Fraud Prevention Policy

June 2026

Public

Contents

1 Introduction

1.1 Background

In accordance with the IRDAI Guidelines, Ref. IRDAI/IID/GDL/MISC/112/10/2025 on Insurance Fraud Monitoring Framework, dated October 9, 2025 (hereinafter referred to as “the Framework”) and Master Circular on Corporate Governance for Insurers, dated May 22, 2024, SBI Life Insurance (hereinafter referred to as “the Company”) is required to have in place a Fraud Prevention Policy (Anti-Fraud Policy)(hereinafter referred to as “the Policy”), duly approved by the Board of Directors.

The Company recognizes the need to establish effective mechanisms for the prevention, detection, mitigation, reporting, and investigation of fraud across its operations. Accordingly, this Policy establishes a framework for the prevention, detection, mitigation, reporting, and investigation of fraud, in line with applicable regulatory requirements. It is based on the principle of proportionality, considering the nature, scale, and risk profile of the Company’s operations, and also addresses fraud risks arising from digital and e-commerce activities.

Further, any regulations/guidelines issued from the regulator and or other entities from time to time shall be adhered to. The Policy shall be reviewed periodically and updated as necessary to ensure continued alignment with regulatory changes and emerging risks from time to time.

1.2 Objective

The objective of this Policy is to establish a comprehensive framework to deter, prevent, detect, monitor, mitigate and report insurance fraud within the Company. The Policy aims to enhance the Company’s resilience against fraud, promote fraud awareness, foster a culture of integrity, protect policyholders’ interests, safeguard financial stability, and maintain public trust.

The Company adopts a “Zero-Tolerance” approach towards fraud and will not accept any dishonest or fraudulent act committed by employees, stakeholders, or any parties associated with the Company.

1.3 Applicability

This Policy applies to all employees, shareholders, vendors, contractors, consultants, distribution channels (insurance advisors, brokers, corporate agents etc.), reinsurers policyholders, beneficiaries, and any other parties having a business relationship with the company.

It covers any fraud or suspected fraud, and investigations will be conducted regardless of the individual’s role, position, tenure, or relationship with the Company.

1.4 Review and approval of the policy

The policy will be reviewed by Board Risk Management Committee and will be recommended to the Board of Directors for approval, at least annually or as and when required.

2 Policy Requirements

2.1 Roles and Responsibilities

- Board of Directors – The Board is responsible for approving, reviewing and monitoring compliance with the Policy at least annually and the Risk Management Committee (RMC) shall be responsible for effective implementation and oversight of the fraud risk management framework.
- Fraud Monitoring Committee – Fraud Monitoring Committee (FMC) shall be responsible for operationalizing the Fraud risk management framework.
- Fraud Monitoring Unit – Fraud Monitoring Unit (FMU) shall support FMC in discharging its functions.
- First Line of Defence – Primary responsibility for the implementation and practice of fraud risk management, including core risk management principles of risk identification, measurement, management, monitoring & reporting rests with the first line of defence i.e. the concerned process owner / business / line function.
- Second Line of Defence – The Compliance and Risk functions are the second line of defence, who are responsible for reviewing and challenging the completeness and accuracy of the first line's risk identification, measurement, management, monitoring and reporting.
- Third Line of Defence – Audit is the third line of defence. Audit is responsible for independent assessment on the effectiveness of the fraud controls framework design and operations and is also responsible for reporting findings and concerns to the Management and the Company's Audit and Risk Committees.

Detailed roles and responsibility of various stakeholders is detailed in the Company's Fraud Response and Monitoring Procedures.

2.2 Fraud Monitoring Committee

The Fraud Monitoring Committee (FMC) shall be responsible for operationalizing the Fraud Risk Management Framework and overseeing the activities, as appropriate to ensure effective fraud deterrence, prevention, detection, reporting, and remediation. The FMC shall,

a. recommend and regularly update, based on experiences, appropriate measures on fraud risk management to various functions.
b. oversee prompt responses to instances or suspicions of fraud and maintain all relevant details pertaining to each instance of fraud
c. 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.
d. 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. and identify areas for improvement and adaptation of the Fraud Risk Management Framework.

The composition of the Fraud Monitoring Committee is detailed in Appendix – Section (6.3)

2.3 Fraud Monitoring Unit

The Fraud Monitoring Unit (FMU), shall support FMC in discharging its functions and effective implementation of the measures suggested by FMC

The Company shall ensure availability of appropriate and adequate resources to the Fraud Monitoring Unit

Fraud Monitoring Unit shall generate fraud mitigation communication within the Company at periodic intervals or on adhoc basis, as may be required. It must also ensure information flow to concerned departments for effective fraud risk management.

2.4 Procedures for Fraud Risk Identification, Mitigation and Monitoring

The Company shall establish and maintain a robust framework to identify, assess, mitigate, monitor, and report fraud risks across all lines of business and operations.

The Company has detailed Fraud Response and Monitoring Procedures outlining the approach to handle confirmed or suspected frauds involving employees, intermediaries, vendors, policyholders, or any other stakeholders, whether internal or external.

a. Fraud risks shall be identified and assessed based on business lines, activities, past experience, emerging trends and applicable regulatory guidance. Appropriate preventive, detective and corrective controls shall be implemented to mitigate identified fraud risks across all processes.
b. The Company shall clearly define responsibilities and establish a delegation of authority for all relevant functions, including identified sensitive posts, to ensure accountability and effective control over fraud risk management.
c. Functional Heads shall be responsible for maintaining, implementing, and strengthening systems, processes, and controls within their respective areas, as well as for conducting due diligence on the various entities or individuals such as personnel, distribution channels, TPAs, vendors, and consultants with whom the Company engages, before entering into agreements or appointments, to minimize the occurrence of fraud and mitigate its impact in a timely manner.
d. Red Flag Indicator (RFI) shall mean a warning sign that may indicate potential fraud. The Company shall define, embed RFIs within relevant operational and analytical processes which will be periodically reviewed for continued relevance and effectiveness.
e. Employees and other stakeholders shall report suspected or detected frauds promptly through the incident reporting mechanism.
f. Centralized investigation of suspected frauds shall be undertaken, with cases being analysed, documented and escalated to the appropriate authority for

disciplinary, recovery and/or legal action, within appropriate timelines as applicable.

g. The Company shall maintain effective monitoring and review mechanisms, including fraud incident databases, fraud sensitive audits, trend analysis of distribution channels, continuous vendor monitoring and review of customer grievances to detect and prevent fraud.

h. The company shall monitor recovery of fraud related losses and undertake continuous improvement initiatives, including review of missed detection opportunities and fraud awareness programs, to promote a culture of zero tolerance to fraud.

i. The Company shall ensure confidentiality of fraud investigations, provide protection to individuals who report fraud in good faith, and take appropriate action in cases of non-reporting or malicious complaints and against the fraudsters.

j. The Company also has an established Whistle-blower Policy to safeguard individuals reporting fraudulent activity while protecting the interests of the organization.

k. The Company shall coordinate with law enforcement agencies for timely fraud reporting and follow-up. Reporting to relevant agencies will be done on a case-to case basis.

2.5 Cyber or New Age Fraud

Cyber or new age frauds are defined as any fraud carried out using digital or new age technologies. The Company shall prevent such frauds by implementing a robust cybersecurity framework, continuously monitoring and strengthening systems and processes for Fraud Risk Management across all functions.

The Company shall utilize a team with relevant risk and technological expertise to manage cyber fraud risk.

2.6 Insurance Information Bureau (IIB)

The Company shall participate in the IIB Fraud Monitoring Technology Framework, share required fraud related data including blacklisted distribution channels, hospitals, vendors and fraud perpetrators, as appropriate. The Company shall report as per the prescribed format within timelines prescribed by IIB and utilize industry wide threat intelligence to prevent frauds.

2.7 Framework for Reinsurance business

The company shall manage fraud risk in reinsurance business and ensure compliance with applicable regulatory requirements and our internal fraud risk framework, wherever relevant, thereby maintaining governance and integrity standards.

2.8 Distribution Channels

Distribution Channels shall include insurance agents, intermediaries or insurance intermediaries, and any persons or entities authorized by the Authority to be involved in the sale and service of insurance policies. The Company shall establish a comprehensive fraud risk management for all distribution channels, including intermediaries, to ensure that they put in place policies, procedures and controls to prevent, detect, report and remedy frauds, incorporate red flag indicators, provide employee training, conduct due diligence, establish internal reporting for investigation procedures, maintain whistleblower mechanisms.

Distribution Channels shall comply with their respective regulatory framework, coordinate with law enforcement agencies for reporting and follow up and promptly inform the Company of any suspected frauds along with the relevant details.

2.9 Training, Education and Awareness

The Company will conduct regular fraud awareness programs for policyholders, the public, employees, senior management including board members, and distribution channels to educate them on fraud risks, prevention, and reporting. Periodic training and communications will reinforce understanding of fraud schemes and promote a culture of vigilance and zero tolerance, supporting the Company's overall fraud risk management framework.

3 Exception handling

Any exception with respect to the Policy shall be reviewed by the Board. The exception request shall be submitted to the Fraud Monitoring Committee in the form of a Note addressing the Risk Management Committee with complete description of the said exception.

4 Reporting

4.1 Internal Reporting:

- The Fraud Monitoring Committee (FMC) will submit quarterly reports to the Risk Management Committee (RMC) on its activities, findings, and recommendations, including the financial impact of fraud.
- The FMC will present the Annual Comprehensive Fraud Risk Assessment to the Board of Directors through the RMC.
- All internal fraud cases will be reported to the Audit Committee, in addition to the RMC, to ensure timely escalation and action.

4.2 External Reporting:

- The Company will report all incidents of fraud to law enforcement and other relevant agencies, as per applicable laws.
- Annual returns shall be filed with the Authority in the prescribed format (FMR-1)

within 30 days of the close of the financial year.

- In the event of fraud involving distribution channels registered with IRDAI, the Company will promptly escalate and report the matter to IRDAI without delay.

In addition to the above, the Company shall adhere to any other requirements / directions for reporting of frauds as may be issued by IRDAI or any other regulators from time to time.

5 Record keeping

All fraud related information / documents shall be preserved for a period as specified in the applicable regulations and internal policies.

6 Appendices

6.1 Definition of Fraud

Fraud in Insurance shall mean an act or omission intended to gain advantage through dishonest or unlawful means, for a party committing the fraud or for other related parties, including but not limited to:

- Misappropriating funds;
- Deliberately misrepresenting/ concealing/ not disclosing one or more material facts relevant to any decision, transaction, financial or otherwise.
- Abusing responsibility, a position of trust or a fiduciary relationship

6.2 Classification of Fraud:

- **Internal Fraud** – Fraud involving internal staff, including employees and/or senior management
- **Distribution Channel Fraud** – Fraud involving distribution channels.
- **Policyholder fraud and/or Claims fraud** – Fraud involving any person(s), in obtaining coverage or payment during the purchase, servicing, or claim of an insurance policy.
- **External Fraud** – Fraud involving external parties' / service providers / vendors etc.
- **Affinity Fraud or Complex Fraud** – Fraud involving collusion among one or more fraud perpetrators in the above categories.

6.3 Composition of Fraud Monitoring Committee

The Fraud Monitoring Committee (FMC) shall assist the Risk Management Committee of Executives (RMC-E), and the relevant issues shall subsequently be put up to the Risk Management Committee of the Board (RMC-B).

The committee will be constituted of the following members:

a) President and Chief Risk Officer
b) President-Operations & IT
c) President & Chief Distribution Officer
d) President & Chief Financial Officer
e) President- Business Strategy
f) EVP & Chief of HR & Management Services
g) Chief Operating Officer
h) Legal Officer - Business Operations
i) Compliance Officer
j) SVP & Head - Risk Management & Fraud Monitoring

Any other personnel as may be required on invitation basis. Fraud Monitoring Committee shall be chaired by President & CRO.

Head - Risk Management and Fraud Monitoring will be the convener of the meetings of the Committee and the committee will have a quorum of 4 members.

The Fraud Monitoring Committee meetings shall be held quarterly or whenever a specific case with important implications has to be discussed.

6.4 Related Policies and Procedures

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

- Anti-Money Laundering Policy;
- Whistle-blower Policy;
- Risk Management Policy;
- Sales and Process Quality Code of Conduct
- Fraud Response and Monitoring Procedures
- Information and Cyber Security Policy

6.5 List of Abbreviations used in the policy

- CBI - Central Bureau of Investigation
- IRDAI - Insurance Regulatory and Development Authority of India
- RMC-E - Risk Management Committee of Executives
- SQ & CFIC - Sales Quality and Complaints & Fraud Investigation Cell
- TPA - Third-Party Administrator
- RFI - Red Flag Indicator
- FMC - Fraud Monitoring Committee
- FMU - Fraud Monitoring Unit