AXIS MAX LIFE INSURANCE

AXIS MAX LIFE INSURANCE LIMITED

ANTI-FRAUD POLICY

Policy Version	2.3
Effective Date	1st April 2026
Policy Owner Department	Fraud Monitoring Unit - FMU
Prepared by	Anurag Parashar Head - Fraud Monitoring Unit
Approved by	Sanjeev Kr. Sood Head - Chief Assurance Executive

Table of Contents

S.no	Section	Page
1	Introduction	3
2	Purpose & Intent	4
3	Definitions	4
3.1	Classification of Frauds	5
4	Fraud Risk Management Framework	5
4.1	Deterrence and Prevention	8
4.2	Detection	9
4.3	Reporting	10
4.4	Remedying	11
4.5	Investigation	11
4.6	Fraud Monitoring Committee (FMC)	12
5	Reporting to Law Enforcement Agencies/ Authority	13
6	Framework for exchange of information	14
7	Failure to comply with the Anti-Fraud Policy	14
8	Communication and Administration	14
Appendix 1	Illustrative list of frauds	14
Appendix 2	Composition of FMC	16
Appendix 3	Closure of Fraud Cases	17

1. Introduction

Axis Max Life Insurance Limited ("Axis Max Life" or "Company") is committed to transparency, integrity and accountability in all its affairs. It is determined to maintain a culture of honesty and strong opposition to Fraud (hereinafter defined) and corruption.

Like any other organization of significant size and complexity, the Company is vulnerable to risks of Fraud and corruption and as such, in accordance with the principle of proportionality, has dedicated adequate resources and priority to combat the same.

The above objective is reinforced through this Axis Max Life's Anti-Fraud Policy ("**Policy**"). The Policy aims to enhance the Company's resilience against Fraud, foster a culture of integrity, protect policyholders' interests, safeguard financial stability and maintain public trust. The Policy also outlines the procedures in relation to its five key Fraud pillars, namely:

- Deterrence;
- Prevention;
- Detection;
- Reporting; and
- Remedying.

The Policy will be administered through a dedicated Fraud Monitoring Unit ("FMU") which shall be headed by the Head, Fraud Monitoring Unit. The FMU shall operate independently from Internal Audit Function and shall remain clearly segregated to preserve functional independence. The FMU and Internal Audit may report administratively into the Chief Assurance Executive or any other functional head, subject to compliance with applicable law. The Management Risk Committee (MRC /RMC) of the Company shall be responsible for effective implementation and oversight of the fraud risk management framework. The FMU shall have appropriate escalation mechanisms and direct access to the Fraud Monitoring Committee (FMC), Audit Committee, senior management, and the MRC, as required, to ensure objectivity, transparency, and regulatory compliance.

The Policy is in compliance with IRDAI (Insurance Fraud Monitoring Framework), Guidelines, 2025 ("Guidelines") and is effective from 1st April 2026.

This Policy shall be read in conjunction with the Company's HR and Compliance policies, including:

- Business Code of Conduct;
- Conflict of Interest Policy;
- Employee Background Verification Policy;
- Whistleblower Policy;
- Anti- Bribery & Anti-Corruption Policy; and
- Information and Cyber Security Policy.

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.

2. Purpose & Intent

The Policy has been formulated to:

- Establish a comprehensive framework for dealing with Fraud risks effectively.
- Develop amongst the employees and other stakeholders (including its Distribution Channels, vendors or other business partners of the Company), the understanding of Fraud and its implications and effects on the Company.
- Create awareness with respect to Fraud and spread a culture in the Company to prevent the occurrence of Fraud.
- Send across a message within the Company and to the public at large that Fraud is not acceptable and shall not be tolerated.
- Ensure that the employees including senior management of the Company are aware of their roles and responsibilities for the deterrence, prevention, detection, reporting and remedying of Fraud and for implementing procedures thereof.
- Provide a mechanism to report any actual/ suspected incident of Fraud.
- Define the action to be taken by the Company when any actual or suspected fraudulent activity occurs.
- Adequately protect the organization from the financial and reputational risks posed by Insurance Frauds;
- Put in place the framework to identify, assess & minimize the risk of Fraud thereby protecting and further strengthening of customers as well as shareholder's confidence.
- Define responsibilities, delegation of authorities for all relevant functions including for identified sensitive posts.
- Put in place the Fraud investigation process, including internal turnaround times from identification to remedy, designated officer(s) for reporting incidents of Fraud and report submission.
- Put in place the mechanism for appropriate action in case of non-compliance to the Fraud risk management framework and against the Fraud perpetrators.
- Putting a due diligence procedures for staff recruitment and vendor engagement
- To review process to identify "missed" insurance Fraud detection opportunities

3. Definitions

A. As per section 447 of Companies Act 2013, explanation of "Fraud" is as below:

(i) **"**Fraud" in relation to affairs of a company or anybody corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or

to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss;

(ii) "Wrongful gain" means the gain by unlawful means of property to which the person gaining is not legally entitled;

(iii) "Wrongful loss" means the loss by unlawful means of property to which the person losing is legally entitled.

B. As per the Guidelines:

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

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

ii. "Red Flag Indicator" or "RFI" means a possible warning sign, that points to a potential Fraud and may require further investigation or analysis of a fact, event, statement, or claim, either alone or with other indicators;

iii. "Cyber or New Age/ E-commerce Fraud" means any insurance Fraud carried out using digital or new age technologies;

iv. "Distribution Channels" shall include insurance agents, intermediaries or insurance intermediaries, and any persons or entities authorized by the Authority to involve in sale and service of insurance policies. ;

v. "IRDAI"/ "Authority" shall mean Insurance Regulatory and Development Authority of India.

3.1 Classification of Frauds

The Company shall establish appropriate systems and processes across its functions to deter, prevent, detect, report and remedy Frauds; and report such Frauds in accordance according to the following categories:

- 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.

An illustrative list of Frauds is attached as Appendix 1 to this Policy.

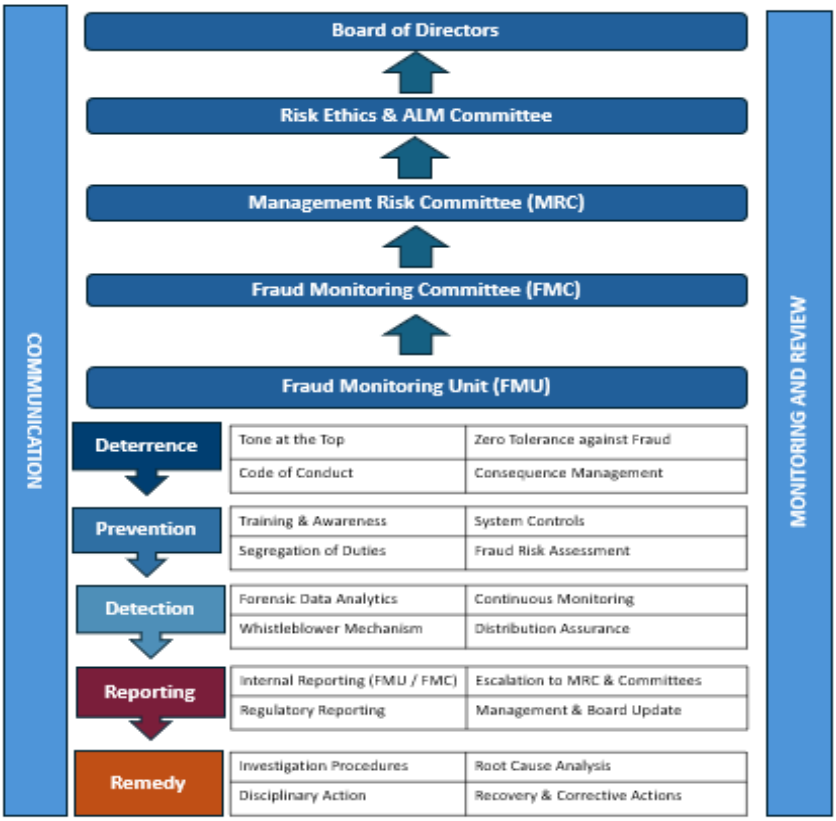
4. Fraud Risk Management Framework

In response to the growing threat of Fraud and vulnerability due to significant size of its operations and the nature of business, the Company has for zero tolerance for Fraud and accordingly has put in place a comprehensive Fraud Risk Management Framework. The Company's Fraud Risk Management Framework is structured around the five core principles prescribed under the Guidelines, namely: deterrence, prevention, detection, reporting, and remedying Fraud. This framework recognizes Fraud risk as part of the key risks and provides for its periodic review by the management and also by the various review committees such as Fraud Monitoring Committee, Management Risk Committee, Risk, Ethics and Asset Liability Management Committee (REALMC) and the Board, as applicable. However, the management holds primary responsibility including its applicability, monitoring, reporting and implementing corrective measures.

The policies, procedures, systems, governance mechanisms, and accountability structures are designed to collectively ensure effective implementation of each of these principles across the Company.

The framework further provides for dedicated processes and teams of specialists embedded within a dedicated FMU. The Company shall assign appropriate and adequate resources to FMU to carry out its functions effectively.

The following diagram shows the Company's Fraud Risk Management Framework:



The FMU is responsible for effective implementation of the Policy and shall inter alia also be responsible for the following:

- Putting in place appropriate measures to identify and assess Fraud risks;
- RFIs shall be reviewed regularly for their continued relevance and effectiveness in detecting Fraud;
- Laying down procedures for internal reporting from/and to various departments;
- Creating awareness among employees/ Distribution Channels /policyholders/partners to counter Insurance Frauds;
- Furnishing various reports on Frauds to the Authority as stipulated in this regard;
- Conduct an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines and activities for Fraud, using past experiences, emerging trends RFIs, etc.
- Perform investigations with respect to financial and non-financial Frauds e.g. mis-selling, suspicious claims, mortality frauds, information security breaches, behavioral and misconduct related issues etc.
- Design and implement forensic enabled Early Warning Systems (EWS) and RFIs to proactively identify potential fraudulent incidents across business processes;
- 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
- Identify positions, roles, and functions that are exposed to heightened Fraud risk ("Sensitive Positions") based on access to customer funds, systems, data, decision-making authority or override powers. Enhanced controls for such positions shall include, as applicable, segregation of duties, maker–checker mechanisms, periodic role rotation, mandatory leave, heightened supervision, access controls, and independent reviews. The identification of Sensitive Positions and related controls shall be reviewed periodically by management and overseen by the FMC;
- Define, document and maintain RFIs for identification and early detection of Fraud risks across underwriting, claims, Distribution Channels, vendors, employees, and information systems. RFIs shall be embedded within operational processes, analytics tools, and surveillance mechanisms and shall be reviewed periodically, and at least annually, for their continued relevance and effectiveness. The FMC shall oversee the adequacy, review and enhancement of RFIs based on Fraud trends, emerging risks, regulatory advisories, and learnings from internal and industry-wide Fraud cases.
- Furnishing periodic reports to the board of Directors and various committees for their review.

In order to discharge its responsibilities of companywide monitoring and reporting of Frauds, the Fraud Monitoring Unit (FMU) works closely with:

- Claims: Claims team assesses the need for investigation basis the defined parameters and guidelines for reported claims. The suspected claims are assigned for investigation to FMU and based on incriminating evidence so procured, fraudulent claims are recommended for repudiation to the Claims team.
- Information Security Unit (Cyber or New Age/ Ecommerce Fraud): This team is responsible for driving implementation and reviewing Information Security processes within ISO 27001

Framework. Incidents, involving information security breaches, are investigated by Information Security Unit. Repeated incidents and incidents of significant nature are assigned to FMU.

- Underwriting Risk Management Unit (URMU): URMU forms part of the Underwriting function and aims to mitigate the underwriting and operational Fraud risk at the time of policy issuance. The unit identifies exceptional/ suspicious cases through back-end analytics and for suspicious transactions performs further checks including field verifications.
- Human Resources (HR): HR team provides necessary inputs and support for investigation of any Fraud or misconduct involving employees and also for finalizing the disciplinary action against the established cases of Fraud or misconduct.

A brief snapshot on the key activities under the Fraud Risk Management Framework is provided below:

4.1 Deterrence and Prevention

The Company shall implement appropriate measures for monitoring and review of Fraud risks, including maintaining an Incident Database of persons convicted of or attempting Fraud, conducting fraud-sensitive audits for compliance with the Fraud Risk Monitoring Framework, tracking business trends from Distribution Channels, continuously monitoring vendor activities for compliance with Fraud prevention measures and contractual obligations, and analyzing customer grievances and complaints to detect and prevent Fraud.

Prevention of Fraud involves identifying the cause of an integral Fraud risk by means of risk assessment and implementing effective controls to stop Fraud before it happens. The organization invests considerable efforts into prevention/ mitigation measures such as:

4.1.1 Training and Awareness

a. Training- Training on internal controls, Fraud detection and prevention is conducted by FMU at periodic intervals so as to cover all employees once a year. Advisories on emerging Fraud risks are published by FMU based on learning derived from emerging Fraud issues on at least annual basis.

   Training on compliance and regulatory framework (including Anti Money Laundering "AML") is done by Compliance function for employees and by the training team for agents to cover employees/agents and to Distribution Channels on Fraud risk management once a year.

b. Awareness - The Company will conduct regular Fraud awareness programs to educate policyholders and the general public about the risk of Fraud and how to prevent and protect against it.

the policyholders will also be informed about the Policy, necessary cautions are to be included in insurance contracts/ relevant documents, highlighting the consequences of submitting a false statement and/ or incomplete statement.

Distribution Channels (other than insurance agents and POSP) shall independently maintain Fraud risk management frameworks as per IRDAI requirements. Distribution Channels (insurance agents and POSP) shall be required to comply with the Policy, procedures and controls, whenever there is a suspicion of Fraud which may also impact the Company, the same shall be informed to the Insurer providing all relevant details.

4.1.2. Due Diligence

Due Diligence is a process of verifying the background and credentials of the personnel (management and staff) / Insurance agent / Corporate Agent / Intermediary / Vendors. The Company has laid down the broad procedures below for conducting due diligence:

- Employees (Management and Staff): Employee background verification is conducted by Human Resources by checking the background (professional and educational) of the new hires.
- Insurance Agents and POSPs: Agent and POSPs background verification is conducted through reference checks and Know Your Customer (KYC) checks by Distribution Service Delivery Operations (DSDO) before their appointment.
- Distribution Channels (other than insurance agents and POSP) : Due Diligence for Distribution Channels will be conducted by Compliance before entering into agreements with them.
- Vendors: Due Diligence for vendors will be conducted by Procurement as per the Procurement Policy before entering into agreements with them in accordance with the applicable sourcing/governance processes as notified by the Company from time to time. In addition, Compliance shall do the due-diligence for the vendors which come under the category of outsourcing.

4.1.3. Fraud Risk Assessment (FRA)

FRA identifies and recognizes Fraud risks in the organization, determines their likelihood and how to prevent and mitigate the Fraud risks proactively. Including identifying potential vulnerabilities across business lines and activities for Fraud, using past experiences, emerging trends & RFIs, etc.

4.1.4. 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.
- continuously monitor and strengthen systems and processes for Fraud risk management, such as incident databases, customer verification, and access control.
- utilize a team with relevant risk and technological expertise to manage cyber Fraud risks across various insurance business lines.
- Incidents of Cyber or New-Age Fraud having material impact shall also be reported in accordance with regulatory reporting obligations and included in the annual Fraud return.

4.2 Detection

Fraud detection is the identification of actual or potential Fraud. It relies upon the implementation of appropriate systems and processes to get early warning signs of Fraud.

Fraud identification and detection includes a combination of the following techniques:

4.2.1 The primary responsibility for detection and Fraud Prevention set up lies with the functional heads. Further Department wise anti-fraud procedures are embedded into processes such as:

- Segregation of duties;
- Inbuilt maker-checker controls;
- System access controls – access rights restricted as per job responsibilities;
- Quality checks;
- Scrutiny of application / proposal forms; and
- Delegation of authority matrix.

4.2.2 Customer Complaint Management System – Centralized system for logging and tracking policyholder grievances (received through letters, online, on call or email) for monitoring market conduct issues etc.

4.2.3 Whistleblower Policy: This policy aims to provide employees an avenue to anonymously raise concerns regarding any Fraud or misconduct including violation of Business Code of Conduct, Conflict of Interest and instances of non-compliance to policies and procedures, laws and regulations. Any employee who discovers or suspects fraudulent activity ("Concern") must raise it via modes and in the manner as described in Whistleblower Policy for appropriate action.

4.2.4 Offsite Monitoring /Surveillance: Under the Fraud Risk Management Framework, data-mining procedures using analytical techniques on an ad-hoc, repetitive or continuous basis are part of the surveillance conducted. It is particularly useful for analyzing operational and transactional information to highlight anomalies or identify Fraud 'red-flags' such as unusual or suspicious gaps (examples – cheques being issued by agents, signature mismatch cases in multiple policies, impersonation by sellers to receive fraudulent customer payouts, etc.). Information derived from data mining is acted upon and reviewed by FMU. Mystery shopping as a tool is proactively used to identify and detect Frauds. The list above is illustrative only, not exhaustive.

4.3 Reporting

Reporting ensures that suspected or confirmed Fraud incidents are formally captured, escalated, and disclosed to the appropriate internal and external stakeholders.

- Fraud Reporting Platform (Whistleblower): The Fraud reporting platform provides a safe, confidential, and anonymous channel for employees, agents, and third parties to report suspected Fraud or unethical behavior.
- Internal Reporting: Internal Reporting ensures that identified Fraud cases are promptly escalated within the Company to designated governance bodies.

- Regulatory Reporting: Regulatory reporting ensures compliance with statutory and regulatory obligations related to Fraud, AML, and misconduct.

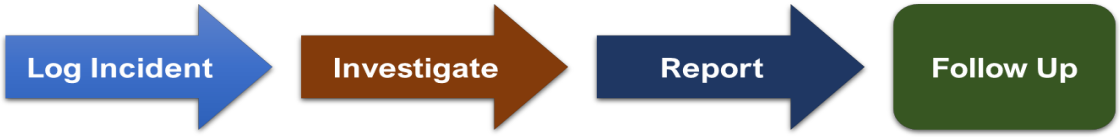
4.4 Remedying

Remedying focuses on corrective actions after Fraud is detected, including recovery, disciplinary action, system strengthening, and prevention of recurrence.

- System Capabilities: System enhancements are used to correct weaknesses exposed by Fraud incidents.
- Forensic Data Analytics: Forensic analytics help quantify impact, trace transactions, and identify linked Fraud cases.
- Distribution Assurance: Distribution assurance focuses on addressing Fraud originating from agents, intermediaries, or third-party channels.
- Dedicated Investigation Procedures: Formal investigation procedures ensure fair, structured, and legally sound handling of Fraud cases.

4.5 Investigation

Investigations shall be undertaken independently, objectively, and professionally in a manner that preserves confidentiality and in accordance with laws and regulations. Investigation includes performing root cause analysis through identifying the point of control failure along with necessary corrective and preventive actions and follow-up for recovery of Fraud losses wherever applicable. Brief process is as follows:



Investigation Unit of the FMU is responsible to ensure;

- Utmost confidentiality is maintained of the person reporting the incident in good faith.
- Information relating to investigation is shared strictly on 'legitimate need to know' basis.
- Reported cases are investigated within least possible time and reports issued accordingly.
- To abstain from any conflict of interest in accordance with 'conflict of interest' policy of the Company.
- To follow defined TATs as per standard operating process as updated from time to time.

Members of the Investigating Unit are empowered to:

- Have free and unrestricted access to the Company's records and premises, whether owned or rented.
- Obtain full co-operation from any employee or associate of the organization.

- Obtain written and / or oral statements from people they may deem fit, provided such enquiries are under the scope of current investigation.
- Examine, copy, and / or seize/ obtain all or any portion of the contents of files, desks, cabinets, and other storage facilities including personal items linked to the Fraud on the premises without prior knowledge or consent of any individual who may use or have custody of any such items or facilities when it is within the scope of their investigation.

All the relevant evidences obtained during the course of investigation must be preserved as the same may be required to support legal proceedings.

Where legally required by law enforcement and regulatory bodies or government agencies, Management is to ensure that all cases of Fraud or malpractice are adequately reported.

4.5.1 Coordination with law enforcement Agencies

Coordination with law-enforcement agencies will be done as per the investigation procedure, including the reporting of Frauds on timely and expeditious basis and follow-up process thereon. Decisions, as to the timing of the involvement of the Police or Legal Advisors, will vary on a case-by-case basis.

The recovery of monies lost due to Fraud should be actively pursued using available legal means where appropriate.

4.6 Fraud Monitoring Committee (FMC)

Fraud Monitoring Committee ('the Committee') shall be responsible for operationalizing the Fraud Risk Management Framework within the Company and oversee activities, as appropriate, to ensure Fraud deterrence, prevention, detection, reporting and remedying. FMU will support FMC in discharging its functions and effective implementation of measures suggested by FMC.

4.6.1 Composition of the FMC

The Committee of the Company shall be headed by a Key Management Personnel (KMP) and shall include senior representatives from relevant departments, such as underwriting, claims, legal or any other departments as deemed necessary. The current composition of FMC is attached as Appendix 2 to this Policy. The Committee will be chaired by Chief Financial Officer (CFO). FMC may form subcommittees, as required, for its effective functioning. FMC shall avoid conflicts of interest in its composition and functioning.

In addition to the above, the Committee may include other members of the Company's senior management as members or as invitees. In case of any change in designation or resignation of any member/invitee, the person handling the stated portfolio/position shall be considered to be a member or invitee.

4.6.2 Roles and Functions of FMC

(i) Recommend and regularly update, based on experiences, appropriate measures on fraud risk management to various functions.
(ii) Oversee prompt responses to instances or suspicions of Fraud
(iii) Maintain all relevant details pertaining to each instance of Fraud
(iv) 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.
(v) 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.
(vi) Identify areas for improvement and adaptation of the Fraud Risk Management Framework.
(vii) The FMC shall periodically review instances where Frauds were detected belatedly or where opportunities for earlier detection were missed. Such reviews shall aim to identify control gaps, process weaknesses, or system limitations and recommend corrective measures, including enhancements to controls, RFIs, monitoring tools, and awareness programs.

4.6.3 Frequency & Quorum of Meeting

- FMC shall convene on a quarterly basis and shall discuss the matters tabled by FMU.
- The quorum for FMC shall be a minimum of 3 members, including the Chairperson.

4.6.4 FMC Reporting

The FMC shall interalia:

a) submit quarterly reports to the Risk Ethics and ALM Committee (REALMC) of the Board on its activities, findings, and recommendations including the financial impact of Fraud on the Company.
b) submit report of the Annual Comprehensive Fraud Risk Assessment before the Board of Directors through REALMC.
c) report to the Audit Committee, in addition to the REALMC, in case of all internal Frauds.

5. Reporting to Law Enforcement Agencies/ Authority

i. The Company shall report incidents of Fraud to Law Enforcement Agencies and/or other relevant agencies/authorities subject to applicable laws.
ii. The Company shall within 30 days of closing of the financial year file annual returns with Authority in the formats as may be issued by the Authority from time to time.
iii. In the event of Fraud committed by Distribution Channels, the Company shall promptly escalate and report the matter to IRDAI without delay.

iv. For reporting purposes, only in the instances of Fraud cases as may be specified in Appendix 3 will be considered as closed.

6. Framework for exchange of information

i. In order to ensure that the data available with insurers is effectively utilized to prevent Frauds, 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.
ii. the Company shall share to IIB the details of Distribution Channels, hospitals, third party vendors and Fraud perpetrators blacklisted and IIB shall maintain the caution repository concerning all such details in order to safeguard the integrity of the insurance sector by preventing the involvement of those with a record of fraudulent activities.

7. Failure to comply with the Policy

The Company expects all its employees, Distribution Channels (only insurance agents and POSP) to act in full compliance with this Policy. The failure to comply with this Policy will result in appropriate disciplinary actions, up to and including termination, including further legal and regulatory actions against the individuals involved as may be required as per the Employee Disciplinary Action policy (E-DAP)/ Agent Disciplinary Action policy (A-DAP) and according to local laws and regulations. Further, for cases where Fraud is established, criminal proceedings in consultation with the legal function will be initiated which may be punishable with fine, imprisonment, or both. Employees of the Company/ Distribution Channels would be responsible to make good the financial loss to the Company caused by their fraudulent actions.

8. Communication and Administration

The Policy will be communicated to all stakeholders, including employees, vendors, Distribution Channels (only insurance agents and POSP), and policyholders. It is the responsibility of the process owners to inform their relevant staff, including vendors about the stipulations on Fraud detection, classification, monitoring and reporting as per the Policy.

The Policy will be reviewed periodically, at least on annual basis, and presented to the Board for its approval.

Appendix 1 – Illustrative list of Frauds

As per the Guidelines, broadly, the potential areas of Fraud include amongst others those committed by the officials of the Company, Distribution Channels and the policyholders/ their nominees. Some examples of fraudulent activities or triggers, include but are not limited to the following:

1. Internal Fraud:

- Misappropriating funds
- Fraudulent financial reporting
- Stealing cheques
- Overriding decline decisions so as to open accounts for family and friends
- Inflating expenses claims/over billing
- Paying false (or inflated) invoices, either selfprepared or obtained through collusion wit h suppliers
- Permitting special prices or privileges to customers, or granting business to favoured su ppliers, for kickbacks/favours
- Forging signatures
- Removing money from customer accounts
- Falsifying documents
- Selling insurer's assets at below their true value in return for payment.

2 Policyholder and Claims Fraud:

- Exaggerating damages/loss
- Staging the occurrence of incidents
- Reporting and claiming of fictitious damage/loss
- Medical claims Fraud
- Fraudulent death claims

3 Distribution Channel Fraud:

- Premium diversion-
  intermediary takes the premium from the purchaser and does not pass it to the insurer
- Inflates the premium, passing on the correct amount to the insurer and keeping the diff erence
- Non-disclosure or misrepresentation of the risk to reduce premiums
- Commission Fraud ensuring nonexistent policyholders while paying a first premium to t he insurer, collecting commission and annulling the insurance by ceasing further premi um payments.

4. External Fraud: Fraud involving external parties' / service providers / vendors etc.

- creating fake website of Company
- doing fake collections in the name of Company
- running fake job scams in name of Company
- fake sales in name of Company

- social engineering with an intent to commit Fraud
- deduping customer/ general public in the name of Company

5. Affinity Fraud or Complex Fraud: Fraud involving collusion among one or more Fraud perpetrators in the above categories.

- Community Investment Scam
- Multi-Layer Vendor and Invoice Manipulation
- Nexus Frauds

Appendix 2 – Composition of FMC

Sl. No	Designation	Role in FMC
1	Chief Finance Officer	Chairperson
2	Chief Assurance Executive	Member
3	Chief Underwriter	Member
4	Head of Operations	Member
5	Chief Compliance Officer	Member
6	Head Legal	Member
7	Chief Information Security Officer	Member
8	Head, HR Operations	Member
9	Head, Enterprise Center of Excellence	Member
10	Head, Fraud Monitoring Unit	Convener & committee coordinator for reporting requirements

Appendix 3 – Closure of Fraud Cases:

For reporting purposes, only in the following instances of Fraud cases can be considered as closed:

1. The Fraud cases pending with CBI/Police/Court are finally disposed of.
2. The examination of staff accountability has been completed.
3. The amount of Fraud has been recovered or written off.
4. The Company has reviewed the systems and procedures, identified the causative factors and plugged the lacunae and the fact of which has been taken note of by the appropriate authority of the Company (Board / Audit Committee of the Board)
5. The Company is allowed, for limited statistical / reporting purposes, to close those Fraud cases, where:

    a. 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
    b. The trial in the courts, after filing of charge sheet / challan by CBI / Police, has not started, or is in progress.

The Company should also pursue vigorously with CBI for final disposal of pending Fraud cases especially where the Company have completed the staff side action. Similarly, the Company may vigorously follow up with the police authorities and/or court for final disposal of Fraud cases and / or court for final disposal of Fraud cases.