Anti-Fraud Policy

November 2022

Key Policy Information:

Policy reference number	Policy Owner	Policy Approver	Creation date
SHAIC – AFP	Chief Risk Officer	Board	23-Feb-2013

Summary - Version Control:

Version	Reviewed By	Approved By	Revision date	Reason for review
1	Board	Board	2012-13/ February 23 2013	Initial Policy
2	Risk Management Committee	Board	2022-23/ November 09 2022	Periodic review

Table of Contents

1. Introduction

1.1 Background

In accordance with the Insurance Fraud Monitoring Framework, dated January 21, 2013 (hereinafter referred to as "the Framework"), SHAIC is required to have in place an Anti-Fraud Policy (hereinafter referred to as "the Policy"), duly approved by the Board of Directors.

Further, as laid down in the "Guidelines on Insurance e-commerce" dated March 9, 2017, an Insurer is required to have a pro-active fraud detection policy for insurance e-commerce activities, which is to be approved by the Board of Directors.

Also, Corporate Governance Guidelines for Insurance Companies dated May 18, 2016 issued by IRDAI, requires insurance companies for formulation of a Fraud monitoring policy and framework for effective deterrence, prevention, detection and mitigation of frauds.

This Policy has been further devised to ensure that the fraud detection framework is in line with the requirements as laid down under the Framework, as well as it recognizes the principle of proportionality and reflects the nature, scale and complexity of the business of the Company and risks to which it is exposed. The Policy shall also provide guidance with respect to prevention, detection, mitigation and investigation into fraudulent activities.

In order to provide regulatory supervision and guidance on the adequacy of measures taken by insurers to address and manage risk emanating from fraud, the IRDA vide its circular no. IRDA/SDD/MISC/CIR/009/01/2013 dated January 21, 2013 (Circular) laid down the guidelines requiring insurance companies to have in place the Fraud Monitoring Framework. The circular mandates all insurance companies to put in place, as part of their corporate governance structure, a Fraud Monitoring Framework.

Further, to address and manage risks emanating specifically from online e-commerce fraud, IRDAI vide its circular No. IRDA/INT/GDL/ECM/055/03/2017 dated March 9, 2017 laid down the guidelines requiring insurance companies to include Insurance e-commerce in their Fraud Monitoring Framework. The Circular mandates the insurers to have a pro-active fraud detection policy for the insurance e-commerce.

1.2 Objective

Effective deployment of controls which will aid in the identification, detection, prevention and investigations of frauds reported. SHAIC is dedicated to conducting business in a fair and honest manner and will work to eliminate fraud from all activities. SHAIC has a "Zero-Tolerance" stance to fraud and will not tolerate any dishonest or fraudulent behavior on the part of internal or external stakeholders.

This policy covers the following aspects:

- Provide systems and adequate system-based controls to identify proactively potential fraud areas, assess these and provide a framework of people, process, and technology-based controls of processes to prevent fraud
- Ensure that management understands the risk of fraud to the organization and establish a sound control environment through policies, procedures and controls to detect, monitor and mitigate occurrences of finds within various functions of SHAIC that are vulnerable to the fraud risk
- Create ongoing awareness among all stakeholders including employees, clients and other parties having business relation with SHAIC to deter them from indulging in fraudulent activities and measures to be

taken by them in case they suspect any fraudulent activities.

- Provide a set of measures and procedures to respond adequately and quickly to frauds.
- Lay down procedures to report frauds to board, senior management and regulator and exchange of information on fraud and framework for reviewing the procedures from time to time

1.3 Applicability / Scope

This Policy applies to any fraud or suspected fraud involving employees as well as shareholders, consultants, vendors, contractors, outside agencies doing business with SHAIC and/or any other parties having a business relationship with the SHAIC including insurance advisors/ brokers/ corporate agents of SHAIC. The policy would also be applicable to policyholders and beneficiaries. Any investigation activity required will be conducted irrespective of the suspected wrongdoer's length of service, position/title, or relationship to SHAIC.

All employees shall confirm to having read and understood this Policy and not violate any of its provision, on an annual basis, in the form as may be advised by the HR Department.

1.4 Review and approval of the policy

This policy shall be reviewed and approved annually by the Board. Fraud Risk Mitigation Committee (FRMC) shall assist the Board in the review process and recommend necessary changes in the policy. Policy may be reviewed based on the newly released changes to Acts, regulatory requirements, independent audits and/ or internal review.

1.5 Zero Tolerance Policy

SHAIC does not tolerate any unethical or dishonest behaviour, even if the result of the action benefits the SHAIC itself.

Action as deemed fit will be initiated including termination and referring the case to appropriate government authorities.

2. Policy Requirements

2.1 Definition & Introduction

"Fraud" is a wilful act committed by an Individual(s)/Entity(ies) - by deception, suppression, cheating or any other fraudulent or any other illegal means, thereby, causing wrongful gain(s) to self or any other individual(s) and wrongful loss to other(s)/organisation. This includes such acts undertaken to deceive/mislead others leading them to do or prohibiting them from doing a bonafide act or take bonafide decision which is not based on material facts.

Fraud in insurance is an act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties. This may, for example, be achieved by means of:

- Misappropriating assets
- Deliberately misrepresenting, concealing, suppressing, or not disclosing one or more material facts relevant to the financial decision, transaction or perception of SHAIC's status
- Abusing responsibility, a position of trust or a fiduciary relationship.

In order to adequately protect itself from the financial and reputational risks posed by insurance frauds, SHAIC shall have in place appropriate framework to detect, monitor, mitigate and report occurrence of such insurance frauds within SHAIC.

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

2.2 Illustrative List of Frauds

Broadly, the potential areas of fraud include those committed by the officials of SHAIC, SHAIC's agent/corporate agent/intermediary/TPAs and the policyholders/ their nominees. Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

a. **Internal Fraud:** Fraud / misappropriation against the insurer by its Director, Manager and/or any other officer or staff member (by whatever name called)
   i. Misappropriating funds
   ii. Fraudulent financial reporting
   iii. Overriding decline decisions so as to open accounts for family and friends
   iv. Inflating expenses claims/over billing
   v. Paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
   vi. Permitting special prices or privileges to customers, or granting business to favoured suppliers, for kickbacks/favours or misrepresentation of customer
   vii. Forging signatures
   viii. Removing money from customer accounts
   ix. Falsifying documents
   x. Selling SHAIC's assets at below their true value in return for payment.
   xi. Intentional concealment
   xii. Collusion or nexus with concerned stakeholders
   xiii. System Fraud

b. **Policyholder Fraud and Claims Fraud:** Fraud against the insurer in the purchase and/or execution of an insurance product, including fraud at the time of making a claim
   i. Exaggerating damages/loss
   ii. Staging the occurrence of incidents
   iii. Reporting and claiming of fictitious damage/loss
   iv. Medical claims fraud
   v. Fraudulent Death Claim
   vi. Non-Disclosure of Pre-Existing Disease (PED) illness before taking policy
   vii. Suppression of facts
   viii. Duplicate or false claims

Examples of some other important types of frauds:

- Vendor fraud (e.g., Kickbacks including the receipt of excessive gifts or accepting or seeking anything of material value from contractors, vendors or persons providing services/materials);

- Forgery or alteration of documents or accounts belonging to the Company; Concealment or misrepresentation of transactions, assets or liabilities;
- Expense report fraud (e.g., claims for services or goods not actually provided, seeking fake reimbursements);
- Loss of intellectual property (e.g., disclosing confidential and proprietary information to outside parties);
- Conflicts of Interest resulting in actual or exposure to financial loss;
- Embezzlement (e.g. misappropriation of money, securities, supplies, property or other assets);
- Cheque fraud (forgery or alteration of cheques, bank drafts or any other financial instrument);
- Payroll fraud;
- Bribery & corruption (misusing the vested authority to seek personal gains);
- Fraudulent financial reporting (e.g. forging or alteration of accounting documents or records; intentional concealment or mis-statement of transactions resulting in falsification of records or misleading statements;
- Intentional failure to record or disclose significant information accurately or completely
- Improper pricing activity;
- Unauthorized or illegal use of confidential information (e.g. profiteering as a result of insider knowledge of company activities);
- Electronic Fraud and/or illegal hacking, unauthorized or illegal manipulation of information technology networks or operating systems;
- Tax evasion;
- Destruction, removal or inappropriate use of records, furniture, fixtures and equipment of the Company; Sales or assignment of fictitious or misrepresented assets;
- Utilizing company funds for personal purposes.

c. **Intermediary Fraud:** Fraud by Insurance Agents, Brokers, POSP, IMF, Corporate Agents

i. Premium diversion-intermediary takes the premium from the purchaser and does not pass it to SHAIC
ii. Inflates the premium, passing on the correct amount to SHAIC and keeping the difference
iii. Non-disclosure or misrepresentation of the risk to reduce premiums
iv. Commission fraud - insuring non-existent policyholders while paying a first premium to SHAIC, collecting commission and annulling the insurance by ceasing further premium payments.
v. Collusion or nexus with concerned stakeholders
vi. Document Tampering, falsification of records and policy churning by the intermediaries to their advantage

The above list is illustrative and not exhaustive. To protect its e-commerce business, the company will also oversee the adoption of proactive fraud detection measures in conjecture with IRDAI Guidelines on insurance e-commerce (IRDA/ tTNT/ GDU ECM/ 055t O3t 2017) Dtd. 9th March 2017.

2.3 Roles and Responsibilities

2.3.1 Board of Directors

The Board of Directors provide the overall guidance on fraud management and has delegated the responsibilities relating to fraud management activities to the Board Risk Management Committee (BRMC).

The Chief Risk Officer (CRO) independently reports to the board risk management committee. The CRO is supported by the risk, investigation, Vigilance, Internal Audit, underwriting and claims team for performing the fraud management activities of the organization.

Other business leaders such as functional heads should also participate in responsibilities under the organization's anti-fraud strategy as they are directly responsible for overseeing areas of daily operations in which risk might arise as defined under the three lines of defence framework. Such function heads can serve as subject matter experts to assist the Chief Risk Officer with respect to their particular areas of expertise or responsibility.

2.3.2 Board Risk Management Committee (BRMC)

The Board Risk Management Committee (BRMC) is responsible for this policy and will remain, interpret and communicate the policy in the SHAIC. The committee is responsible for the following –

- Monitor implementation of Anti-fraud policy for effective deterrence, prevention, detection and mitigation of frauds.
- The Board of Directors, senior leadership establish the "tone at the top" for ethical behaviour by acting ethically and expressing ethical requirements to employees honestly
- Review the issues identified during entity's fraud risk assessment as well as during internal and external audit
- To ensure the Board of Directors are informed on occurrence of any fraud incident through quarterly reporting process.

2.3.3 Fraud Risk Mitigation Committee

Fraud Risk Mitigation Committee (FMRC) shall be constituted consisting of three senior level officers not below the rank of Sr. GMs headed by the CRO. The committee shall meet at least on a monthly basis to discuss the matters relating to Fraud Prevention and Monitoring also giving a quarterly update to the Risk Mitigation Committee of the Board.

The quorum shall be 2 committee members with CRO being present in person and being the convenor of the committee.

The FRMC is responsible

- Creation and review of the Anti-Fraud policy.
- To design procedures for detecting, reporting, investigating and for taking proper action against the persons committing fraud
- Create awareness among employees, intermediaries, and policyholders to counter insurance frauds
- To initiate and oversee a prompt investigation of any suspected fraudulent act or omission or noncompliance with the policy's requirement
- To ensure that this policy and related guidelines are communicated, updated and made available to all employees and representatives within the SHAIC
- For recovery of loss from the persons committing fraud against the SHAIC
- To ensure that Board of Directors are informed of fraud on occurrence of any fraud incident through periodical reporting process

- Furnish reports on frauds to Authority, as required and an annual submission of the Fraud Monitoring Report (FMR) at the end of each financial year.
- Coordinate with the Internal Audit and Vigilance mechanism in SHAIC to report to the Risk Management Committee and the Board.

2.3.4 Fraud Management Unit (FMU) / Vigilance:

Fraud Management Unit / Vigilance will be responsible for laying down appropriate fraud management processes and procedures in consultation with the CRO, across the Company. It shall report the status of significant cases of fraud detected in the Company to the Fraud Risk Mitigation Committee (FRMC) headed by the CRO at least on a quarterly basis or earlier if required.

Functions of FMU / Vigilance shall include but not be limited to the following:

Identify Potential areas of Fraud: Fraud Management Unit / Vigilance shall proactively try to identify potential areas of fraud. It shall undertake data analytics to find any fraud patterns/trends and subject the same to field/vigilance investigation. Further, it shall also analyse the data based on frauds detected during field/vigilance investigations.

- Fraud Management Unit / Vigilance shall collate all cases of frauds reported by the whistle-blower or any other entities. ·

- Fraud Management Unit / Vigilance shall investigate all such cases and render report to the duly highlighting the breaches of conduct, process and system etc. Report shall also highlight the financial implication, if any. ·

- Fraud Management Unit / Vigilance shall get the cases having involvement of non-related entities reviewed and closed through Head – Fraud Management Unit / CVIO and submit details of such cases to the FRMC.

Disciplinary Action Process: For all proven cases, disciplinary action should be initiated as per the defined disciplinary matrix and should be shared with FRMC for information.

Automation Initiatives: Active participation should be taken by FRMC & FMU in all automation initiatives related to proactive identification & mitigation of frauds.

Fraud Management Unit / Vigilance shall take appropriate steps to share information pertaining to fraud cases amongst all insurers, regulators, government authorities and to establish coordination platforms through the General Insurance Council/Insurance Information Bureau (IIB).

2.3.5 Nodal Officer

a. Appointment of Nodal Officer

- Every Zonal/Area office shall have a Nodal Officer at the level of Manager. Officer-in-Charge not below the level of DGM shall be the Competent Authority to appoint the Nodal Officer for these Offices. In Corporate Office there shall be a Nodal Officer not the below the rank of GM appointed by Executive Director who will act as overall coordinator of the entire organisation.

- Competent Authority concerned will notify the name and designation of link Nodal Officer who will discharge the duties and responsibilities of nodal officer during his/her leave.

b. Responsibility

Nodal Officer(s) shall share the responsibility of prevention and detection of fraud and for implementing the "Anti-Fraud Policy" of the SHAIC. It is the responsibility of all Nodal Officer(s) to ensure that complete mechanism in respect of Fraud Prevention Policy is in place within his/her area of control to:

- Familiarise each employee with the measures to be taken for prevention and detection of fraud.
- Create a whistleblowing culture whereby employees are encouraged to report any fraud or suspected fraud which comes to their knowledge, without any fear of victimization. Promote awareness among the employees of ethical standards.
- Creating awareness among employees / intermediaries / policy holders to counter insurance frauds.
- Coordinating with the Vigilance Dept. to investigate the complaints of fraud and secure necessary documentary evidence
- Liaise with Human Resource Management, marketing, claims Department to take disciplinary action against employees / intermediary under Conduct, Discipline and Appeal (CDA) Rules if they are found to have been involved
- Furnishing various reports on frauds to the Authority as stipulated in this regard and Furnish periodic reports to the Board for its review.
- The Nodal Officer shall implement the modules suggested by the FRMC to create awareness among the employees and officers in fraud detection and mitigation.

2.3.6 Employees

Employees and officers at every level, in every function, at all offices of SHAIC and at all the locations have a responsibility to speak up when they believe that they have knowledge or suspect that fraud is being committed. As soon as it is learnt that a fraud or suspected fraud has taken or is likely to take place, they should immediately apprise the same to the concerned party as per the laid down whistleblowing policy in place.

2.4 Code of Conduct

An organization's code of conduct is one of the most important communications that management should use to communicate to employees on key standards that define acceptable business conduct. The code of conduct should be in place based on below key attributes:

- High-level endorsement from the organization's leadership, underscoring a commitment to integrity
- Simple, concise and positive language that can be readily understood by employees
- Guidelines on each of the SHAIC's major policies or compliance risk areas • Ethical decision-making tools to assist employees in making right choices
- A designation of reporting channels and viable mechanisms that employee can use to report concerns or seek advice without fear of retaliation

2.5 Preventive Mechanism

SHAIC shall inform both potential clients and existing clients about their fraud prevention policies. SHAIC shall take steps to appropriately include necessary caution in the insurance contracts / relevant documents, duly highlighting the

consequences of submitting a false statement and / or incomplete statement, for the benefit of the policyholders, claimants and the beneficiaries. SHAIC shall put up a notice board in every office mentioning the name of the Nodal Officer, phone No. and Official address to enable every person to send intimation about commission of Fraud or suspected Fraud.

In addition, SHAIC shall conduct the following activities:

- Fraud Detection Through data analytics and document review
- Awareness on fraud among existing and prospective customers and identifying/reporting of suspicious activity.
- Investigate the whistle blower complaints, if any, received from time to time
- Establish a strong fraud risk & control assessment
- 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 SHAIC, in order to clearly communicate expectations for ethical behaviour to staff members

2.6 Procedure for Fraud Monitoring

Internal Audit and Inspection Department and Vigilance Department operating in the organizational set up will have the primary responsibility to identify, detect, and report insurance frauds. While the Audit and Inspection Dept. will monitor fraudulent activities during their exercise, the Vigilance Department will carry out the exercise during their surprise inspection of offices from time to time.

SHAIC will have well defined procedures to identify, detect, investigate and report frauds. The risk management, fraud monitoring department and Information technology will develop/ manage systems and framework and analytical tool methodologies to identify potential fraud areas/ red flags.

2.7 Identification and reporting of frauds

Employees shall promptly communicate any concerns about unethical behaviour and report any actual or suspected incident of fraud or violations of the company policies on a confidential basis.

SHAIC 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:

- sharingsecret@starhealth.in
- risksupport@starhealth.in
- whistleblower@starhealth.in
- The Chief Compliance Officer
- The Chief Risk Officer
- The Chief Human Resources Officer
- The Head of Internal Audit
- The Chief Executive Officer
- The Chairperson of the Audit Committee
- Another Manager or Supervisor
- Other touch points defined in the company policies

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

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

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

Address: Chairman, Audit Committee, Star Health and Allied Insurance Co Ltd, No.1, New Tank Street, Valluvar Kottam High Road, Nungambakkam, Chennai- 600034

Email: chairmanacb@starhealth.in

Any employee who suspects dishonest or fraudulent activity shall notify the above mentioned parties immediately, and should not attempt to personally conduct investigations or interviews/ interrogations related to any suspected fraudulent act. It is the responsibility of the Authorities to ensure that concern is duly investigated with full confidentiality, in fair and transparent manner and the concern is duly addressed.

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

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

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

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

2.8 Framework for exchange of information

SHAIC will ensure exchange of necessary information on frauds, amongst all insurers through the General insurance council.

2.9 Due Diligence

SHAIC will ensure that pre-employment verification is done before appointing persons for every job. Similarly, steps will be taken to ascertain the antecedents of insurance agent/corporate agent/intermediary/TPAs before appointment/agreements with them.

2.10 Regular Communication Channels

Risk Management, Fraud Monitoring Unit, HR, Vigilance, any other function who is involved in identification of a fraud to generate fraud mitigation communication within SHAIC at periodic intervals or on ADHOC basis, as may be required. It must also ensure information flow to concerned departments with respect to frauds.

2.11 Confidentiality

All fraud investigation and related information will be treated confidentially. Investigation results will not be disclosed or discussed with anyone other than those who have a valid business need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct.

2.12 Security to Individuals

SHAIC strongly encourages individual to report fraudulent activity. Any employee of SHAIC making a report in good faith, can do so in the knowledge and confidence that the Board of Directors / senior management of SHAIC will ensure that the act will not lead to the employee facing any recrimination, punishment or victimization.

However, any abuse of this protection (e.g. any false or bogus allegation made by an individual knowing them to be false or bogus or with a mala fide intention) will warrant action as deemed necessary by SHAIC.

2.13 Fraud Investigation Procedure

Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way. The fraud investigation shall consist of gathering sufficient information about specific details and performing those procedures that are necessary to determine whether fraud has occurred, the loss or exposures associated with the fraud, who was involved in it and the fraud scheme.

The members of the Fraud Investigation Team shall comply with Fraud investigation procedure manual at all times.

In performing their duties under this Policy, the members of the Fraud Investigation Team should 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.

2.14 Co-ordination with Law Enforcement Agencies

Whenever an allegation of fraud of grave nature is prima facie found to be true, efforts will be taken to file a complaint with police authorizes for initiating action under criminal law of the land.

SHAIC may coordinate with Various law enforcement agencies for fraud reporting on timely and expeditious basis and follow-up processes thereon. Reporting to CBI/Police and other law enforcement agency will be done on case-to-case basis or as per requirement raised by any government authority

2.15 Disciplinary Measures

Based on the investigation findings, staff and intermediary accountability and complicity disciplinary measures will be decided. Efforts will be made to recover the loss amount fully. Based on the nature of the fraud, an internal committee may decide on suitable penal action as per the grid (disciplinary action matrix) defined or pursue the matter with other law enforcement agencies for appropriate action against the concerned person(s). An employee, intermediary and agent shall be subject to disciplinary action, including the termination of their employment, if the employee fails to cooperate in an investigation, or deliberately provides false information during an investigation.

2.16 Loss monitoring and recovery

SHAIC shall keep a track of all losses to be recovered from the fraudsters and monitor the same periodically.

2.17 Fraud Awareness

Making employees aware of their obligations concerning fraud prevention controls begins with practical communication and training in formulating training and communications plan, management should consider developing fraud initiatives that are

- Comprehensive and based upon job functions and risk areas
- Integrated with other training efforts, whenever possible
- Regular and frequent, covering the relevant employee / intermediaries population

In particular, the functions identified as potential business areas of fraud should get initial and ongoing training on fraud matters. Training can help to raise staff awareness of the risk of fraud and the importance of compliance with internal control procedures and security checks to prevent such frauds Additionally, close monitoring of staff / intermediary compliance with these controls helps ensure their consistent application.

There should be communication to both potential clients and existing clients about SHAIC's anti-fraud policies. Proposal form and Policy document will need to be included with cautionary statements / specific disclaimers highlighting the consequences of submitting a false statement as part of Governance based fraud prevention controls.

FMU, Vigilance Team and Risk management team to share awareness communications on periodic basis with motive to spread awareness among employees at all level about new emerging risks, insurance frauds and ways of preventing fraud.

3. Reporting

3.1 Internal Reporting

Nodal Officer in every Zone/Area Office shall provide a list of cases of fraud occurring in their jurisdiction on monthly basis to the Nodal Officer in Corporate Office. Marketing, HR and Claims Team to report any fraud identified to the risk and investigation team as and when observed. The information received from all the offices will be collated by the Nodal Officer and this will be shared with all other Nodal Officers.

Besides, this information will be passed on to the Training Dept. for dissemination in Training sessions conducted for employees including Agents. Audit and Inspection Dept. as well as Vigilance Dept. will be given this information to be used during their routine exercises.

3.2 External Reporting

SHAIC shall furnish the statistics on various fraudulent cases which come to light and action taken thereon shall be filed with the Authority in forms FMR 1 and FMR 2 providing details of

i. Outstanding fraud cases; and
ii. Closed fraud cases

Within 30 days of the close of every financial year.

4. Appendices

4.1 Related policies and procedures

This policy should be read in conjunction with the following Policies and Procedures:

- Anti-Money Laundering Policy
- Whistle-blower Policy
- Enterprise Risk Management (ERM) Policy
- Disciplinary Action matrix

4.2 Annexures

Annexure 1: Illustrative List of function wise frauds

1. Marketing & Communication

a. Intentional misrepresentation of product features or making false claims for selling a product on social media or press media
b. Intentional circulation of obsolete products brochures resulting in damage to the reputation of SHAIC
c. Unauthorised usage of SHAIC name / logo to gain undue benefits
d. Circulation of inflated financial analytics of SHAIC deliberately
e. Intentionally posting Sensitive / Confidential information on social media or press media resulting in reputational / financial loss to the organization

2. Administration

a. Employee steals assets including cash from SHAIC, either by physically taking it or diverting it in some other way leading to inventory shrinkage
b. Vendor Fraud includes employee colluding with others to process false claims for benefits or payments or intentional non-disclosure of conflict of interest during empanelment of vendor.
c. Employee colludes with the vendor and provides information about SHAIC's budget of procuring an asset or pricing quoted by other vendors for kickbacks from the vendor
d. Employee intentionally submits inflated expense claims, false reimbursement claims, forged receipt for reimbursement or claims the expenses multiple times against same bill.
e. Procurement fraud includes over-ordering of assets and selling them below their true value for personal gains
f. Employee uses SHAIC’s assets in an unauthorized manner for personal gains.

3. Finance

a. Employee creates fictitious vendor account or manipulates the account of an existing vendor for generating false payments for personal gain
b. Employee forges signature on the cheque or alters the payee details, amount or other details mentioned on the cheque or creates an unauthorized cheque for personal gain.
c. Employee submits and/or approves fake/tampered food bills, vendor bills, hotel bills, travel bills, to gain monetary benefits.

4. Human Resource

a. Hiring an employee without proper credential check, criminal/dubious background and employment records verification

b. Payroll employee creates a fake employee in payroll records and diverts the salary in his own account Ex-employee is intentionally kept active on the payroll and salary payable is diverted to another account for personal gain.
c. Salary is intentionally transferred to matching or duplicate salary bank accounts of an employee for kickbacks Falsification of entries in attendance record resulting in inflated salary processing
d. Marking attendance in the system for self-whilst the employee is absent from duty or marking attendance in the system for another employee, whether the other employee is on duty or absent from duty
e. Allowing another person to mark attendance on behalf of an employee, whether the employee allowing is on duty or absent from duty
f. Dual employment
g. Hiring relatives leading to conflicts of interest or otherwise not in accordance with HR Policy of SHAIC (including contractual employees)
h. Onboarding a vendor without proper background check and documents verification

5. Information Technology

a. Employee intentionally shares confidential information pertaining to SHAIC or its customers or its employees to the third party.
b. Employee steals or intentionally shares client list, account numbers, personal information with another person.
c. Not disabling email/system access of inactive employees resulting in unauthorized usage by others
d. Employees fraudulently breaking IT rules built to safeguard the data systems

6. Legal & Compliance

a. Seek kickbacks / favours for not initiating Governance Action or for lower severity punishment
b. Suppress evidences to avoid Governance action

7. Operations

a. Overriding actual decision in family / friend's policies at issue at standard rate (otherwise would have been over-rated or declined/postponed)
b. Approving fraudulent claims by suppressing actual reports for monetary gain
c. Cancelling & refunding policy premium post FLC period without following due approval process resulting in substantial premium loss
d. Misappropriation of office cash or misuse of cheques or any other payment instrument
e. Tampering office documents to conceal any operational fraud done by an employee
f. Manipulation of bank account details for misappropriation of funds
g. Misuse of credit cards, debit cards or net banking or any other online payment methods for misappropriation of funds
h. Any other fraud within the operation function

8. Sales Function

a. Misappropriation of customer money
b. Forging signatures in documents
c. Misrepresentation of critical details of customers KYC documents of customers misused or tampered

d. Recruiting relatives as direct reportee under them without disclosing relationships
e. Impersonating like customer in Verification calls or any other call done by SHAIC to the Customer
f. Giving false Agents' Confidential Reports or Moral Hazard Report hiding the financial or health status of the life assured, including physical existence of the life assured
g. Tampering any document including Proposal form, Benefits illustration, payment instruments, Age proof, KYC documents with the intention of defrauding SHAIC
h. Colluding with the Medical Centre and arranging for medical examination reports without the life assured not undergoing medical examination
i. False certification of copies of documents
j. Fraudulent or unauthorised usage of SHAIC's letterhead & logo
k. Delay in deposit of premium remitted by the Policyholder, to SHAIC

4.3 List of applicable regulations

Date of issuance	Ref. No	Name of Legislation
02-04-2002	F.No. IRDA/REG/03/2002	IRDAI (Preparation of Financial Statements and Auditors Report of Insurance Companies) Regulations, 2002
21-01-2013	No.IRDA/SDD/MISC/CIR/009/01/2013	Insurance Fraud Monitoring Framework
18-05-2016	IRDA/F&A/GDL/CG/100/05/2016	Corporate Governance Guidelines for Insurance Companies
09-03-2017	IRDA/INT/GDL/ECM/055/03/2017	Guidelines on Insurance e-commerce