI will strive towards prevention of fraud at the first place. GCI has well defined procedures to carry out due diligence on the Employee, Agents, Intermediaries, Third Party administrators, etc. In addition, GCI shall have in place following measures:

a. **Due Diligence**: Implement robust underwriting and approval processes to evaluate risks and identify potential fraudulent activities before issuing policies or claims.

b. **Risk Assessment:** Regularly assess and update fraud risks specific to the insurance industry through internal audits and external experts.

c. **Training and Awareness**: Conduct regular training awareness programs to educate employees and stakeholders about fraud prevention, detection, reporting, and ethical conduct.

d. Fraud Monitoring: Implement effective systems and technology to monitor and detect potential fraud patterns or suspicious activities.

GCI shall further conduct the following preventive activities:-

- Fraud detection through data analytics and documents review;
- Awareness on Fraud among existing and prospective customers, its implication and importance of complying with GCI's policies & procedures and identifying/ reporting of suspicious activity;
- Investigate the whistle blower complaint, if any, received from time to time, under supervision of CCO;
- Establish a strong Fraud Risk and Control Assessment;
- Identify red flag indicators and carry out timely investigation thereon;
- Additional red flag indicators identified during the course of the business basis industry experience; and
- Identifying the control weakness and adopting the learnings for process enhancement

iii. **Detection** – All employees of GCI have a responsibility to detect potential fraud and should be familiar with the types of fraud that might occur within his/her area of responsibility and be alert for any indication of irregularities. Every employee shall immediately report any suspected fraud or dishonest act or omission to his/ her Supervisor/ Manager.

6 Constitution of Fraud Risk and Surveillance

GCI shall constitute a separate department i.e., Fraud Risk and Surveillance ('FR&S', 'GCI Accountable Function') for implementing the Fraud Monitoring Framework. FR&S must be separated from other functions of the Company and must operate independently under a person from senior management. It will be responsible for laying down appropriate fraud management processes and procedures across the Company. It shall report the status of significant cases of fraud detected in the Company to the Board of Directors through Risk Management Committee (RMC) on Quarterly basis.

Functions of FR&S shall include but not be limited to the following:

- FR&S shall collate all cases of frauds reported to it or by any other entities.
- FR&S shall investigate all such cases and render report to the CRO duly highlighting the breaches of conduct, process and system etc. Report shall also highlight the financial implication, if any.
- FR&S shall be responsible for implementing the decisions by RMC
- FR&S shall track the closure of the decisions through Action Taken Report (ATR).
- FR&S shall get the cases having involvement of non-related entities reviewed and closed through Head – FR&S and submit details of such cases to the RMC.
- FR&S shall investigate claim cases referred from respective claim departments.
- FR&S shall analyse the data based on claim / fraud investigation to know the pattern and potential areas of fraud.
- FR&S shall ensure reporting of cases to FCC and convene meeting of FCC for reviewing the findings of the investigation on case of case basis.
- Due Diligence/Background Verification: The HR Department shall conduct due diligence/background verification of employees at the time of on-boarding as per the HR policy. The due diligence of intermediaries, channel partners, vendors, Hospitals, Garages etc. shall be carried out by the respective departments.
- Reporting: FR&S shall lay down the procedure for internal / external reporting from / and to various departments.

7 Reporting of Fraud

All persons including employees, vendors, TPAs, agents, intermediaries are expected to take all reasonable steps to prevent the occurrence of Frauds including online Frauds and to identify and report instances of known or suspicious Fraud committed against the Company, whether by the employees or by outside parties.
All employees should timely, expeditiously, unhesitatingly and fearlessly report any Fraud including Cyber / Online Fraud against the Company to FR&S at alert@generalicentral.com.
No employee shall investigate / interview / interrogate such cases of actual / suspected frauds himself except the responsible person within FR&S or authorized team/ person identified to investigate the same by FR&S/CCO.

The identity of the complainant will be maintained confidential and it shall not be disclosed. Detection techniques have been established to uncover fraud events when preventive measures fail or unmitigated risks are realized. GCI detects fraud through means including but not limited to data analysis, investigation, verifying trends, interviewing the alleged etc.

8 Fraud identification and Investigation

8.1 External Fraud

a. FR&S 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.

b. Employees are required to be alert and vigilant with respect to external frauds. If any external fraud comes to the attention of any employee, 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.

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

8.2 Internal Fraud

Reporting Procedures - Communicating Concerns about Alleged or Suspected Fraud

a. 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.

b. 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:

   a. The Chief Executive Officer;
   b. Chief Operating Officer
   c. Chief Compliance Officer;
   d. Chief People Officer;
   e. Chief Risk Officer and
   f. Head of Fraud Risk and Surveillance;

c. 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.

d. The manager or supervisor shall promptly escalate the concern to the Chief Compliance Officer, the Chief People Officer, the Chief Executive Officer; the Head of Fraud Risk and Surveillance or the Chief Risk officer as the case may be.

e. 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.

f. 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.

g. 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.

h. 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.

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

8.2.1 Fraud Investigation, Fact Finding & Corrective Action

i. Preliminary Analysis:

- The alleged internal fraud case is reviewed jointly by Chief People officer and the Head of Fraud Risk and Surveillance 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.

Chief People Officer and the Head of Fraud Risk and Surveillance shall be excluded from the preliminary analysis or the subsequent investigations if the alleged or suspected internal fraud case involves him/her.

The Fraud Risk and Surveillance has the primary responsibility for the investigation of all suspected or alleged internal fraudulent acts as defined in this Policy.

ii. Investigations:

Great care must be taken by the FR&S 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 members of the FR&S 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 FR&S 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 in line with the Company's Record and Retention Policy or as required by applicable laws.
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.

The investigations shall be completed normally within forty-five (45) working days from the disclosure or discovery of the fraud case, however based on the facts and circumstances of each case, the period may be extended beyond 45 working days.

The recovery amounts, the controls implications and the resolution. Management is responsible for resolving fraud incidents 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.

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

iii. 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 based on the principle of proportionality (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.

FR&S shall monitor the implementation of the resolution to ensure that proper corrective action was taken and report to the Risk Management Committee accordingly.

9 Fraud Control Committee (FCC)

FCC shall be constituted to review the findings of the investigations done by FR&S and to take appropriate actions thereupon. The Composition of FCC should be as below:

- Chief Compliance Officer
- Chief Financial Officer
- Chief Risk Officer
- Chief Operating Officer
- Chief People Officer

Frequency of Meeting

The Committee shall meet at least once a quarterly basis with a provision for seeking decision through circulation to decide on urgent cases. Such decisions shall be noted at the immediate next meeting of the Committee. The Committee shall be responsible inter-alia for effective implementation and to monitor and decide fraud cases.

Quorum

The quorum for the meetings of the Committee shall be at least three members. In case of Complaints against any members of FCC, the concerned member shall not attend the meetings of FCC wherein the subject matter is being discussed. Further, in case such matter requires investigation by FR&S, the concerned member shall restrain from initiating any instruction to FR&S.
In case, if any woman is summoned to the meeting, presence of a woman representative from the Company is mandatory.
In case of Complaints against the Managing Director and Chief Executive Officer and other Whole-Time Directors, the same shall be reported to the Nomination and Remuneration Committee of Directors.
Head of the Department of the accused shall be invited at the meetings of the Committee without having any right to vote. Head of Fraud Risk and Surveillance shall be the permanent invitee at the meetings of the Committee and inter-alia record the proceedings of the meeting and keep safe custody of said minutes ensuring its confidentiality.

10 Reports to the Authority

Based on the data received in the prescribed format from the FR&S, Compliance Function shall file a report on statistics on various fraudulent cases which come to light and action taken thereon to the Insurance Regulatory and Development Authority of India (“IRDAI”) in forms FMR 1 and FMR 2 (as prescribed by IRDAI 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, as amended theron, 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 Committee appointed 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.

11 Confidentiality and Non – Retaliation

Under the Policy, every reasonable effort shall be made to ensure the confidentiality of the person who has reported the Fraud. The identity of those providing information shall be kept confidential in order to carry out an appropriate, fair and thorough investigation. If a fraud is reported anonymously, the person must provide credible and sufficient information to enable the FR&S to investigate. GCI shall adhere to the Anti Retaliation and reporting Concern Policy and ensure that no retaliatory action is taken against any individual for reporting, in good faith, known or suspected Fraud.

12 Roles and Responsibilities

Please include all roles and responsibilities entrusted to each stakeholder (corporate bodies/functions/structures/units) mentioned in the document.

Role	Responsibility
Chief Executive Officer (CEO)	• Receives and Monitors Escalations of Fraud Complaints • ensure that Employees are protected against any form of Retaliation; • receive and approve recommendations received post investigation
Fraud Risk and Surveillance (FR&S)	• Conducts preliminary investigation • Ensures timely submission of investigation report • Submits recommendations to the CEO • Ensures timely submission of data for reporting purpose • Shall convene periodical meeting of FCC for reviewing the findings of investigation on case of case basis
Chief People Officer	• ensures that investigation is conducted in the right direction. • ensures that the channels for reporting suspected fraud are available to all Employees and third parties;
Chief Compliance Officer	• receives escalations of Fraud complaints. • monitors that any form of Retaliation occurs as a result of a Fraudulent activity being highlighted by an Employee.
Employee	• performs his/ her duties with professional due diligence, care and good faith in compliance with the provisions of Anti - Fraud Policy; • supports with care the internal and external investigations providing true and accurate information when requested by the Compliance Officer(s), by any person appointed to conduct the investigation or by any competent authority(ies); • reports a complaint when he/she becomes aware of any fraudulent activity.
Human Resource (HR)	• Collect Annual declaration on Anti-Fraud policy from existing employees and new employees. • Provide regular and periodic training to all employees upon joining the organization and throughout their association with the Company, in order to clearly communicate expectations for ethical behaviour to employees. • Conduct due diligence of employees at the time of onboarding.
Fraud Control Committee	• Shall review the findings by FR&S team on quarterly basis. • shall recommend to the Chief Executive Officer of the Company to take such disciplinary or corrective actions based on the principle of proportionality

Future Generali India Insurance Company Limited

Anti - Fraud Policy

FGII Fraud Control Unit

FGII POLICY

For internal purposes only

Document summary

Title	Anti - Fraud Policy
FGIRS Classification	Policy
Document code	FGII/FCU/20-21/26
Approved by	Board of Directors of FGII
Effective date	2023-11-07
Accountable Function	Fraud Control Unit
Key contact	Virendra.Batra@futuregenerali.in

Versioning and Ownership

Version	Date of issuance	Document code	Reason for and Extent of Changes	Owner
7.0	2023-11-07	FGII/FCU/20-21/26	Revision and Updation	FCU

Main related internal regulatory references

- FGII Code of Conduct
- Reporting Concern and Anti – Retaliation Guideline
- Whistle Blower Policy

Any substituted/abrogated internal regulations

- -n/a

Main related external regulatory references

Regulatory	X	Yes		No	• IRDAI Insurance fraud Monitoring Framework (Ref. IRDA/SDD/MISC/CIR/009/01/2013), dated January 21, 2013 • IRDAI Guidelines for Corporate Governance for insurers in India (Ref. IRDA/F&A/GDL/CG/100/05/2016), dated May 18, 2016

Relevant for the purposes of Legislative Decree 231/2001 ☐ Yes ☒ No

Annexes

- -n/a

EXECUTIVE SUMMARY

Anti - Fraud Policy provides guidelines to employees to understand their responsibilities in prevention, detection and reporting of fraud or financial irregularities.

In particular, the document regulates:

- Objective of the Policy
- Scope of the Policy
- Fraud Risk Governance Framework
- Fraud Identification and investigation
- Reporting to the Authority

FUTURE GENERALI
TOTAL INSURANCE SOLUTIONS

INDEX

1 Glossary and Definitions

Acronym/Term	Explanation/Definition
FGII	Future Generali India Insurance Company Limited
Fraud Control Unit (FCU)	The function that, is accountable to manage the Anti - Fraud Policy relevant activities at FGII.
Date of approval	Date on which FGII Anti – Fraud Policy is approved by the Board of Directors.
Effective Date	Date of the Implementation of Anti – Fraud Policy.
FGII Accountable Function	Fraud Control Unit/Department
Fraud	Fraud is a term which generally refers to any act committed intentionally to secure an unfair or unlawful gain.
Insurance Fraud	Insurance Fraud is an act or omission related to the conclusion of an insurance contract or to a claim; meant to gain unjustified enrichment for the fraudster or another party or meant to cause a loss to another party.
Act	The Insurance Act, 1938 (4 of 1938) as amended from time to time
Authority	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).

2 Introduction

2.1 Objectives

The Policy is established to detect, monitor and mitigate occurrence of insurance fraud in FGII. It would facilitate development of processes to prevent, detect and manage frauds. It will also ensure development of control measures at an organizational level. FGII is committed to conducting business in an environment of fairness and integrity and will strive to eliminate fraud from all operations.

2.2 Approval and Review

The FGII Policy was approved by Board of Directors of FGII, upon proposal of the FGII CEO.

It shall be promptly reviewed, and in any case atleast on an annual basis, to include developments in legislation, market and/or best practices, Group strategy and organization.

2.3 Effective Date and Implementation Deadline

The FGII Policy is effective as of 08 November 2023 and shall be immediately implemented.

2.4 Scope of Application

The Policy applies to:

- Internal Stakeholders
- External Stakeholders
- Intermediaries

Illustratively, this Policy shall apply to all employees and officers of FGII at whatever level, at every location and whatever the terms of employment, hours of work or length of service, including contractual staff and directors of FGII, 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 FGII.

3 Scope of the Policy

3.1 Fundamental Elements of the Policy:

This document identifies the measures that FGII 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 the various types of fraud; and

(3) Develop an appropriate oversight process.

3.2 Applicability of the Policy

The Policy shall be effective from the date of its approval by the Board. The Policy is to be read in conjunction with the Code of Conduct and Anti – retaliation and Reporting Concern Guideline and is intended to supplement / compliment all applicable laws, rules and regulations and other corporate policies.
All employees shall confirm to having read and understood this Policy and not violated any of its provision, on an annual basis, in the form as may be advised by the HR Department. All new joiners shall adhere to this requirement also at the time of joining to the HR department.

4 Types of Fraud

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 mostly falls into one of the following categories. However, this list is only illustrative and not exhaustive.

4.1.1 Internal Fraud:

Fraud/mis - appropriation against FGII by its Director, employee and/or anyone else associated with FGII (by whatever name called). Few illustrations of Internal fraud:

- Misappropriating funds.
- Fraudulent financial reporting.
- Stealing cheques.
- Inflating expenses claims/over billing.
- Paying false (or inflated) invoices, either self-prepared or obtained through collusion with vendors.
- Permitting special prices or privileges to customers or granting business to favoured vendors, for kickbacks/ personal favours.
- Forging signatures.
- Falsifying documents.
- Selling Company assets at below their true value in return for personal benefit.

4.1.2 Policyholder Fraud and Claims Fraud:

Fraud against FGII in the purchase and/or execution of an insurance product, including fraud at any time during the term of the policy and at the time of making a claim. Few illustrations of fraud:

- Staging the occurrence of incidents.
- Reporting and claiming of fictitious damage/loss.
- Medical claims fraud.
- Fraudulent Death Claims.

4.1.3 Intermediary fraud:

Fraud perpetuated by an Insurance agent /Intermediaries/Third Party Administrators (TPAs) and service providers against FGII and/or policyholders. Few illustrations of fraud:-

- Premium diversion-intermediary takes the premium from the purchaser and does not pass it to FGII.
- Inflates the premium, passing on the actual amount to FGII and keeping the difference.
- Non-disclosure or misrepresentation of the insurance risk to reduce premiums.
- Commission fraud - Insuring non-existent lives while paying the first premiums to FGII, collecting commission and annulling the insurance by ceasing further premium payments.

4.1.4 Third Party Fraud:

Fraud committed by third parties against FGII and the general public which primarily includes activities such as the issue of fake/forged policies and cover notes in the name of FGII.

4.1.5 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 such as–

- *Buyer side frauds:* Where buyers file fraudulent claims using online medium.
- *Merchant side frauds:* Frauds committed by any of the merchant partners of FGII which would include non-remittance of premium collected on behalf of FGII 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 FGII. Threat of confidential data of FGII being comprised due to any cyberattack/hacking of FGII systems.
- *Other Frauds* – Any other type of online fraud which does not fall under either of the above three sub-categories.

The above list is only illustrative and not exhaustive. FGII would also ensure deployment of proactive fraud detection measures to protect its e-commerce activities.

5 Fraud Risk Governance Framework – Creating a Culture of Honesty and High Ethics

The Board of Directors and Senior Management at FGII set the “tone at the top” for ethical behaviour by behaving ethically and openly communicating expectations for ethical behaviour to the Employees. The Anti - Fraud Policy is clearly communicated to all employees of the company in an understandable fashion. 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 employees.

Directors, employees and contractors shall internally self - disclose potential or actual conflicts of interest to appropriate functional head in the organisation as part of the company’s due diligence for fraud detection and mitigation, background checks on new employees and personnel (management and staff) / insurance agent / corporate agent / intermediary shall be carried out in order to prevent fraud at the source. Background checks shall be duly formalized and documented in writing.

FGII seeks to establish and maintain a robust framework to provide reasonable assurance that dishonest acts

are prevented or promptly detected and actioned upon, which have been reinforced through this Policy, which outlines the procedures in relation to the following:

i. **Oversight** – FGII has built adequate procedures and policies to oversee that the Fraud Risk Governance Framework is established, implemented and adequate internal controls exist to prevent, identify, detect, investigate, deter fraud and report frauds.

ii. **Prevention** – FGII will strive towards prevention of fraud at the first place. FGII has well defined procedures to carry out due diligence on the Employee, Agents, Intermediaries, Third Party administrators, etc. In addition, FGII shall have in place following measures:

a. **Due Diligence**: Implement robust underwriting and approval processes to evaluate risks and identify potential fraudulent activities before issuing policies or claims.

b. **Risk Assessment:** Regularly assess and update fraud risks specific to the insurance industry through internal audits and external experts.

c. **Training and Awareness**: Conduct regular training awareness programs to educate employees and stakeholders about fraud prevention, detection, reporting, and ethical conduct.

d. Fraud Monitoring: Implement effective systems and technology to monitor and detect potential fraud patterns or suspicious activities.

FGII shall further conduct the following preventive activities:-

- Fraud detection through data analytics and documents review;
- Awareness on Fraud among existing and prospective customers, its implication and importance of complying with FGII's policies & procedures and identifying/ reporting of suspicious activity;
- Investigate the whistle blower complaint, if any, received from time to time, under supervision of CCO;
- Establish a strong Fraud Risk and Control Assessment;
- Identify red flag indicators and carry out timely investigation thereon;
- Additional red flag indicators identified during the course of the business basis industry experience; and
- Identifying the control weakness and adopting the learnings for process enhancement

iii. **Detection** – All employees of FGII have a responsibility to detect potential fraud and should be familiar with the types of fraud that might occur within his/her area of responsibility and be alert for any indication of irregularities. Every employee shall immediately report any suspected fraud or dishonest act or omission to his/ her Supervisor/ Manager.

6 Constitution of Fraud Control Unit

FGII shall constitute a separate department i.e., Fraud Control Unit ('FCU', 'FGII Accountable Function') for implementing the Fraud Monitoring Framework. FCU must be separated from other functions of the Company and must operate independently under a person from senior management. It will be responsible for laying down appropriate fraud management processes and procedures across the Company. It shall report the status of significant cases of fraud detected in the Company to the Board of Directors through Risk Management Committee (RMC) on Quarterly basis.

Functions of FCU shall include but not be limited to the following:

- FCU shall collate all cases of frauds reported to it or by any other entities.

- FCU shall investigate all such cases and render report to the CRO duly highlighting the breaches of conduct, process and system etc. Report shall also highlight the financial implication, if any.
- FCU shall be responsible for implementing the decisions by RMC
- FCU shall track the closure of the decisions through Action Taken Report (ATR).
- FCU shall get the cases having involvement of non-related entities reviewed and closed through Head – FCU and submit details of such cases to the RMC.
- FCU shall investigate claim cases referred from respective claim departments.
- FCU shall analyse the data based on claim / fraud investigation to know the pattern and potential areas of fraud.
- FCU shall ensure reporting of cases to FCC and convene meeting of FCC for reviewing the findings of the investigation on case of case basis.

- Due Diligence/Background Verification: The HR Department shall conduct due diligence/background verification of employees at the time of on-boarding as per the HR policy. The due diligence of intermediaries, channel partners, vendors, Hospitals, Garages etc. shall be carried out by the respective departments.
- Reporting: FCU shall lay down the procedure for internal / external reporting from / and to various departments.

7 Reporting of Fraud

All persons including employees, vendors, TPAs, agents, intermediaries are expected to take all reasonable steps to prevent the occurrence of Frauds including online Frauds and to identify and report instances of known or suspicious Fraud committed against the Company, whether by the employees or by outside parties.
All employees should timely, expeditiously, unhesitatingly and fearlessly report any Fraud including Cyber / Online Fraud against the Company to FCU at alert@futuregenerali.in
No employee shall investigate / interview / interrogate such cases of actual / suspected frauds himself except the responsible person within FCU or authorized team/ person identified to investigate the same by FCU/CCO.

The identity of the complainant will be maintained confidential and it shall not be disclosed. Detection techniques have been established to uncover fraud events when preventive measures fail or unmitigated risks are realized. FGII detects fraud through means including but not limited to data analysis, investigation, verifying trends, interviewing the alleged etc.

8 Fraud identification and Investigation

8.1 External Fraud

a. FCU 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.

b. Employees are required to be alert and vigilant with respect to external frauds. If any external fraud comes to the attention of any employee, 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.

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

8.2 Internal Fraud

Reporting Procedures - Communicating Concerns about Alleged or Suspected Fraud

a. 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.

b. 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:

    a. The Chief Executive Officer;
    b. Chief Operating Officer
    c. Chief Compliance Officer;
    d. Chief People Officer;
    e. Chief Risk Officer and
    f. Head of Fraud Control Unit;

c. 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.

d. The manager or supervisor shall promptly escalate the concern to the Chief Compliance Officer, the Chief People Officer, the Chief Executive Officer; the Head of Fraud Control Unit or the Chief Risk officer as the case may be.

e. 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.

f. 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.

g. 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.

h. 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.

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

8.2.1 Fraud Investigation, Fact Finding & Corrective Action

i. Preliminary Analysis:

- The alleged internal fraud case is reviewed jointly by Chief People officer and the Head of Fraud Control Unit 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.

Chief People Officer and the Head of Fraud Control Unit shall be excluded from the preliminary analysis or the subsequent investigations if the alleged or suspected internal fraud case involves him/her.

The Fraud Control Unit has the primary responsibility for the investigation of all suspected or alleged internal fraudulent acts as defined in this Policy.

ii. Investigations:

Great care must be taken by the FCU 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 members of the FCU 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 FCU 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 in line with the Company's Record and Retention Policy or as required by applicable laws.
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.

The investigations shall be completed normally within forty-five (45) working days from the disclosure or discovery of the fraud case, however based on the facts and circumstances of each case, the period may be extended beyond 45 working days.

The recovery amounts, the controls implications and the resolution. Management is responsible for resolving fraud incidents 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.

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

iii. 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 based on the principle of proportionality (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.

FCU shall monitor the implementation of the resolution to ensure that proper corrective action was taken and report to the Risk Management Committee accordingly.

9 Fraud Control Committee (FCC)

FCC shall be constituted to review the findings of the investigations done by FCU and to take appropriate actions thereupon.
The Composition of FCC should be as below:

- Chief Compliance Officer
- Chief Financial Officer
- Chief Risk Officer
- Chief Operating Officer
- Chief People Officer

Frequency of Meeting
The Committee shall meet at least once a quarterly basis with a provision for seeking decision through circulation to decide on urgent cases. Such decisions shall be noted at the immediate next meeting of the Committee. The Committee shall be responsible inter-alia for effective implementation and to monitor and decide fraud cases.

Quorum
The quorum for the meetings of the Committee shall be at least three members. In case of Complaints against any members of FCC, the concerned member shall not attend the meetings of FCC wherein the subject matter is being discussed. Further, in case such matter requires investigation by FCU, the concerned member shall restrain from initiating any instruction to FCU. In case, if any woman is summoned to the meeting, presence of a woman representative from the Company is mandatory.
In case of Complaints against the Managing Director and Chief Executive Officer and other Whole-Time Directors, the same shall be reported to the Nomination and Remuneration Committee of Directors.
Head of the Department of the accused shall be invited at the meetings of the Committee without having any right to vote. Head of Fraud Control Unit shall be the permanent invitee at the meetings of the Committee and inter-alia record the proceedings of the meeting and keep safe custody of said minutes ensuring its confidentiality.

10 Reports to the Authority

Based on the data received in the prescribed format from the FCU, Compliance Function shall file a report on statistics on various fraudulent cases which come to light and action taken thereon to the Insurance Regulatory and Development Authority of India ("IRDAI") in forms FMR 1 and FMR 2 (as prescribed by IRDAI 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, as amended theron, 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 Committee appointed 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.

11 Confidentiality and Non – Retaliation

Under the Policy, every reasonable effort shall be made to ensure the confidentiality of the person who has reported the Fraud. The identity of those providing information shall be kept confidential in order to carry out an appropriate, fair and thorough investigation. If a fraud is reported anonymously, the person must provide credible and sufficient information to enable the FCU to investigate. FGII shall adhere to the Anti Retaliation and reporting Concern Policy and ensure that no retaliatory action is taken against any individual for reporting, in good faith, known or suspected Fraud.

12 Roles and Responsibilities

Please include all roles and responsibilities entrusted to each stakeholder (corporate bodies/functions/structures/units) mentioned in the document.

Role	Responsibility
Chief Executive Officer (CEO)	• Receives and Monitors Escalations of Fraud Complaints • ensure that Employees are protected against any form of Retaliation; • receive and approve recommendations received post investigation
Fraud Control Unit (FCU)	• Conducts preliminary investigation • Ensures timely submission of investigation report • Submits recommendations to the CEO • Ensures timely submission of data for reporting purpose • Shall convene periodical meeting of FCC for reviewing the findings of investigation on case of case basis
Chief People Officer	• ensures that investigation is conducted in the right direction. • ensures that the channels for reporting suspected fraud are available to all Employees and third parties;
Chief Compliance Officer	• receives escalations of Fraud complaints. • monitors that any form of Retaliation occurs as a result of a Fraudulent activity being highlighted by an Employee.
Employee	• performs his/ her duties with professional due diligence, care and good faith in compliance with the provisions of Anti - Fraud Policy; • supports with care the internal and external investigations providing true and accurate information when requested by the Compliance Officer(s), by any person appointed to conduct the investigation or by any competent authority(ies); • reports a complaint when he/she becomes aware of any fraudulent activity.
Human Resource (HR)	• Collect Annual declaration on Anti-Fraud policy from existing employees and new employees. • Provide regular and periodic training to all employees upon joining the organization and throughout their association with the Company, in order to clearly communicate expectations for ethical behaviour to employees. • Conduct due diligence of employees at the time of onboarding.
Fraud Control Committee	• Shall review the findings by FCU team on quarterly basis. • shall recommend to the Chief Executive Officer of the Company to take such disciplinary or corrective actions based on the principle of proportionality