

Anti-Fraud Policy and Monitoring Framework Version-6.0

Document Control

Document No.	:	Anti –Fraud Policy and Monitoring Framework
Current Version	:	6.0
Financial Year	:	2026-2027

		Particulars
Document Owner	:	Fraud Investigation Unit
Reviewed By	:	MD and CEO, Risk Management Committee and Audit Committee
Approved By	:	

Classification	:	Internal Use
Distribution List	:	HOD Departments

Issue / Revision History:

Ver	Approved by	Issue / Revision Date	Description
1.0	60 th BOD Meeting	13 th March 2013	-----
2.0	65 th BOD Meeting	28 th July 2018	Incorporating the proactive fraud detection mechanism ISNP
3.0	74 th BOD Meeting	28 th November 2019	In Clause 15-Manner of Detection and identifying E-commerce Frauds: Changes in reporting line: Vertical Heads shall inform about fraudulent activity to DGM –IT and Head –IT.
4.0	82 nd BOD Meeting	25 th February 2021	In the Policy document following changes are incorporated: a. Clause 1: Policy Statement IRDAI Guidelines on Insurance E commerce released dated 9 th March 2017 , necessary clause is included in regard to

Anti-Fraud Policy and Monitoring Framework Version-6.0

			<p>the proactive fraud detection mechanism Insurance Self Network Platform (ISNP) hence, Policy is amended to version 2 in 65th BOD Meeting</p> <p>b. Clause 3: Scope of Policy Section: C</p> <p>Minor Wording Corrected</p> <p>All departments and employees are covered under this policy. All departments are required to incorporate active due diligence measures into its procedures and review these from time to time to prevent and identify frauds incidents if any, specially:</p> <ul style="list-style-type: none"> • Underwriting • Marketing • Claims • PPC • HR/Admin • Finance & Accounts • Legal & Compliance • Health • Information Technology <p>In USGI Fraud Monitoring Framework Diagram</p> <p>COD –Block diagram of Committee of director (COD)is replaced by MD &CEO, as COD is dissolved.</p> <p>Designation Ex–Officio authority nomenclature is corrected.</p> <p>. Designation Ex-officio MD is corrected with Managing Director and Chief Executive Office (MD and CEO).</p> <p>Exe Chairman is replaced to Non-Executive Chairperson.</p> <p>Minor Correction in Block Diagram IRDAto IRDAI</p> <p>clause 5: Fraud Risk Assessment & Implementation of Control</p>
--	--	--	---

Anti-Fraud Policy and Monitoring Framework Version-6.0

			<p>Risk Management Team is replaced by Risk Management Department.</p> <p>d. Clause 6: Due diligence and fraud monitoring by department</p> <p style="padding-left: 40px;">Intermediary Fraud: Agent Licenses are obtained prior to incorporating the relevant intermediary in company database for commission payout. Fraud Complaints/ Grievances, if any reported at USGI customer service is communicated to Risk Management Department.</p> <p style="padding-left: 40px;">Communication to risk management dept instead Internal Audit dept to retained line of communication.</p> <p>Nomenclature is replaced by adding word "Department" instead of "Team"</p> <p>e. Clause 7: Investigation</p> <p>Intimation:</p> <p style="padding-left: 40px;">Suspected frauds noticed within the department through internal due diligence measures should be reported to Management & Risk Management Department by respective HOD immediately on identification.</p> <p>Internal Audit department is replaced by Risk Management</p> <p>Any area which seems suspicious during course of Audit (Internal Audit) including TPA will be reported to the Risk Management Department</p> <p>Commencement</p> <p>Designation Ex-officio Nomenclature</p> <p>Head-HR is replaced with Head-Human Resources. Head Marketing is replaced by Chief Marketing Officer/Deputy CEO-Global Marketing.</p> <p>Managing Director and Exe-Chairman is replaced with MD and CEO and Non-</p>
--	--	--	---

Anti-Fraud Policy and Monitoring Framework Version-6.0

			<p>Executive Chairperson.</p> <p>Internal investigation will be done by Risk Management Department.</p> <p>Commencement of Investigation shall also be kept informed to Audit Committee and Risk Management Committee.</p> <p>f. Clause:8 Disciplinary Action: COD is replaced by MD and CEO</p> <p>MD and Executive Chairman is replaced by MD and CEO and Non-Executive Chairperson.</p> <p>g. Clause :9 Coordination with law enforcement agencies and follow up process on fraud recovery.</p> <p>In case of Fraud has been committed, Risk Management Department shall inform to MD &CEO.</p> <p>MD and Executive Chairman is replaced by MD and CEO and Non-Executive Chairperson.</p> <p>h. Clause 10: Fraud Remediation</p> <p>The Risk Management Department will be updating the status to the Audit Committee and Risk Management Committee.</p> <p>Risk Management Department will be responsible for monitoring and ensuring implementation of action plans and reporting the remediation status to Audit Committee & Risk Management Committee.</p> <p>Audit and Risk Committee is replaced by the Audit Committee and Risk Management Committee.</p> <p>i. Clause 12: Exchange of Information</p> <p>Requisition for information/ documentation relevant to fraud from other insurance company & regulatory authority will be considered by Risk Management</p>
--	--	--	--

Anti-Fraud Policy and Monitoring Framework Version-6.0

			<p>Department. Risk Management Department may share the information</p> <p>MD and Executive Chairman is replaced by MD and CEO / Non-Executive Chairperson</p> <p>j. Clause 13: Review of Policy</p> <p>Risk Management Team is replaced by Risk Management Department.</p> <p>Committee of Director (COD) is dissolved.</p> <p>k. Clause 14: Communication to Policyholder /external parties & training</p> <p>There is minor grammatical mistake in the sentence, hence, it is corrected.</p> <p>clause 15: Change in the Reporting line</p> <p>Vertical Head –IT application, network and database are replaced by Head-IT application</p> <p>Head–IT infra and CISO is incorporated in the Policy.</p> <p>Head –IT application, Head –IT Infra shall report about the online fraud to Chief Technology Officer and CISO.</p> <p>Heads-IT Application, and Head-IT Infra and Chief Information Security Officer (CISO) shall report about fraudulent activity to Chief Technology Officer.</p> <p>Chief Technology Officer and Chief Information Security officer shall perform root cause analysis on identified fraud cases /suspected fraud.</p> <p>Risk Management Department shall keep centralize database for Cyber Frauds.</p>
--	--	--	---

Anti-Fraud Policy and Monitoring Framework Version-6.0

5.0	BOD	2 nd March 2022	Changes mentioned Annexure A
5.0	BOD	Feb 2023	Annual review of policy. No changes proposed.
5.0	BOD	Feb 2024	Annual review of policy. No changes proposed.
5.0	BOD	10 th Feb 2025	Annual review of policy. No changes proposed.

Anti-Fraud Policy and Monitoring Framework Version-6.0

6.0	BOD	11 th Feb 2026	<p>Multiple Changes made to the policy based on IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025 Ref: IRDAI/IID/GDL/MISC/112/10/2025 dtd 9/10/2025.</p> <p>Department Name "Risk Control Unit has been changed to Fraud Investigation Unit.</p> <p>Fraud Reporting has been aligned as per the IRDAI/IID/GDL/MISC/112/10/2025 dtd 9/10/2025</p>
-----	-----	---------------------------	--

Table of Contents

1.	Policy Statement	9
2.	Fraud Definition:	9
3.	Scope of Policy:	9
4.	Fraud Risk Governance:	100
5.	Fraud Risk Assessment & Implementation of Controls:	111
6.	Due diligence and fraud monitoring by departments:	133
7.	Investigation:	144
a)	Intimation	144
b)	Commencement	144
c)	Execution	155
d)	Reporting	155
8.	Disciplinary Action:	155
9.	Co-ordination with Law Enforcement Agencies & Follow up process on Fraud Recovery:	166
10.	Fraud Remediation:	166
11.	Regulatory Reporting:	166
12.	Exchange of Information:	166
13.	Review of Policy:	177
14.	Communication to Policyholders/external parties, distribution channels, employees & training:	177
15.	Fraud Committed on Insurance Self Network Platform (ISNP):	177
a.	Potential Areas of E-Commerce and Cyber Fraud on ISNP:	177
b.	Manner of Detecting and Identifying E-Commerce Frauds	187
c.	Follow – up Mechanism for prosecuting person who committed fraud	188
d.	As per direction given by DAC, appropriate action (includes legal action) against employees/other than employees involved in such fraud /suspected cases hereby may include:	188
	Case a: Other than Employee	188
	Case b: Any Fraudulent employee/vendors	188
e.	Prevention and Mitigation Controls:	188
f.	Exchange of Information and Record Keeping:	188
16.	Insurance Information Bureau (IIB)	19
17.	Annexure I: Illustrative List of Insurance Fraud	19
	Policyholders/ Claims Fraud	19
	Distribution Fraud	20
	Internal Fraud	21
	External Fraud	21
	Affinity Fraud & Complex Fraud	21

Anti-Fraud Policy and Monitoring Framework Version-6.0

Note – Anything other than the above said categories of fraud/ misrepresentation/ misconduct will be considered for investigation and necessary action. ----- 22

19. Annexure II: Fraud Monitoring Report (FMR)----- **Error! Bookmark not defined.**2

FMR – 1 -----
222

1. Policy Statement

Universal Sampo General Insurance Ltd., (USGI) is committed to conducting business in an environment of honesty and integrity and will strive to eliminate fraud from all operations. The USGI Anti-Fraud Policy (“Policy”) sets forth the framework and principles required for the anti-fraud program.

Objective of Zero tolerance to fraud would be adopted by USGI. The Company will not accept any level of dishonest or fraudulent act by any employee, intermediary, shareholder, stake holder or any other party. The company shall follow the principle of proportionality that is aligned to the above said antifraud goals & objectives.

The company shall have a Board approved Anti-Fraud Policy in place which will be annually reviewed.

2. Fraud Definition:

“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.

3. Scope of Policy:

A. Broad categories of Fraud:

- 1) Internal Fraud : Involves staff, including employee and / or senior management.
- 2) Distribution Channel Fraud : Involves distribution channel.
- 3) Policyholder Fraud : Involves in obtaining coverage or payment, servicing, or claim of

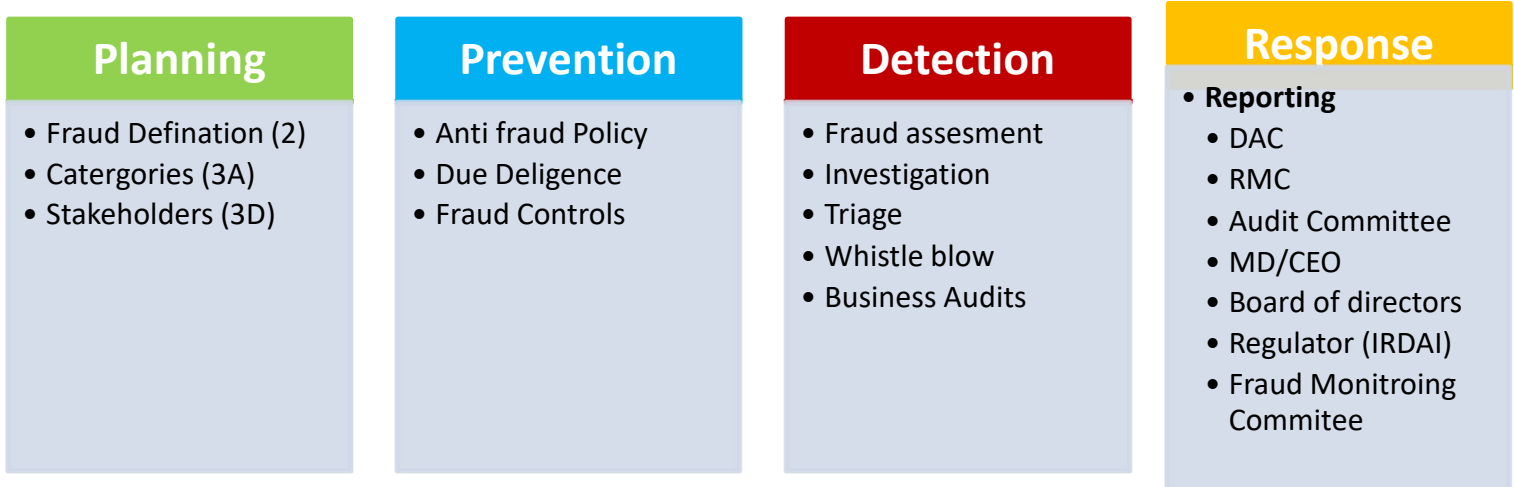
Anti-Fraud Policy and Monitoring Framework Version-6.0

insurance policy.

- 4) External Fraud : Involves external parties' / service providers / vendors.
- 5) Affinity Fraud or Complex Fraud : Fraud involving collusion among one or more fraud perpetrators in the above categories.

B. This policy applies to any Internal or External Parties, which are directly or indirectly associated with the USGI for Providing or Consuming services. All departments and employees are covered under this policy required to incorporate active due diligence measures into its procedures and review these from time to time to prevent and identify fraud incidents if any

USGI FRAUD MONITORING FRAMEWORK



Anti-Fraud Program – Procedure of Fraud Monitoring & Control

4. Fraud Risk Governance:

Fraud Monitoring Committee (FMC) is responsible for operationalizing the Fraud risk management framework within the insurer and oversees activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying.

Fraud Investigation Unit (FIU), independent from internal audit, to support FMC in discharging its functions and effective implementation of measures suggested by FMC.

FMC is headed by Chief Risk Officer and includes senior representatives such as Chief Finance Officer, Appointed Actuary, Head Internal audit, Chief Underwriting Officer and Chief Customer Officer.

Functions of the FMC: The FMC shall, inter alia:

Anti-Fraud Policy and Monitoring Framework Version-6.0

- a) recommend and regularly update, based on experiences, appropriate measures on fraud risk management to various functions.
- b) oversee prompt responses to instances or suspicions of fraud
- c) maintain all relevant details pertaining to each instance of fraud
- d) facilitate 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.
- e) conduct an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerability mitigation across business lines and activities for fraud, using past experiences, emerging trends & Red Flag Indicators (RFIs), etc.
- f) identify areas for improvement and adaptation of the Fraud Risk Management Framework.

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 insurer.
- 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 fraud.

5. Fraud Risk Assessment & Implementation of Controls:

Fraud Investigation Unit is responsible for overseeing fraud risk assessments and ensuring that adequate anti-fraud program has been established and measures implemented based on business, activities, past experience, trends, etc.

Zero tolerance for fraud and appropriate fraud risk management framework sensitive to its business profile to enable it to deter, prevent, detect, report and remedy insurance frauds.

a) Identify potential areas of fraud Performing fraud risk assessments, including the identification and evaluation of fraud risks and potential fraud schemes

Fraud Investigation Unit will identify the areas of business & specific departments of the organization that are vulnerable to insurance frauds (Refer Annexure I for Illustrative list of Potential Fraud).

Fraud Investigation Unit will also do periodic fraud assessments basis red flag indicators

Fraud risk & controls identified will regularly updated in Risk Register of the departments/ Risk Assessment Matrix & will be reported to Chief Risk officer & Risk Management Committee.

Anti-Fraud Policy and Monitoring Framework Version-6.0

The Risk Management Committee (RMC)/ Fraud management committee of the insurer shall be responsible for effective implementation and oversight of the fraud risk management framework.

The fraud risk management framework shall be specific to the insurance business considering the nature of business, size, risk profile, overall business strategy, products, distributions channels, technology infrastructure, and any other applicable parameter including various activities carried out by the insurer.

It shall inter-alia include: Board approved Anti-Fraud Policy: The Board approved Anti-Fraud Policy shall be relevant to the entire operations of the insurer's business and activities. The insurer shall review such policy regularly, at least annually, and it shall, inter-alia, include:

- a) red flag indicators, as applicable.
- b) adequate procedures to deter, prevent, detect, report and remedy fraud in each category of fraud across various activities
- c) responsibilities, delegation of authorities for all relevant functions including for identified sensitive posts
- d) fraud investigation process, including internal turnaround times from identification to remedy, designated officer(s) for reporting incidents of fraud and report submission
- e) mechanism for appropriate action in case of non-compliance to the fraud risk management framework and against the fraud perpetrators f) appropriate and adequate resources to the Fraud Monitoring Unit to carry out its functions effectively.
- g) due diligence procedures for staff recruitment and vendor engagement h) review process to identify "missed" insurance fraud detection opportunities i) whistle blower protection policy

b) Establishing and implementing adequate internal controls regarding the detection and prevention of fraud and ensuring the controls are designed and operating effectively.

Fraud Risk indicators are defined by the Fraud Investigation Unit for every fraud risk identified & it will be continuously monitored. Quarterly Report of the fraud monitoring status will be presented in Risk Management Committee.

Fraud Investigation Unit is responsible for performing independent reviews to evaluate the adequacy and effectiveness of anti-fraud controls and communication of control deficiencies and weakness to the Risk Management Committee on a continuous basis.

c) Reporting to risk management committee on the result of fraud risk and control assessments, any issues and associated action items.

Fraud Investigation Unit is responsible for performing independent review to evaluate the adequacy and effectiveness of anti-fraud controls and communication of control deficiencies and weakness to the Risk Management Committee on continuous basis.

Anti-Fraud Policy and Monitoring Framework Version-6.0

Recommendation Action Plan will also be placed in Risk Management Committee for their perusal & continuously followed up with the process owner for action initiated.

6. Due diligence and fraud monitoring by departments:

Every department as listed in 3 C above should implement suitable due diligence measures for Potential Fraud Risks (refer Annexure I) and update relevant Risk registers. Department policies and processes should be updated to cater all identified fraud risk.

Illustrative list of due diligence measures for these departments are mentioned below:

a) Internal Fraud:

USGI employees are made aware of company policies at the time of Induction Training which include education of HR policy, AML policy, Whistle blowing policy, Anti-fraud policy and compliance policy. Any substantial complaint can be referred through fraud.alert@universalsompo.com ; whistleblow@universalsompo.com .

Fraud involving internal staff, including employees and / or senior management.

b) Distribution Channel Fraud:

Any fraud or mis-selling (Covered under 3 (a)) done by USGI agent can be reported using fraud.alert@universalsompo.com or customer service department.

Fraud involving distribution channels such as Intermediary, Broker, OEM etc.,

c) Policyholders/ Claims Fraud:

- Fraud involving any person(s), in obtaining coverage or payment during the purchase, servicing, or claim of an insurance policy.
- Claim Department monitors on case-to-case basis the validity of every claim reported & are approved by competent authority defined as per matrix.
- Fraud Indicators has been defined by the Fraud Investigation Unit & Claim department & educated to its personnel for identifying the fraud prone instances.
- AML Policy Compliance is ensured while making the claim & refund payment
- Any substantial complaint can be referred through fraud.alert@universalsompo.com ; whistleblow@universalsompo.com

- d) **External Fraud:** Any suspicion, fraud alert, referral through internal or external sources will be investigated by Fraud Investigation Unit and will be reported as per fraud Monitoring framework. Any substantial complaint can be referred through fraud.alert@universalsompo.com ; whistleblow@universalsompo.com

Fraud involving external parties' / service providers / vendors etc.

- e) **Affinity Fraud or Complex Fraud:** Fraud involving collusion among one or more fraud

perpetrators in the above categories.

7. Investigation:

a) Intimation

The below mentioned scenarios will trigger the investigation into potential fraud cases:

- Suspected frauds noticed within the department through internal due diligence measures should be reported to Management, Fraud Investigation Unit and respective HODs immediately on identification.
- Employee, Customer, Intermediaries & Third party can report fraud to ID fraud.alert@universalsompo.com and Fraud Investigation Unit will take action and communicate the same to Management, Authority & Risk management committee
- Any area which seems suspicious during course of Audit (Internal Audit) including Third Party Administrator (TPA), External parties including vendors, affiliates will be reported to the Fraud Investigation Unit
- Fraud Grievances reported to USGI Customer Service
- Investigation of Management Request

b) Commencement

Based on fraud intimation, indicator, reference, Fraud Investigation Unit will check the intensity of the trigger communicated & take decision on whether the investigation needs to be initiated.

Depending on the magnitude and the complexity of the fraud as evaluated by Fraud Investigation Unit, independent investigation will be carried out based on the SOP of Fraud Investigation Unit. In case internal fraud is investigated, assistance would be sought from Chief People Officer, whenever required. Similarly, in cases related to intermediary, assistance would be sought from concerning Department Head.

Investigation information and results will not be disclosed or discussed with anyone other than those with a legitimate need to know to avoid damaging the reputation and privacy of persons under investigation or who may be involved in legal proceedings, and who may not have been involved in any misconduct. This policy requirement serves to protect the USGI from potential liability and in compliance with the IRDAI guidelines on Insurance Regulatory and Development Authority of India (Insurance Fraud Monitoring Framework) Guidelines, 2025 Ref IRDAI/IID/GDL/MISC/112/10/2025 dated 09.10.2025

c) Execution:

Investigations will be conducted without regard to any person's relationship to the organization, position or length of service. The company will keep records of all actions in the investigation, to ensure success in any future criminal, civil or disciplinary action.

Fraud Investigation Unit will be provided with full access of work area in question, including any files, computers and basis the gravity of case in coordination with **People, Culture and Capability Team** request for providing bank a/c statements, mobile bills and other necessary information which may support the process of Investigation. All searches are to be conducted in a lawful manner, to ensure that evidence is admissible in court, if required. The Investigation team will keep records of any action or handling of evidence. After completion of Investigation, report with evidence to be submitted to respective HODs

Interviews, if necessary, will be structured and documented as much as possible. Timelines for all category of fraud investigations are separately documented as per the triage procedure.

d) Reporting

In case of Internal Fraud Investigation, the final report will be submitted to People, Culture and Capability team for necessary action.

Upon completion of the investigation, the final outcomes of cases related to Distribution Channel Fraud shall be communicated to the concerned Distribution Channel Head

Upon completion of the investigation, the final outcomes of Claims Fraud reports shall be formally submitted to the concerned Claims Team for necessary action

The final outcomes of Policyholder, Affinity, Complex, and External Fraud reports shall be shared with the concerned stakeholders, and decisions shall be taken based on the severity of the cases in coordination with the relevant departments.

Quarterly reports related to all category of Frauds reporting being done to Risk Management Committed (RMC) and Fraud Monitoring Committee (FMC).

8. Disciplinary Action:

Disciplinary Action committee (DAC) has the responsibility and authority authority to consider the findings of fraud investigations and to determine the appropriate disciplinary actions to be taken against the Employee, intermediaries, External Parties or claimant involved. Investigation team should act quickly when

Anti-Fraud Policy and Monitoring Framework Version-6.0

suspected fraud is intimated & gives the communication to CRO, CHRO
Disciplinary actions on detection of fraud will be taken as per DAC Procedure
All local applicable laws and legislation must be considered in the execution of this policy requirement.

9. Co-ordination with Law Enforcement Agencies & Follow up process on Fraud Recovery:

Where it is reasonably believed that a fraud has been committed, Fraud Investigation Unit (after approval from Senior Management and Non-Executive Chairperson) will report the case to the regulator or other relevant authorities, if required, in accordance with the prevailing laws and regulations.

If legal action required after the fraud is being detected and established, the report would be shared with Legal Head. Wherever required the Legal team in coordination with Fraud Investigation Unit will take the following steps to take necessary legal action:

- Lodging an FIR against the concerned party.
- Filing a case in the Court of Law for Recovery, Civil Suit and Criminal case based on the appropriate jurisdiction.
- Reinvestigation and Police complaints cases can be done by with Fraud Investigation Unit as per the defined process.

Provisioning/Write-off Fraud Losses

All provisioning and write-off losses shall be processed in compliance with the procedures prescribed under the Finance SOP.

10. Fraud Remediation:

Weakness in procedures or controls identified in fraud investigation must be addressed by process owners without undue delay. Action Taken Report giving the status of process change as recommended by the Fraud investigation report should be presented into Disciplinary committee. (basis the severity and gravity of the case)

The team is also responsible for ensuring that Fraud events are reviewed and considered for scenario analysis and inclusion in the Risk Assessments Matrix & Risk Register.

11. Regulatory Reporting:

The statistics on various fraudulent cases which come into light & action taken thereon shall be filled with the IRDA authority in forms FMR 1 (as per circular no-IRDAI/IID/GDL/MISC/112/10/2025) providing details of outstanding fraud instances & closed fraud instances every year within 30 days of close of the financial year.

12. Exchange of Information:

Anti-Fraud Policy and Monitoring Framework Version-6.0

Requisition for information/ documentation relevant to fraud from other insurance company & regulatory authority will be considered by Fraud Investigation Unit
Departments may share the information relevant to customer frauds with General Insurance Council, Industry Subgroup in Insurance Industry, our partner banks or other institution

13. Review of Policy:

The Fraud Investigation Unit will review the policy on annual basis & changes if any will be presented to the BOD for review and approval.

14. Communication to Policyholders/external parties, distribution channels, employees & training:

Apart from various measures for creating awareness amongst our potential and existing policyholders, snippets/ do's & don't/ knowledge series or other awareness measures shall be updated on website & other platforms. Further the policy document issued to policyholders should include sufficient reference to this policy.

At the time of *Induction Training*, USGI Employees are made aware of various company policies which include HR policy, AML policy, whistle blower policy, **Anti-Fraud Policy** and all the necessary Compliance policies. Individual Departments will be responsible to train its employees with respect to various fraud scenarios & way to control it.

In addition to the above, USGI will also provide periodic training to distribution channels as well on fraud risk management.

15. Fraud Committed on Insurance Self Network Platform (ISNP)

Insurance Self-Network Platform mean an electronic platform set-up by USGI with the permission of the IRDAI for selling and servicing the insurance products on web portal.

Potential Areas of E-Commerce and Cyber Fraud on ISNP:

1. Transaction level activity carried on USGI website using fake /stolen credit card or bank account details.
2. Threats to confidential data of company due cyber threat like -phishing, unethical hacking and un-authorize access to USGI network.
3. Intrusion to company website bypassing the firewall route.
4. Fake email account generation for bogus customer using misrepresentation in KYC documents.
5. Payment gateway merchant execute fraud during settlement of premium amounts collected through web portal on behalf of the USGI.
6. Any other online fraud that executed on ISNP Portal
7. Establish and implement robust cybersecurity framework to protect against evolving cyber frauds or threats.
8. Continuously monitor and strengthen systems and processes for fraud risk management, such as incident databases, customer verification, and access control.
9. Utilize a team with relevant risk and technological expertise to manage cyber fraud risks across various insurance business lines.
10. A separate cyber security policy and framework is in place.

Anti-Fraud Policy and Monitoring Framework Version-6.0

Manner of Detecting and Identifying E-Commerce Frauds

USGI have in place sufficient mitigation controls to minimize impact of all identified frauds in ISNP portal. Head – Fraud Investigation Unit and CISO shall report about fraudulent activity to CRO and Chief Technology Officer.

Chief Information Security Officer and Operations Head shall perform root cause analysis involving Fraud Investigation Unit on identified fraud cases /suspected fraud. Such cases shall be brought into notice of Senior Management. Senior Management shall give directions to take appropriate action against such fraud cases /suspected fraud cases.

Follow – up Mechanism for prosecuting person who committed fraud

As per direction given by DAC, appropriate action (includes legal action) against employees/other than employees involved in such fraud /suspected cases hereby may include:

Case a: Other than Employee ---

- a. Lodging the FIR and filing cases against such fraud in the court as per Information Technology Act, 2000

Case b: Any Fraudulent employee/vendors ---

- a. Any employee/s found involved in fraudulent activity will lead to termination of employment. Appropriate disciplinary action (includes recovery of damage thus caused) followed by lodging the FIR against such employee/s.
- b. Any Vendors/TPA/Garage/Hospitals or any other associated affiliates found involved in fraudulent activity will lead to discontinuation of vendor service. Appropriate disciplinary action (including recovery of damage (financial and reputational) thus caused) followed by lodging the FIR against such entities/blacklisting/necessary disciplinary action as per the guidelines is the sole discretion of USGI Senior Management.

Prevention and Mitigation Controls:

1. The IT Department, CISO, Fraud Investigation Unit shall implement such controls on its Insurance Self Network Platform (ISNP) that prevent and deter any online transactions.
2. Privacy of personal information and data security
 - USGI shall keep the personal information collected during the course of the business transaction confidential and prevent its misuse.
 - USGI shall put in place efficient measures to safeguard the privacy of the data that is maintained on systems to prevent manipulation of records and transactions.
 - USGI shall ensure that data security maintained as per Authority's rules/regulations/guidelines and applicable Acts and Statutes

Exchange of Information and Record Keeping:

Fraud Investigation Unit shall maintain centralize database of reported E-

Anti-Fraud Policy and Monitoring Framework Version-6.0

Commerce and cyber frauds. The fraud information shall be reported to General Insurance Council on FRMP Portal and IRDA FMR Reports and /or any others reports desired by Authority.

16. Insurance Information Bureau (IIB)

To ensure that the data available with USGI is effectively utilized to prevent frauds in insurance sector, we are actively participating in the Fraud Monitoring Technology Framework of IIB, as applicable to our businesses, to help the insurance industry combat fraud and protect policyholders & all stakeholders to regularly share to IIB, through designated channel. The details of distribution channels, hospitals, third party vendors and fraud perpetrators blacklisted periodically. IIB maintains the caution repository concerning all such details in order to safeguard the integrity of the insurance sector by preventing the involvement of those with a record of fraudulent activities. The responsibility of submission of data will be followed by Operations dept. in coordination with Fraud Investigation Unit.

17. Annexure I: Illustrative List of Insurance Fraud

<u>Policyholders/Claims Fraud</u>	<u>Potential Areas of fraud:</u>
	<ul style="list-style-type: none">- Staged motor accidents.- Multiple claim intimation with duplicate supporting.- Conflicting reports from insured, creditors, regarding the quantum and proof of loss.- Reporting of a high quantum claim within the short duration of commencement of policy.- Impersonation of individuals claiming to have been injured in the motor accident.- Falsification of motor vehicle/list of household articles/ insured goods etc., Theft reports.- Exaggerated claim amounts as against the actual loss- Insurance claims for preexisting motor vehicle damage.- Intentional damage caused to property in order to claim the insurance benefits.- Exaggerated health claims or prolonged treatment.- Hospitalization claim where no hospital exist.

Anti-Fraud Policy and Monitoring Framework Version-6.0

	<ul style="list-style-type: none"> - Impersonation of patient - Submission of fabricated medical bills. - Submission of exaggerated medical bills by Hospitals and unsubstantiated surgery bills not related to original reason for hospitalization. - Treatment not supported by related diagnosis reports or treatment with no diagnosis report. - Incomplete supporting documents. - Claimants/ Beneficiaries with questionable insurable interest
<p><u>Distribution Fraud</u></p>	<p><u>Potential areas of Fraud:</u></p> <ul style="list-style-type: none"> - Frequent change of address - Abnormal increase in business volumes in a short period of time. - Licensed intermediaries colluding with the false claimants and rendering the assistance in claim settlement to the detriment of company. - Authorized insurance intermediaries issuing fake cover notes/fake premium receipts. - Authorized insurance intermediaries delaying the remittance of premium collections beyond the prescribed time limit. - Portfolio containing substantial adverse claim history. - Alleged cases of corruption on insurance intermediaries registered with/licensed by insurance companies. - Collecting (from clients) & remitting (to office) different amount of premium i.e., retaining part of the premium collected. - Embezzlement of Policyholders' money. - Commission fraud. - Non-disclosure or misrepresentation of the risk features with an aim to seek reduced premiums.

Anti-Fraud Policy and Monitoring Framework Version-6.0

<p><u>Internal fraud</u></p>	<p><u>Potential areas of fraud:</u></p> <ul style="list-style-type: none"> - Cases of negligence and cash shortages. - Misappropriation of funds either belonging to the company or the policyholders. - Theft of official data. - Theft or misuse of property, facilities or services. - Deriving profit personally from an official position or enabling family members or others to do so. - Forgery or alteration of any document or account belonging to the insurer or its clients. - Personnel of insurance company conniving with the claimants in making false claims and/or setting the claims. - Employees suspected of corruption in past companies. - Any fraud, whether or not material, that involves management and other employees who have a significant role in internal controls. - Any attempt to conceal fraudulent activities or support an attempt to conceal fraudulent activities.
<p><u>External fraud</u></p>	<p><u>Potential areas of fraud:</u></p> <ul style="list-style-type: none"> - Alteration in the documents by vendors. - Being offered a bribe or inducement by a partner or supplier. - Receiving fraudulent (i.e., intentionally inaccurate, rather than erroneous) invoices from supplier. Known instances of corruption, deception or misuse by a supplier or partner. <p>Cyber threats lead to manipulation in online transactions</p>

Anti-Fraud Policy and Monitoring Framework Version-6.0

<u>Affinity Fraud & Nexus fraud</u>	Fraud involving collusion among one or more fraud perpetrators
--	--

Note – Anything other than the above said categories of fraud/ misrepresentation/ misconduct will be considered for investigation and necessary action.

18. Annexure II:

FMR – 1

Fraud monitoring Report

Name of the Insurer:
Report for the year ending:

Part I

Fraud outstanding – business segment wise*:

Sr. No	Description of fraud	Unresolved cases at the beginning of the year		New cases detected during the year		Cases closed during the year		Unresolved cases at the end of the year	
		No.	Amount involved (Rs. Lakh)	No.	Amount involved (Rs. Lakh)	No.	Amount involved (Rs. Lakh)	No.	Amount involved (Rs. Lakh)
	Internal Fraud								
	Distribution Channel Fraud								
	Policyholder and/or Claims Fraud								
	External Fraud								
	Affinity Fraud or Complex Fraud								
	Total								

In addition to the above, irrespective of the category of fraud, details of **Cyber / New Age Fraud** shall be reported separately in the following table.

SI No	Brief description of Cyber Fraud (nature of data used to carry out the fraud, modus operandi, etc)	Financial Impact	Other relevant details

Part II – Age-wise analysis of unresolved cases

Anti-Fraud Policy and Monitoring Framework Version-6.0

Sl No	Unresolved Cases at the end of the year (age-wise)	Number	Amount Involved (In Lakh)
1	30-60 days		
2	60-180 days		
3	180-360 days		
4	More than 360 days		

Part III

Cases reported to Law Enforcement Agencies

Sr. no.	description	Unresolved cases at the beginning of the year		New cases reported during the year		Cases closed during the year		Unresolved cases at the end of the year	
		No	Amount Involved (Lakh)	No	Amount Involved (Lakh)	No	Amount Involved (Lakh)	No	Amount Involved (Lakh)
	Cases reported to Police								
	Cases reported to CBI								
	Cases reported to other agencies (specify)								
	Total								

*Business segments shall be as indicated under IRDAI (Actuarial, Finance and Investment Functions of Insurers) Regulations 2024

CERTIFICATION

Certified that the details given above are correct and complete to the best of my knowledge and belief and nothing has been concealed or suppressed.

Date:

signed/-

Place:

Name of Chief Executive Officer of the Insurer