Document Control

Document No.	:	**Anti –Fraud Policy**
Current Version	:	3.0
Financial Year	:	2019-2020

		Particulars
Document Owner	:	Risk Management Department ,Internal Audit Department
Reviewed By	:	COD ,Risk Management Committee and Audit Committee
Approved By	:	BOD dated : 29th November 2019

Classification	:	Internal Use
Distribution List	:	HOD Departments

Issue / Revision History:

Ver	Approved by	Issue / Revision Date	Description
1.0	60th BOD Meeting	13th March 2013	-------
2.0	65th BOD Meeting	28th July 2018	Incorporating the proactive fraud detection mechanism ISNP
3.0	74 th BOD Meeting	29th November 2019	In Clause 15-Manner of Detection and identifying E-commerce Frauds: Changes in reporting line: Vertical Heads shall informed about fraudulent activity to DGM –IT and Head –IT.

1. Policy Statement:

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.

Zero tolerance approach to fraud would be adopted by USGI. The Company will not accept any level of dishonest or fraudulent act by any employee, intermediary or any other party.

As per the IRDAI guidelines on Insurance E-Commerce issued vide circular no IRDA/INT/GDL/ECM/055/03/2017 dated-9th March 2017 USGI has incorporate new amendment in existing Anti-Fraud policy Version-1.

2. Fraud Definition:

Fraud generally involves intentional dishonest acts committed to secure an unfair or unlawful gain for oneself or another, or a loss to another, and can include misuse or conversion of corporate property or resources for personal use.

3. Scope of Policy:

A. Broad categories of Fraud:

- Policyholders/Claims Fraud – Fraud executed while purchase and execution of an insurance product, including a fraud at the time of making a claim.
- Intermediary fraud – Fraud perpetuated by an insurance agent/corporate agent/broker/intermediary/TPA against the company or policyholder.
- Internal Fraud – Fraud and Misappropriation by its internal staff (Director, Manager, and/or any other officer or staff member).
- External Fraud – Fraud committed by any external party against the company.
- E-Commerce and Cyber Fraud – fraudulent activity related to E-Commerce and Cyber Frauds.

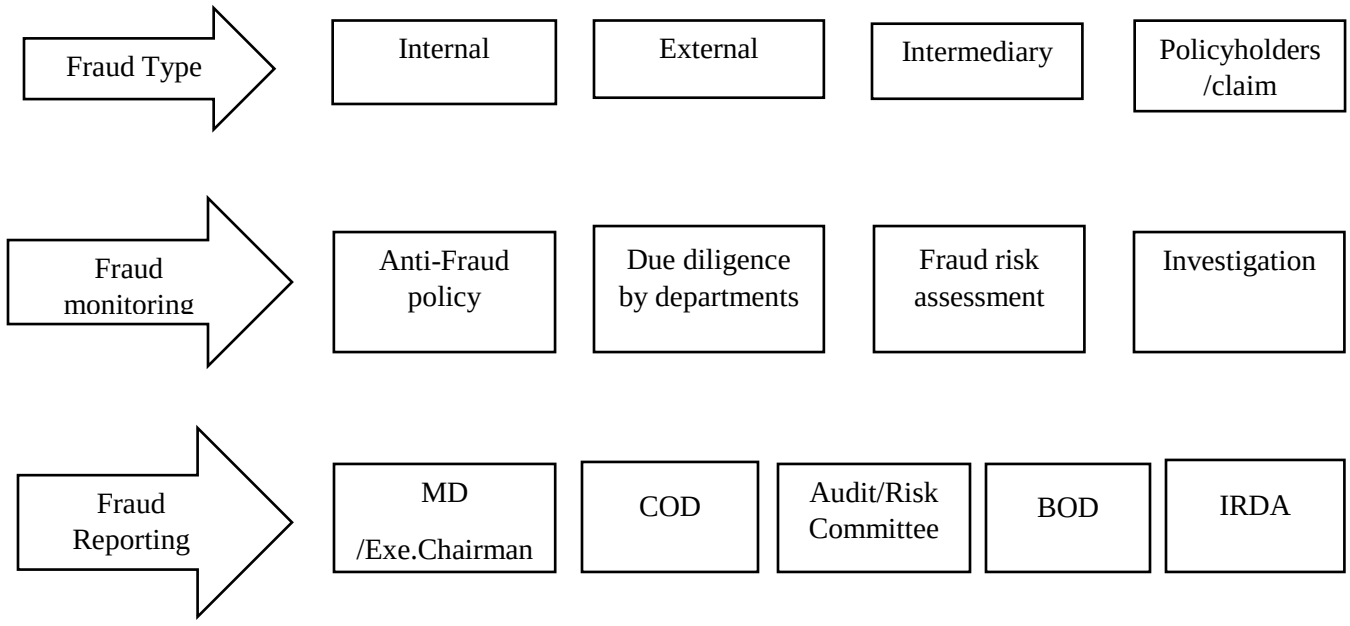
B. This policy applies to any fraud or suspected fraud involving:

- Employees
- Policyholders
- Intermediaries (Agents, Brokers, Surveyors & TPA's)

- Consultants/Vendors/Contractors
- Any Other party

C. Though all departments and employees are covered under this policy the following departments would be 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:
    - Underwriting
    - Marketing
    - Claims
    - PPC
    - HR/Admin
    - Finance & Accounts
    - Legal & Compliance
    - Health
    - Information Technology

USGI FRAUD MONITORING FRAMEWORK



Anti-Fraud Program

4. Fraud Risk Governance:

USGI Risk Management Committee is responsible for overseeing of fraud risk assessments and ensuring that adequate anti-fraud program has been established and measures implemented.

5. Fraud Risk Assessment & Implementation of Controls:

USGI Risk Management Committee is responsible for overseeing of fraud risk assessments and ensuring that adequate anti-fraud program that consists of:

- **Performing fraud risk assessments, including the identification and evaluation of fraud risks and potential fraud schemes-:**

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

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

- **Establishing and implementing adequate internal controls with regard to the detection and prevention of fraud and ensuring the controls are designed and operating effectively.**

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

  Risk management team 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. 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) & update the 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:

- **Policyholders/ Claims Fraud:** Claim Department monitors on case to case basis the validity of every claim reported. Post Loss Endorsements are approved by competent authority defined as per matrix. Fraud Indicators have been defined by the Claim department & educated to its personnel for identifying the fraud prone instances. In addition to above, **AML Policy** Compliance is also ensured while making the claim & refund payments. Company has defined a criteria based on which Suspicious Transaction are identified & reported to relevant Authority as per AML policy.
- **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 Internal Audit/Risk Management Team.
- **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.
- **External Fraud:** Prior to generating the vendor code in accounting system, KYC documents are obtained from the vendors by respective departments. Before making any payment, proper approvals are sought from the user department.

7. Investigation:

- **Intimation**

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

  - Suspected frauds noticed within the department through internal due diligence measures should be reported to Management & Internal Audit Department by respective HODs immediately on identification.
  - Fraud highlighted by employees in accordance with the whistle blowing policy.
  - Any area which seems suspicious during course of Audit (Internal Audit) including TPA audits.
  - Fraud Grievances reported to USGI Customer Service
  - Management Request

- **Commencement**

  Based on fraud intimation, USGI management 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, investigations will be carried out either in-house or by external parties such as external audit firms with specialized forensic accounting expertise and access to criminal law expertise. In case fraud to be investigated is related to employees, assistance would be sought from Head HR whenever required. Similarly in cases related to intermediary assistance would be sought from Head Marketing.

  The decision whether to use internal or external investigation services, or a combination of both, will be made by the Managing Director/Exec Chairman. Internal investigation may be done by Internal Audit or another function as per directive by the management. Commencement of Investigation shall be informed to COD, Risk Management Committee & BOD.

  Investigation information and results will not be disclosed or discusses with anyone other than those with a legitimate need to know. This is an important policy requirement to avoid damaging the reputation and privacy of persons under investigation or who may be involved in legal proceedings, and who may actually not have been involved in any misconduct. This policy requirement serves to protect the USI from potential liability.

- **Execution**

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

  Full access of work area in question, including any files and computers should be given to the Investigation Team (In-house o External). 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.

  Interviews, if necessary, will be structured and documented as much as possible.

- **Reporting**

  Once investigation is completed, a report will be issued to the management detailing the findings and conclusions including recommendations for future action.

  Results of investigations will be kept strictly confidential & will be shared only on need to know basis. This is important to avoid damaging the reputation of those suspected of wrong doing and subsequently found innocent, and to protect the company from potential civil liability and loss of reputation and goodwill.

  Final report of investigation will be placed before Management, COD, Audit Committee, Risk Management Committee and BOD for their perusal.

8. Disciplinary Action:

COD, MD & Exec Chairman has the responsibility and 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 fraud is first suspected & gives the communication to COD, MD & Exec Chairman. Investigation team should not wait until investigations are completed before acting.

COD, MD & Exec Chairman should make appropriate decision with respect to disciplinary action to be initiated as soon as reasonable grounds of evidence have been established.

Following could be the disciplinary actions (*) on detection of fraud:

- Denial of access to his/her working area, including access to the computer, systems, documents, records, or any other work-related matters, pending finalization of the investigation.
- Verbal or written reprimand.
- Punishment such as unpaid suspension or loss of privileges or benefits.
- Implementation of a probationary period, during which the employee will be carefully monitored.
- Denial of a pending or planned promotion.
- Demotion from the current position of authority.
- Dismissal from the company.
- Civil action to recover proceeds of fraud.
- Report of fraud to law enforcements for possible criminal action.
- Termination of contract (with the intermediary & external party).
- Denial of claims.
- Denial use of cover notes & recovery (of cover notes) in inventory.

(*) disciplinary action as described in HR policy may also be considered.

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, internal Audit team/ Risk Management team (after approval from Exec Chairman and MD) will report the case to the regulator or other relevant authorities, if required, in accordance with the prevailing laws and regulations.

After the fraud is being detected and established, the report would be shared with Head-Legal. Where ever required the Legal team will take the following steps so as to recover the amount and file necessary legal complaint against the concerned party:

- Lodging an FIR against the concerned party.
- Filling a case in the Court of Law for Recovery

Provisioning/Writing-off Fraud Losses

Creation of provision & subsequent write off will be done based on the report/opinion provided by Legal department / concerned official handling the case in consultation with Managing Director & Executive Chairman.

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 in Audit &Risk Committee.

Internal Audit/ Risk Management Team will be responsible for monitoring and ensuring implementation of action plans and reporting the remediation status to Audit& Risk Management Committee.

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 & FMR 2 (as per circular no-IRDA/SDD/MISC/CIR/009/01/2013) providing details of outstanding fraud instances & closed fraud instances every year within 30 days of close of the financial year.

12. Exchange of Information:

Requisition for information/ documentation relevant to fraud from other insurance company & regulatory authority will be considered by Internal Audit/ Risk Management Department. Internal Audit/ Risk Management Team may share the information after approval from MD/Exec Chairman.

Departments may share the information relevant to customer frauds with General Insurance Council, Industry Subgroup in Insurance Industry, our partner banks or other institution after approval from MD/Exec Chairman.

13. Review of Policy:

The risk management team will review the policy on annual basis & changes if any will be presented to the BOD/COD for review and approval.

14. Communication to Policyholders/external parties & training:

Apart from various measures for creating awareness amongst our potential and existing policyholders, updated anti -fraud policy should be displayed on the USGI website. Further he policy document issued to policyholders should include sufficient reference to this policy.

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

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

Manner of Detecting and Identifying E-Commerce Frauds

E-Commerce Fraud being a serious threat to the Company hence early identification detection is important. USGI have in place sufficient mitigation controls to minimize impact of all identified frauds in ISNP portal. Vertical Heads of Web Application, Networks, Database and Information Security Officer shall report about fraudulent activity to Deputy General Manager (DGM)-IT and Head-IT.

Head –IT and Chief Information Security officer shall perform root cause analysis 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 Senior Management, appropriate action (includes legal action) against employees/other than employees involved in such fraud /suspected cases hereby:

Case a: Other than Employee ---

a. Lodging the FIR and filing cases against such fraud in the court.

Case b: Any Fraudulent employee/vendors ---

a. Any employees 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.
b. Any Vendors found involved in fraudulent activity will lead to discontinuation of vendor service. Appropriate disciplinary action (includes recovery of damage thus caused) followed by lodging the FIR against such vendors.

Prevention and Mitigation Controls:

1. The IT Department, CISO, Risk Management 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 measure 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.

Exchange of Information and Record Keeping:

Risk Management Department and Audit Department shall maintain centralize database of reported E-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. **Annexure I:**

	Illustrative List of Insurance Fraud
Policyholders/Claims Fraud	**Potential Areas of fraud:** - 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. - 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.

Intermediary Fraud	**Potential areas of Fraud:** - 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.

Internal fraud	**Potential areas of fraud:** - 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.
External fraud	**Potential areas of fraud:** - 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. - Cyber threats leads to manipulation in online transactions.

17. **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)
	Total								

Part II

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

Sr. No.	Description of fraud	No. of cases	Amount involved (Rs. Lakh)
	Total		

Part III

Preventive and corrective steps taken during the year – business segment wise*

Sr. No.	Description of the fraud	Preventive/ corrective action taken

Part IV

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 Involve (rs. Lakh)	No	Amount Involve (rs. Lakh	No	Amount Involve (rs. Lakh	No	Amount Involve (rs. Lakh
	Cases reported to Police								
	Cases reported to CBI								
	Cases reported to other agencies (specify)								
	Total								

*Business segments shall be as indicated under IRDA

(Presentation of financial statements and auditor's report of insurance companies) regulations, 2002.

CERTIFICATION

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

Date: signed/-

Place: Name of Chief Executive Officer of the Insurer

FMR – 2

Fraud cases Closed during the Year

Name of Insurer:

Report for Year Ending:

Sr. no	Basis of Closing a Case	Number of Cases Closed
1	The fraud cases pending with CBI/ Police/Court were finally disposed off	
2	The examination of staff accountability has been completed	
3	The amount involved in the fraud has been recovered or written off	
4	The insurer has received the systems and procedure; identified the causative factors; has plugged the lacunae; and the portion taken note of by appropriate authority of the insurer (Board, Committee thereof)	
5	Insurer is pursuing vigorously with CBI for final disposal of pending fraud cases, staff side action completed. Insurer is vigorously following up with police authorities and/or court for final disposal of fraud cases.	
6	Fraud cases where: The investigation is on or challan/charge sheet not filed in the court for more than three years from the date of filing of first information report (FIR) by the CBI/Police; or Trial in the courts, after filing of charge sheet/ challan by CBI/ police has not started, or is in progress.	

CERTIFICATION

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

Date: signed/-

Place: Name of the Chief Executive Officer of the Insurer