



ANTI - FRAUD POLICY

AVIVA LIFE INSURANCE COMPANY INDIA LIMITED
MAY 2013

POLICY OWNER	CHIEF COMPLIANCE OFFICER
Changes made in currentVersion	- Considering recent changes to the whistle-blow process and availability of a separate Whistle-Blower Policy, reference to the policy has been given and relevant reporting section has been summarized. - Fraud Response Plan (FRP) has been renamed as Financial Crime Response Plan (FCRP). - The Movement of GI team fraud Internal Audit team to Legal has been reflected in the document.

VERSION CONTROL

2013.01 (May 2013)
2014.02 (Aug 2014)
2015.01 (Sep 2015)
Ver.2.0/AFP/082016
Ver. 3.0/AFP/10212016
Ver. 3.1/AFP/17052017
Ver. 3.2/AFP/16052018
Ver. 3.3/AFP/12.12.2018
Ver. 4.0/AFP/20.01.2020
Ver. 4.1/AFP/31.03.2021
Ver. 4.2/AFP/14.01.2022
Ver. 4.3/AFP/16.05.2023

Table of contents

- 1. Introduction**
- 2. Objective**
- 3. Scope**
- 4. Regulation**
- 5. Fraud categories and definition**
- 6. Fraud risk management framework**
 - 6.1. Fraud management strategy**
 - 6.2. Fraud detection**
 - 6.3. Fraud prevention**
 - 6.4. Fraud response plan**
 - 6.5. Reporting and recording**
 - 6.5.1. Internal incident reporting and recording**
 - 6.5.2. External & internal reporting**
 - 6.6. Internal accountability, responsibility, expertise and resourcing**
- 7. Information sharing and co-ordination with law enforcement agencies**
- 8. Fraud monitoring functions**
- 9. Training and awareness**
- 10. Disciplinary action plan**
- 11. Glossary**
- 12. Appendix**
 - 12.1. Appendix – a : actions constituting fraud**
 - 12.2. Appendix – b : classification of frauds**

1. INTRODUCTION

Aviva India has a “Zero Tolerance” approach to fraudulent acts. Aviva India strives to maintain the highest standards of governance, personal and corporate ethics, compliance with all laws and regulations. Aviva India values integrity and honesty while dealing with all employees, customers, suppliers and other stakeholders.

Aviva India is committed to support government, law enforcement and international bodies to combat financial crime. Anti – Fraud policy will be made available for public viewing on all Aviva India Website.

Fraud Risk Preference Statement:

- Aviva India has no appetite for acts of fraud or dishonesty perpetrated by employees, directors or representatives of Aviva.
- Aviva India has no appetite for acts of fraud or dishonesty directed against or enabled through Aviva by customers, suppliers, distributors and third parties including those where Aviva has no business relationship.
- Aviva India seeks a continually improving trend on instances of fraud loss or acts of dishonesty.

2. OBJECTIVE

In order to adequately protect the organization from the financial and reputational risks posed by insurance and other frauds, framework has been put in place to identify, measure, manage, monitor and report occurrence of frauds in the company.

3. SCOPE

The framework applies to any fraud or suspected fraud in Aviva India, involving employees (including contractual employees) as well as shareholders, customers, insurance agents, corporate agents, vendors, suppliers or any third party / intermediaries who have a business relationship with Aviva India.

The Anti Fraud Policy at any point of time shall be read in conjunction with the latest version of internal manuals/procedures which also incorporate Financial Crime Minimum Compliance Standards requirements, detailed transaction monitoring framework and scenarios. The manuals/procedures will be updated from time to time depending upon changes in laws/regulations/learning from best practices and maintained with version controls.

4. REGULATION

The Insurance Development and Regulatory Authority of India (IRDAI), vide its circular IRDA/SDD/MISC/CIR/009/01/2013 dated 21st January 2013, called upon all insurers in India to recognize and assess the implication of fraud as a risk management measure and to put in place an effective and comprehensive policy to deal with fraud.

The Guidelines mandate insurance companies to put in place, as part of their corporate governance structure:

- fraud detection and mitigation measures; and

- submit periodic reports to the Authority in the formats prescribed herein (FMR – 1 and FMR – 2)
- All insurers are required to ensure that the risk management function is organized in such a way that the insurer is able to monitor all the risks across all lines of business on a continuing basis and to initiate measures to address them suitably.

5. FRAUD CATEGORIES AND DEFINITION

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 the insurer's status;
- abusing responsibility, a position of trust or a fiduciary relationship

Broadly, Insurance frauds can be categorized into following:

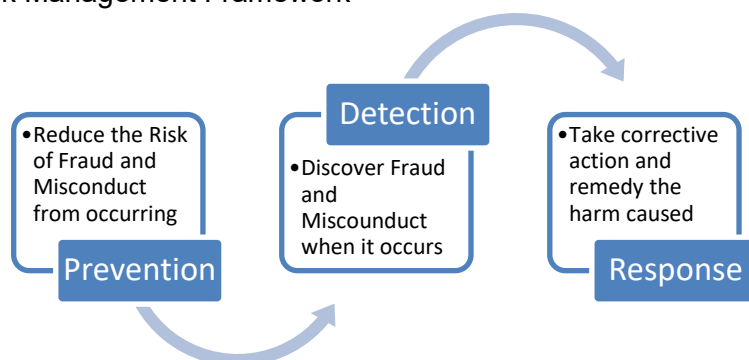
- Policyholder Fraud and / or claims fraud** – Fraud against the insurer in the purchase and / or execution of an insurance product, including fraud at the time of making a claim.
- Intermediary fraud** – Fraud perpetrated by an Insurance agent / Corporate Agent / Intermediary / Third Party Administrators (TPAs) / vendors against the insurer and / or policyholders.
- Internal Fraud** – Fraud / mis-appropriation against the insurer by its employees, Director, Manager and / or any other or staff member (by whatever name called).
- Third Party Fraud** – Fraud committed by third parties/external parties (such as suppliers, distributors including those who have no business relationship with Aviva) against the Insurer and the general public which primarily includes activities such as issue of fake / forged policies and cover notes in the name of the Insurer.

For actions constituting fraud, please refer Appendix A and detailed classification of Policyholder / Intermediary/ Internal Fraud, please refer Appendix B.

6. FRAUD RISK MANAGEMENT FRAMEWORK

Aviva India fraud risk management framework will include identifying, measuring, managing, monitoring, and reporting of fraud risks.

Fig : Fraud Risk Management Framework



6.1. Fraud Management Strategy

Fraud Management Strategy will focus on fraud prevention and to be proactive in our approach towards mitigating fraud risk through mandatory and non-mandatory controls. Mandatory controls

are primarily documented in the Financial Crime Business Standard Attestation and Non-mandatory controls are in place in form of several investigation processes, such as Sales compliance, Risk Control Unit, Claims investigation, Proposal Stage investigation, etc. Key components of an effective strategy to mitigate fraud risk are set out below –

- **Risk Identification** – Execution of a fraud risk assessment to understand Aviva India's inherent fraud risks.
- **Prevention** – Implementation of risk based, proportionate fraud prevention controls.
- **Detection** – Implementation of risk based, proportionate fraud detection controls
- **Investigation** – Design and implementation of a Fraud Response Plan (FRP) which sets out amongst other things responsibility for different types of fraud investigations (internal, claims, underwriting and etc.).
- **Reporting and Recording** – Implementation of documented fraud reporting requirements which are transparent and accurately reflect fraud data in Aviva India.
- **Management Information** – Production of relevant management information to enable effective understanding and oversight.
- **Roles and Responsibilities** – Documentation and implementation of a Fraud Target Operating Model in order to have clear roles and responsibilities related to a fraud risk management programme across the 3 lines of defence.

6.2. Fraud Detection

Detection is the proactive and reactive identification of fraud. Aviva has a detection programme to monitor activities where fraud risk has been identified through the risk assessment process or through Risk Control Unit (RCU).

Fraud detection is carried out through data mining, scrutiny of policy and other documents, screening of employees, due diligence of vendor / third party / advisors, exception reporting, red flag monitoring, quality assurance, internal audit, risk monitoring, training and awareness, transaction monitoring, information sharing.

6.3. Fraud Prevention

Fraud prevention involves identifying the root cause of an inherent fraud risk through risk assessment and implementing effective controls to stop fraud before it happens.

Following will form the basis for a proactive fraud prevention strategy

- **Risk Assessment** – The completion of a comprehensive risk assessment to initially identify the inherent fraud risks in Aviva India. Risk assessment in Aviva India will be carried out through the Risk Control Self Assessment (RCSA) framework. Continuous monitoring of identified risks will be carried out as per the prescribed methodology.
- **Risk Based Approach** – Implement risk based approach to fraud prevention.
- **Application of Controls** – Where inherent fraud risks have been identified, Aviva India should assess whether resources are sufficient and implemented controls are effective in preventing fraud or whether residual risks are present and require additional or more enhanced controls to achieve a robust control environment.
- **Training and Awareness** – Annual Financial crime training and assessment to be conducted for all employees as per stipulated timelines.
Awareness amongst employees to be created through regular mailers, e-education series, messages from the leadership, etc. Point number 9 details about the training and awareness programme.
- **Deterrence** – Framework and action grids have been created and communicated to employees through a formal channel to create awareness on Aviva's response to fraud. Identified instances may be used as deterrent. 'Tone from the top' clearly states that Aviva has a zero tolerance

approach to fraud and those found to have engaged in fraud will be disciplined and may be referred for prosecution.

- **Management Information** – Management information will be used as a fraud prevention tool e.g. training completion rates, high percentage of fraud in a particular category, region etc.
- **Independent Review of Control Effectiveness** – Independent audits are carried out by second line and third line of defence to provide an assessment of design and control effectiveness (As per their annual review plan / adhoc review).
- **Due diligence / Pre-employment Screening and Vetting** – Documented empanelment process is in place for employees, insurance agents, corporate agents, intermediaries, third party which is carried out before concluding the relationship.
- **Risk Control Unit (RCU)**: RCU has been embedded to identify potential fraud cases basis inbuilt red flags i.e. customer's profile, occupation, geographical location, Risk Coverage etc..
- **Implementation of a Whistle Blower policy** - A Whistle-blower Policy is in place to enable confidential reporting of fraud suspicions.

6.4. Fraud Response Plan

Aviva India has a documented Financial Crime Response Plan (FCRP). FCRP sets out a detailed plan and investigation procedure which covers internal reporting process, investigation responsibilities, whistle blowing charter, feedback mechanism, disciplinary actions, reporting and recording etc.

6.5. Reporting and Recording

6.5.1. Internal Incident Reporting and Recording

Aviva India has defined internal reporting and recording procedures. The Company urges its' employees, policyholders, beneficiaries, agents, brokers, corporate agents, vendors, suppliers & all concerned to act in a lawful & proper manner and to report allegations or irregularities in respect of Life Insurance Fraud to the Company. In case of any incident of fraud/possible attempt of fraud regarding the Company, kindly e-mail to speakup@avivaindia.com or refer Company's Whistle-blower Policy for more details on fraud reporting procedures.

6.5.2. External & Internal Reporting:

Fraud investigations are managed by Group Investigation (GI) team which is part of Legal team in the Company. Sales Compliances related matters also get reported to Sales Compliance team which is 2nd line of defense who then investigate, recommend appropriate actions to governance and report to GI at agreed frequency or in certain cases refer the matter to GI for investigation.

External: The FMR (FMR 1 & 2) report on policy related frauds (including both external & internal frauds) are created by Group Investigation team which is submitted to IRDAI on an annual basis (within 30 days of the close of financial year) through Compliance team as required by the regulator providing details of:

- Outstanding fraud cases and
- Closed fraud cases

Any other ad-hoc report/s required by regulator and authorities from time to time are created by GI team and submitted through Compliance team.

Internal: Fraud reports for all Internal & External frauds (including non policy related frauds) are created and reported to the Board committees by the Group Investigations team. Further, an update on Financial Crime including Fraud, Money Laundering, Sanctions, Bribery & Corruption and Facilitation of Tax Evasion is submitted to Board committees by Compliance team.

6.6. Internal Accountability, Responsibility, Expertise and Resourcing

Aviva has a defined three lines of defence fraud risk management programme where clear lines of internal accountability and responsibility have been laid out in FCTOM and roles and responsibility document.

The 'three lines of defence model' is structured as follows:

- **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 1st line of defence.
- **Second line of Defence** – The Compliance and Risk function are 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** – Internal Audit (IA) is the 3rd line of defence. IA is responsible for independent assessment on the effectiveness of the fraud controls framework design and operation is also responsible for reporting findings and concerns to group and Aviva's audit and risk committees.

Role of Chief Compliance Officer: The Chief Compliance Officer is also the Head of Financial Crime and Designated Individual & Nominated Officer to monitor measure and report all financial crime risks for the business in line with the job description of the Chief Compliance Officer and in line with the performance key result areas assigned by the Company and reviewed by the reporting manager at appropriate intervals.

7. Information sharing and Co-ordination with Law Enforcement Agencies

Aviva is committed to provide the necessary support & information on fraud as required through Life and General Councils and co-ordinate with law enforcement agencies for exchange of information. Necessary information on Frauds can be shared amongst all insurers through respective Councils / Forums. Requirements of dealing with law enforcement agencies have been broadly categorized in following two categories:-

- Coordination for frauds detected by the Company and frauds reported to the Company by Authority.
- Coordination for policy related information sought by a Statutory Authority like CBI / Income Tax etc.

As per the new regulations issued by IRDAI for Appointment of Insurance agents, 2015 (dated 16-Mar-15) the designated officer has to update to other Insurance companies regarding the action taken (only termination) on the agents, list of terminated agents needs to be updated on the blacklisted agents portal of IRDAI.

8. Fraud monitoring Functions

Activities for fraud monitoring are collectively held by second and third line of defence with clear set out responsibilities. Fraud prevention and detection is carried out by the Risk and Compliance team. Investigations and reporting are undertaken by the Internal Audit team.

SPOC of every department needs to interact directly with the fraud monitoring function and report suspicious activities within their departments or identified during their anti-fraud procedures. Any employee, intermediary or supplier can whistle blow to the Fraud Monitoring Function. The Fraud Monitoring function (FMF) is committed to independently investigate such allegations in confidentiality.

9. Training and Awareness

Financial crime training to all employees is provided at the time of joining through induction programme. All employees need to undergo and ensure timely completion of mandatory annual training on Financial Crime which includes components, such as Anti Money Laundering (AML), Anti-Bribery and Corruption (ABC), Central Monitoring, Gift & Entertainment (G&E) and Market Abuse. To ascertain the successful training completion, assessment is conducted.

In addition, role specific training will include:

- Providing enhanced training to employees with specific roles which may present a higher risk or hold the responsibility of ensuring implementation and effectiveness of financial crime controls.
- Tailored to higher risk roles held by employees;
- Including red flags for potential indicators of financial crime.
- Key components of financial crime laws and regulations e.g. Elements of financial crimes, requirement for financial institutions to implement financial crime prevention programmes consistent with applicable local laws, Politically Exposed Persons (“PEPs”) and other higher risk financial crime issues;
- Applicable local legal and regulatory requirements for the recognition and reporting of suspicious transactions, cash transactions exceeding local thresholds and sanctions reporting; and
- Escalation protocols.

Awareness amongst employees may be created through regular mailers, e-education series, messages from the leadership etc.

10. Disciplinary Action Plan

All employees and agents of Aviva whether active or not can attract an action against any fraud event. There is a defined action grid on the basis of which action will be taken on the employee.

11. Glossary

As per the IRDAI, points included in the framework of the policy are included wholly or partly in the mentioned paragraphs.

- **Procedure for Fraud Monitoring** – Risk Identification point in Point number 6.1 and Risk Assessment point in Point number 6.2 describes the process for identification of potential areas of fraud.
- **Identify Potential Areas of Fraud** – Appendix – A gives the illustrative list of potential areas of fraud.
- **Co-ordination with Law Enforcement Agencies** – Explained in Point number 7 Information sharing and co-ordination with law enforcement agencies.
- **Framework for Exchange of Information** – Explained in Point number 7 Information sharing and co-ordination with law enforcement agencies.

- **Due Diligence** – Explained in Point number 6.3 Due diligence / Pre-employment Screening and Vetting
- **Regular Communication Channels** – Explained in Management information point in Point Number 6.1. Implementation of a Whistle Blower policy point in Point Number 6.3.
- **Fraud Monitoring Function** – Explained in Point Number - 8
- **Reports to the Authority** – Covers in Point Number 6.5.2 External & Internal Reporting
- **Preventive Mechanism** – Covers in Introduction paragraph and Point Number 6.2 Fraud Prevention.
- **Insurer's to Ensure Compliance** – Point 6.5.2, Application of Controls point of Point Number 6.2

Appendix

Appendix – A: Actions Constituting Fraud

Based on the nature, size and distribution of business, following is the illustrative list of potential fraud areas:

- Forgery or alteration of any document including but not limited to the Company's insurance policies or insured parties
- Forgery or alteration of checks, bank drafts, or any other financial documents.
- Fraudulent alteration, addition or removal of information on the Company's management information systems.
- Any dishonest or fraudulent act or attempted act by employees of the Company
- Misappropriation of funds, securities, supplies, or other assets
- Impropriety in the handling or reporting of money or financial transactions
- Disclosing confidential and proprietary information to outside parties
- Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment; and/or
- Fraudulent financial reporting
- Stealing cheques, assets, records etc.
- Inflating expenses claims/over billing, tampering of bills
- Paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
- Permitting special prices or privileges to customers, or granting business to favoured suppliers, for kickbacks/favours
- Forging signatures
- Removing money from customer accounts
- Selling insurer's assets at below their true value in return for payment
- Reporting and claiming of fictitious damage/loss
- Medical claims fraud
- Fraudulent Death Claims
- Policyholder Impersonation
- Signature Forgery
- Misselling which has resulted in Refund of premium or fund value including rebating the customer
- Split of policies: Multiple policies of the same product category sold to the same customer with same beneficiary and term and conditions (within 60 days)
- Proposal documents/claims documents submitted for non-existent customers / person was dead before proposal was logged-in/policy was issued
- Same address proof/ telephone number for multiple unrelated customers
- OSV done for forged documents
- Posting of renewal premium into new business or in other policy or Churning of policies basis customer complaint
- Fraudulently surrender of existing policy of customer by advisor/SM
- Influencing the doctor to conceal information/ alternatively coercing the doctor to submit report without conducting tests or sending a dummy person to attend medicals
- 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 difference
- Disclosing to other persons the confidential or private business activities of the Company.
- Accepting or seeking anything of material value from applicants, beneficiaries,
- The improper withholding of any money or premiums paid on an insurance policy, if the insurance contracted for is not ultimately provided.

- Any false statement made to law enforcement agencies, prosecutors or the insurance departments of any state.
- Any similar or related irregularity.
- Abuse of Aviva brand
- Fraud typologies identified by international organisations, such as Financial Action Task Force.
- Fraud typologies and examples identified in local national risk assessments, law enforcement publications or regulatory guidance.
- Payments made to fictitious suppliers

Fraud investigation manual including investigation procedures are maintained by GI team. Individual fraud investigation procedures are maintained at a functional level within Sales Compliance (2nd line defence) and Claims & Risk Control Unit (1st line of defense).

Appendix – B

Some of the examples of fraudulent acts / omissions include, but are not limited to the following:

Policyholder Fraud and/or 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:

- Claims fraud - death, critical illness, waiver, Private Medical Insurance or Permanent Health Insurance claim is fraudulently made against the policy. For example, death claims when the event has not happened, fraudulent non-disclosure / misrepresentation. Staging the occurrence of incidents
- Medical claims fraud
- Underwriting fraud - where a policyholder or applicant either deliberately misrepresents or deliberately fails to disclose material facts at policy inception (that would materially impact either the terms & conditions applied to a policy of insurance, or the issue/renewal decision itself) for financial gain.
- Assignment fraud -when an insured or owner takes possession of the issued policy, s/he will transfer ownership, or "assign" the policy for value to a person or entity with no insurable interest in the continuation of the insured person's life.
- Trustee fraud - Fraud by trustees or potential beneficiaries of defined benefits pensions schemes. Also includes exaggerated deductible expenses.

Intermediary fraud – Fraud perpetrated by an Insurance agent/ Corporate Agent/ Intermediary/ Third Party Administrators (TPAs) against the insurer and/or policyholders:

- Broker / Agent fraud - fraud or manipulation of records by a general insurance intermediary, agent or broker resulting in a loss to the Company or our policyholders. For example, Manipulation of systems, Non submission of premiums, Overcharging customers
- Policy related fraud - any attempt to obtain payment from a policy to which the recipient is not entitled where there is no suspicion that this is by a member of staff, intermediary or supplier.
- Premium Diversion – Where 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 difference
- Commission Fraud – Insuring non-existent policy holders while paying a first premium to the insurer, collecting commission and annulling the insurance by ceasing further premium payments.

Internal Fraud – Fraud/miss-appropriation against the insurer by its Director, Manager and/or any other or staff member (by whatever name called):

- Misappropriating funds
- Stealing cheques
- Overriding decline decisions to open accounts of family and friends
- Forging signatures
- Forging documents
- Permitting special privileges / kick backs to customer etc.