SHRIRAM Life Insurance

IN PARTNERSHIP WITH Sanlam

ANTI FRAUD POLICY

CONTROL SHEET

Reviewer	Approver	Approval Date
Risk Management Department	Board	20-05-2020
Risk Management Department	Board	19-05-2021
Risk Management Department	Board	18-05-2022
Risk Management Department	Board	12-05-2023
Risk Management Department	Board	23-05-2024

Table of Contents

1. Background

Financial Fraud poses a serious risk to all segments of the financial sector. Fraud in the insurance industry reduces consumer and shareholder confidence and can affect the reputation of individual insurers and the insurance sector as a whole. It also has the potential to impact economic stability. It is, therefore, required that Shriram Life Insurance Company Limited ("Company") understand the nature and impact of fraud and take preventive steps to minimize the vulnerability of the Company's operations to fraud risk.

Insurance Regulatory and Development Authority of India (IRDAI) vide IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025, dated 09 October 2025 IRDAI/IID/GDL/MISC/112/10/2025 have provided the regulatory framework on measures to be undertaken by insurers to manage risks emanating from frauds which includes developing an Anti-Fraud Policy.

With the above stated objectives of fraud risk management, the Company's "Anti-Fraud Policy" referred to as "Policy" lays down the Company's approach towards fraud prevention, detection, investigation, correction and reporting of frauds. This shall help the Company to mitigate frauds as well as handle such frauds appropriately.

2. Purpose

The purpose of this Policy is to:

- Establish the Company's approach to combating Fraud in line with applicable laws and regulations
- Define scope and identify potential areas of Fraud
- Lay down high level procedures for preventing, detecting, investigating, monitoring and reporting frauds
- Set forth roles and responsibilities of Board of Directors, Key Management Persons, each of the functions and the employees.

3. Definition, Scope and Classification of Fraud

Fraud may be defined as an act of omission or commission or connivance or any other act intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties including but not limited to the following:

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

The Policy shall equally apply to all employees of the Company including its Key Management Persons and the Board of Directors as well as stakeholders who conduct business with the company, such as third party agents, representatives, brokers, consultants, contractors, suppliers, Vendors, subcontractors, partners, agents and other business parties with whom the Company has a business relationship.

Frauds can be broadly classified into:

(a) Policy Holder and/ or Claims Fraud – Fraud involving any person(s), in obtaining coverage or payment during the purchase, servicing, or claim of an insurance policy.

Such fraud includes but is not limited to -

- Intentional non-disclosure or misrepresentation of material information pertaining to client
- Misrepresentation of material information
- Fraudulent death claims
- Falsification or fabrication of client documents such as age, KYC, income proofs
- Making false allegations for cancellation policies with intent to get refund of premiums
- Exaggerating damage / loss
- Medical Claim Fraud

(b) Distribution channel Fraud – Fraud perpetrated by an insurance agent/ Corporate Agent/ Intermediary.

Such fraud includes but is not limited to –

- Misappropriation of policyholder or claimant monies
- Intentional non-disclosure or misrepresentation of material information pertaining to client including medical condition of client at time of policy purchase or claim
- Falsification or fabrication or forgery of client documents such as Proposal forms, age proof, KYC, income proofs or any other document
- Collecting premium into own account, submitting unrelated third party premium instruments against customer application
- Inducing Policyholders to cancel policies with intent to earn undue profiteering through commission
- Involvement in submission of fraudulent proposals/ claims such as those on non-existent, dead persons
- Inflation of premium with intent to retain differential after deposit of actual premium amount
- Misselling or misrepresentation or non-disclosure of the product features, benefits or making false promises or offering any form of rebates for purchasing insurance policy or for retention or payment of renewal premium, (Any rebates on premiums for high sum assured etc. per the Product documents of the insurance company are allowed)

(c) Internal Fraud – Fraud/ Misappropriation against the Company by its Directors, Officers and employees

Such frauds include but are not limited to –

- Intentional non-disclosure or misrepresentation of education or past employment information or past salaries or any other information relevant for considering the candidature for appointment and submission of false or fabricated documents relating to consideration of candidate's appointment
- Frauds listed under "Intermediary Fraud" as applicable to sales employees
- Misappropriation of Company, policyholder, intermediary funds
- Fraudulent financial accounting or reporting
- Inflated or fraudulent expense claims
- Violation of Company Policy to approve policies/ claims for family and friends
- Submission of false (or inflated) invoices prepared directly
- Permitting special prices or privileges to customers or suppliers who are family and friends or in return for kickbacks/ non-monetary favours
- Signature forgery or falsification of Company documents
- Misappropriation of Company Assets during employment or at the time of exit
- Theft and/ or misuse of Company's Intellectual Property, customer sensitive data, Company confidential information

(d) External fraud – External fraud is defined as any fraud involving external parties, service providers and vendors

(e) Affinity Fraud or Complex Fraud: Fraud involving collusion among one or more fraud perpetrators in the above categories.

(f) Cyber or New Age fraud - in order to prevent Cyber or New Age fraud, the Company shall *inter alia*, establish and implement robust cybersecurity framework to protect against evolving cyber frauds or threats. Further, the Company continuously monitor and strengthen systems and processes for fraud risk management, such as incident databases, customer verification, and access control. Fraud monitoring unit may utilise services of an expert with relevant risk and technological expertise to evaluate and advise on cyber fraud risks across various insurance business lines. Alternatively, the fraud monitoring unit may in consultation with Chief Information Security Officer ensure controls to prevent Cyber frauds, including website resilience, access controls, identity management and other information security controls to prevent such frauds are in place and perform a Cyber fraud risk assessment as a part of the Annual Fraud risk assessment

4. Cost and Impact of Fraud

The impact of fraud is not restricted to loss of the Company's assets but extend to its image and that of its employees. The impact includes:

- Financial Loss
- Impact on net profit
- Quality of project delivery
- Quality of services rendered
- Customer Satisfaction
- Employee morale
- Company reputation
- Stakeholders' relations
- Employee remuneration, e.g. bonuses, increases and incentives
- Cost of combating fraud and cost of insurance against fraud.
- Negative Media / Publicity

5. Roles and Responsibilities

The following section highlights the roles and responsibilities of the Company's Board of Directors, Key Management Persons , Risk Management Unit and all employees:

5.1 Board of Directors ('Board')

The Board shall ensure that the management of the Company designs an effective fraud risk management program.

The Company's Board, shall:

- Approve the Company's Anti-Fraud Policy and any revisions made to it from time to time.
- Review the Policy on at least an annual basis and at such intervals as it may consider necessary.

5.2 Risk Management Department Committee

The Risk Management Committee shall be responsible for effective implementation and oversight of the fraud risk management framework.

In particular, the Risk Management Committee shall:

- Formulate Fraud monitoring policy and framework for approval by the Board
- Monitor implementation of Anti-fraud policy for effective deterrence, prevention, detection and mitigation of frauds
- Review compliance with the Insurance Fraud Monitoring Framework issued by the Authority relating to risks.

5.3 Risk Management Function

Risk Management Function shall oversee all types of risks, including Fraud risks. Any reports submitted to the Risk Management Committee shall be reviewed by the Risk Management Department and confirmed for submission to the Risk Management Committee.

5.4 Fraud Monitoring Committee

A Fraud Monitoring Committee shall be established by the Company with the following responsibilities:

- operationalizing the Fraud risk management framework within the insurer and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying
- regularly conduct monitoring activities and update, based on experiences, appropriate measures on fraud risk management to various functions, including advising on potential threats, fraud risk and remedial action
- oversee prompt responses to instances or suspicions of fraud
- maintain all relevant details pertaining to each instance of fraud
- 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
- co-ordinate with law enforcement agencies for reporting frauds on a timely basis
- conduct an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines and activities for fraud, using past experiences, emerging trends & Red Flag Indicators (RFIs), etc.
- identify areas for improvement and adaptation of the Fraud Risk Management Framework
- submit quarterly reports to the Risk Management Committee on its activities, findings, and recommendations including the financial impact of fraud on the insurer
- submit report of the Annual Comprehensive Fraud Risk Assessment before the Board of Directors through Risk Management Committee
- report to the Audit Committee, in addition to the Risk Management Committee, in case of all internal frauds
- establish and administer procedures and mechanisms to receive reports from internal or external sources regarding potential unethical or inappropriate events, behavior or practices, as well as any potential breach of Company's policies, or laws and regulations.
- oversee and/or execute investigations and determine corrective actions as warranted by matters reported by employees and stakeholders.
- seek necessary internal or external advice when dealing with issues of suspected fraud cases as necessary and provide specific consideration and oversight related to exposure to fraudulent activities.
- provide necessary reports to Management, Board and Regulator on fraud cases received and actions taken to manage fraud risks.
- create awareness on ways to counter fraud among the employees / policy holders at regular intervals.
- Fraud Monitoring Committee shall be headed by a Key Management Person and include senior representatives from relevant departments, such as

underwriting, claims, legal or any other department as deemed necessary.

- Fraud Monitoring Committee may form subcommittees, as required, for its effective functioning.

5.5 Fraud Monitoring Unit

A Fraud Monitoring Unit comprising of suitable employees with relevant experience in areas such as fraud detection, fraud prevention, fraud risk management etc., shall be formed to continuously monitoring the Company's exposure to fraud risks. The Fraud monitoring unit shall be independent of Internal audit and shall assist the Fraud Monitoring Committee.

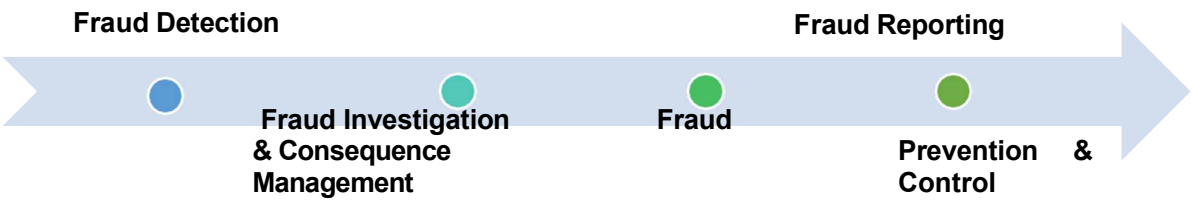
5.6 Employees

All employees are responsible for assisting the Company in safeguarding its funds and other assets, as well as protecting its reputation and business from matters involving fraud, corruption and misconduct.

All levels of employees shall:

- Have a basic understanding of fraud and be aware of red flags pertaining to their areas
- Attend Training Sessions/undergo Training modules on Fraud detection, prevention and mitigation conducted by the Company from time to time
- Participate in the process of creating a strong control environment and understand how they can prevent, detect, monitor and eliminate fraud and other irregularities
- Understand how and when fraudulent acts can occur or go undetected.
- Read and understand Company policies and procedures, especially those designed to ensure compliance with ethical business practices and mitigate/identify fraud risks.
- As a first line of defence, identify, report, monitor and mitigate and the fraud risks pertaining to their respective areas of operations
- Conduct periodic Fraud risk assessments as per the guidance provided by the Fraud Monitoring Unit including rating of risks, identification of actionables to mitigate the risk and getting the risk management registers containing the risks, ratings and mitigants reviewed and agreed by the Fraud Monitoring Unit. If any advice is provided by the Fraud Monitoring Unit on any of the risk register items, to accept, evaluate, discuss and jointly agree with Fraud Monitoring Unit on the advice provided. Any disagreement between the the Functional Head and the Fraud Monitoring Unit on the identification, risk assessment and rating, risk mitigations required, residual risks, shall be escalated by the Fraud Monitoring Unit to the Fraud Monitoring Committee, whose decision will be final on such matters
- Report unethical or inappropriate events, behavior or practices, as well as any potential breach of Company's policies, or laws and regulations to the Human Resources, Fraud Control Unit or members of the Disciplinary Committee.
- Cooperate in investigations and subsequent disciplinary actions or reporting to law enforcement authorities. This includes providing necessary access to Company's records and premises.
- Take responsibility for ensuring that agents, partners, vendors and service providers of the Company adhere to the standards and principles of this Policy.

6. Fraud Management Procedures



6.1 Fraud Detection

Fraud Detection is the identification of an actual or potential fraud. Frauds may be detected through various onsite inspections of processes, employees, documents or early warning signals.

All Functional Heads are primarily responsible for day-to-day management of activities and in charge of maintaining, implementing and improving their Systems & Controls so that they minimise the risk of frauds.

6.1.1 Department–wise Anti-Fraud Procedures

All the business functions are required to have in place procedures and controls that are in compliance with the policy and the line managers are entrusted with the primary responsibility to enforce its adherence in the normal course of business.

Function-wise anti-fraud procedures are required to be embedded into processes Examples of anti-fraud procedures are given below:

- Segregation of duties
- System access controls – access rights restricted as per job responsibilities
- Maker –Checker concept
- Delegation of authority matrix

6.1.2 "Red Flags" / Offsite Monitoring – Offsite monitoring does not seem to be relevant

The Company conducts series of proactive monitoring of processes and transactions across various functions in order to detect potential frauds or negative trends through identification of red flags, i.e. suspicious or unexplained or strange trends patterns or transactions with no rationale or indicators of a potential fraud based on lines of business, activities, past trends, monitoring vendor activities etc. Examples of areas that may be monitored are premium payment through serial cheques, Customer non-contactibility and Policies undelivered higher lapsation especially significant drop 13th month persistency, higher customer complaints in distribution channels, locations, product etc., and higher incidence of claims in specific pockets, with some patterns, i.e. same location, same kind of occupation or higher incidence of repudiation of claims pointing to possible claim frauds , Policy splitting and replacements indicating possible misguidance to Customers, AML transaction monitoring and identification of red flags like frequent freelook cancellations, employee expense claim trends indicating potential false reimbursement claims, sharing of confidential data by employees with unauthorized persons, with some fraudulent intent.

6.1.3 Whistle Blower Policy

The Company has a Whistle Blower Policy to ensure that whistle blower can report suspected unethical or illegal behavior or practices for investigation and necessary action while protecting whistle blowers from acts of retaliation.
Whistle Blower must report suspected unethical or illegal behavior including concerns relating to possible irregularities, governance weaknesses, financial reporting issues or other such matters as per reporting mechanism detailed out in the Whistle Blower Policy. Requests for anonymity will be respected. In cases where an internal or external whistleblower reports a matter to any employee, he/ she is obliged to immediately report such matter as per reporting mechanism detailed out in the Whistle Blower Policy.

6.1.4 Internal and External Audits

Internal and External Audits and inspections play a vital role in detecting and deterring frauds. Auditors may conduct proactive checks to search for frauds not limited to misappropriation of assets, and financial statement fraud. This may include the use of computer-assisted and analytical procedures to isolate anomalies and performing detailed reviews of high-risk accounts and transactions.

6.1.5 External Sources

Complaints regarding malpractice and fraud may include those made by external parties not limited to customers, distributors and agents, vendors and service providers or those routed through regulatory bodies and law enforcement agencies.

6.1.6 Customer Complaints

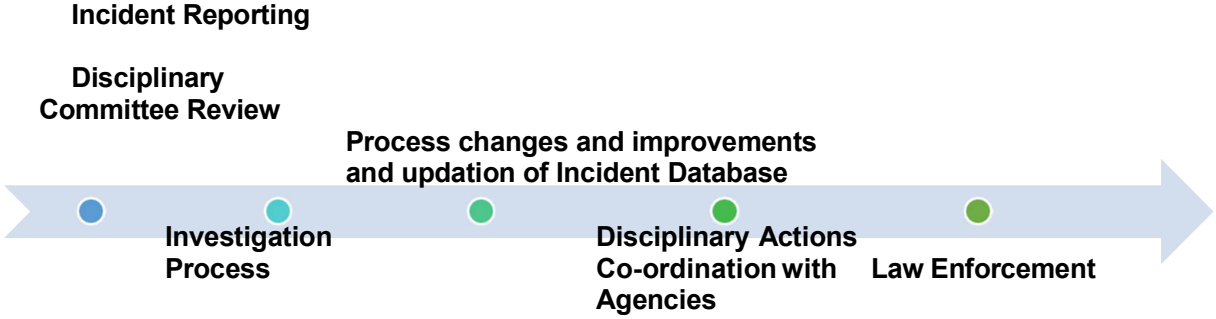
Customer or claimant complaints alleging fraud by employees, agents, distributors or any external party will be escalated to the Fraud Control Unit by Internal teams not limited to Customer Service, Claims and Renewals.

6.1.7 Insurance Fraud Repository

Insurance Fraud Repository is an industry-wide Fraud Analytics system developed under the guidance of Life Insurance Council/Insurance Information Bureau ("IIB"). The Company shall participate in the Fraud Monitoring Technology Framework, as applicable to its businesses, made available by the IIB, to help the industry to combat fraud and protect policyholders and all stakeholders. The Company shall provide such information to the IIB as required by them, on details of distribution channels, hospitals, third party vendors and fraud perpetrators blacklisted by the Company.The repository would be a key tool in identification of fraud by scrubbing the data at underwriting and claims stage through the database of fraud committed across the industry. The fraud repository will act as a key fraud monitoring framework. This will be the mechanism through which cooperation amongst market participants (defined under clause 3 (e) of E - Commerce guidelines) to identify frauds shall be established.

Besides the Company shall also maintain the Incident Database of persons committing fraud/attempted fraud containing the names and other details of persons against whom frauds have been proven. This list shall be referred to by the concerned functions (HR/Sales HR/Hiring Teams) before hiring any employee/Agent and decisions to hire or otherwise shall be taken accordingly.

6.2 Fraud Investigation Process



6.2.1 Incident Reporting:

In case of any incident of fraud / possible attempt of fraud against the Company the person reporting shall communicate the incident/possible attempts of fraud to: Fraud Monitoring Unit, Ramky Selenium, Plot No. 31 & 32, Beside Union Bank Training Centre, Financial District, Gachibowli, Hyderabad-500032.
Email: incident@shriramlife.in (this email ID should be monitored by Fraud Monitoring Unit)

6.2.2 Investigation Process:

The Fraud Monitoring Unit will review relevant information relating to the report/ complaint and conduct detailed investigations with all related internal and external parties to collect evidence and establish the facts of the case.

During the investigation all employees and associates related to the case or that are interviewed would be required to maintain confidentiality of the proceedings and provide information completely and accurately. The investigations team may request written reports or statements from those involved in the case.

The Fraud Monitoring Unit may seek advice and assistance from internal or external teams such as Legal, Internal Audit, Human Resources, Investigation and Verification agencies, Law enforcement agencies, as required.

The final case findings will be collated and documented and conclusions drawn based on evidences and documented into an Investigation Report. The report will include a summary of the sequence of events, factual findings, reference to various documents such as External Investigation Reports including Forensic Reports, if any, witness submissions etc. as evidence, reference to the Company's policies that have been violated

The report may also contain observations on training needs, process gaps or lapses and recommend training re-enforcement, process improvements or changes.

6.2.3 Disciplinary Action Committee Review

The Company has established a Disciplinary Action Committee ("Committee") shall based on the Investigation Report and supporting documents submitted by the Fraud Monitoring Unit decide on the disciplinary actions to be taken against employees and intermediaries. The members of the Disciplinary Action Committee shall include – Chief Risk Officer, Head – HR, CFO, Head Compliance & Head Governance. Quorum for Disciplinary Action Committee shall be three. If any of the member is conflicted with reference to any case, he/she shall recuse himself/herself from participating in the proceedings or decision of the case involving conflict

The Committee, will decide the disciplinary action(s) after reviewing and discussing the report. The Committee will evaluate each instance of misconduct considering the facts and circumstances of the incident(s). While determining disciplinary actions it may take into account relevant considerations such as prior or similar misconduct at the Company, length of experience at the Company of the person against whom charges are framed and nature and severity of the violation/act/omission. The decisions of the Committee will be final and documented.

If the Company has any appellate authority over decisions of the Committee, the provisions relating to appeals needs to be mentioned here. If there is no appellate authority, please forget this comment.

The range of disciplinary actions includes, but is not limited to, warning and training, compensation adjustments including withholding sales incentives, probation, suspensions, and termination of employment. In addition, conduct leading to disciplinary actions by the Company may serve as the basis for disqualifying the employees and associates from Conferences and other recognition programs.

The Committee may also recommend training re-enforcement, process improvements or changes, where applicable.

The Company retains the sole discretion to evaluate violations of Company policy and to determine appropriate disciplinary action.

6.2.4 Disciplinary Actions

As per the decision of the Committee, the Fraud Monitoring Unit will communicate actions to relevant functions for implementation.

Human Resources function will issue applicable letters of warning, probation, probation extension, recoveries, suspensions, termination of employment to employees.

Disciplinary actions involving employees will be communicated to the concerned employee(s) by his/ her/ their management and/ or Human Resources. Human Resources will coordinate any related administrative operations follow-up and implementation and intimate the Fraud Monitoring Unit for its records.
In case of disciplinary action against agents, Distribution Operations will perform the necessary administrative tasks for execution of the Disciplinary action decided by the Disciplinary Action Committee.

6.2.5 Co-ordination with Law Enforcement Authorities

Where misconduct may require disclosure or complaint to regulatory or law enforcement authorities, the Company retains the authority to make such disclosures or seek the support of authorities, as it believes appropriate. Such authorities include but are not limited to Police, Economic Offences Wing (EOW), Central Bureau of Investigation (CBI) and IRDAI.

The Fraud Monitoring Unit will consult or seek assistance from the Legal Team while submitting or following-up on such disclosure and complaints. A copy of all disclosures and complaints will be retained by the Department.

6.2.6 Process Gaps & Change recommendation

The Fraud Monitoring Unit will communicate to relevant functions, any training re-enforcement, process improvements or changes that are recommended by the Committee in order to strengthen controls and prevent possible recurrence of fraud or misconduct. The Key Management person to whom the Function management reports is expected to ensure implementation of the recommendations after due evaluation.

6.3 Fraud Reporting

6.3.1 Internal Reporting

The Fraud Monitoring function will on at least a quarterly basis, share Fraud reports and dashboards with internal management and stakeholders.

The summary of the trends, findings and control activities shall be updated to

the Board and Risk Management Committee on a quarterly basis.

6.3.2 External Reporting

The Company will submit annual statistics on fraudulent cases which come to light and action taken thereon, to IRDAI in formats stipulated by the regulator and at an ongoing frequency the Fraud database will be updated in the Insurance Fraud Repository as and when required.

The details provided will include:

- Outstanding/unresolved fraud cases
- Closed fraud cases
- Preventive/corrective actions taken thereafter
- Cases reported to the Law enforcement agencies

6.4 Fraud Prevention and Controls

The Company's management is responsible for establishing procedures and controls for preventing frauds and safeguarding assets of the Company. Fraud Prevention encompasses an ethical environment, training and re-enforcement, periodic fraud risk assessments and preventive internal control such as authority limits, system and manual checks. A strong tone at the top along with preventive controls and effective processes serve as strong and effective deterrents for fraud.

6.4.1 Fraud Risk Assessment:

Fraud Risk Assessments will be conducted on a periodic basis for all key functions of the Company to assess inherent fraud risks, evaluate adequacy of existing controls and determine counter measures to mitigate risks. The controls may be audited or tested from time to time for high severity risks.

6.4.2 Training & Awareness:

The Company and its management will ensure that its Distribution channels, employees, including the senior management, Board of Directors and associates undergo training on ethical conduct and fraud awareness. The objective of such training will be familiarize personnel with the Anti-Fraud Policy, raise awareness of what constitutes fraud, how to prevent, detect and report frauds.

{ End of the Document }