Pramerica | LIFE INSURANCE

ANTI FRAUD POLICY

VERSION: 1.7.1

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 Pramerica Life Insurance Limited ("Company") understand the nature and impact of fraud and take preventive steps to minimize the vulnerability of our operations to fraud.
Insurance Regulatory and Development Authority (IRDA), vide circular IRDA/SDD/MISC /CIR/ 009/ 01/2013 and **Master circular IRDAI/F&I/CIR/MISC/82/5/2024 on Corporate Governance for Insurers**, has laid down the guidelines requiring insurance companies to have in place a comprehensive Fraud Monitoring Policy and Framework

And in March 2017 Insurance Regulatory and Development Authority of India (IRDAI) has issued guidelines on Insurance E-Commerce vide circular ref. no. IRDA/INT/GDL/ECM/055/03/2017 dated March 09, 2017 wherein fraud detection measures in e commerce activities undertaken by the company also needs to be included in Anti Fraud Policy.

With the above stated objectives of fraud risk management, the Company's "Anti-Fraud Policy" referred to as "Policy" lays out the Company's stance on fraud prevention, detection, investigation, correction and reporting of frauds. This shall help the Company to mitigate fraud, corruption and misconduct, as well as respond to such matters, should they arise.

2. Purpose

The purpose of this Policy is to:

- Establish the Company's position on 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, Management, employees and specific Functions

3. Definition, Scope and Classification of Fraud

Fraud may be defined as an act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties. This may be achieved by means such as:

- 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 Management and the Board of Directors as well as stakeholders who conduct business with the company, such as third party agents, representatives, brokers, Insurance Self Network Platform (ISNP), 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:

1) Policy Holder and/ or Claims Fraud – Fraud against the Company by a client or policy holder or any other external party other than intermediary in the purchase and/ or execution of an insurance product, including fraud at the time of making a claim.

   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
   - Collusion with sales persons to purchase and cancel policies with intent to collect commission
   - Exaggerating damage / loss
   - Medical Claim Fraud

2) Intermediary Fraud – Fraud perpetrated by an insurance agent/ Corporate Agent/ Intermediary/ policies sourced through ISNP/ Third Party Administrators (TPAs) against the insurer and/or policyholders.

   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 of client documents such as age, KYC, income proofs,
   - Collecting premium into own account, submitting unrelated third party premium instruments against customer application
   - Collusion with policyholder to purchase and cancel policies with intent to collect 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

3) 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
   - Frauds listed under "Intermediary Fraud" as applicable to sales employees
   - Misappropriation of Company, policyholder, intermediary funds
   - Fraudulent financial 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 or in collusion with suppliers
   - 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

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 our Board of Directors, Managing Director & CEO & Management Team, Fraud Control 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 or any of its Committees that it so appoints, 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.
- Monitor reports provided by management on Fraud risk, policies and control activities.

5.2 Managing Director & CEO and Functional Heads

The Managing Director & CEO and Functional Heads of the Company have overall responsibility for the design and implementation of a fraud risk management program including:

- Setting the tone at the top for the rest of the organization in the promotion of fraud risk management, internal controls and a zero tolerance anti-fraud culture.
- Assessing the risks, including but not limited to fraud risks, involved in their area of responsibility
- Ensuring that adequate internal controls exist and function to detect, report and deter fraud that are cost effective and commensurate with the magnitude of identified risks.

- Encouraging staff to report reasonable suspicions of fraud and ensuring that staff is comfortable to report fraud without fear of reprisal.
- Reviewing and monitoring reports provided to the management on fraud risk, policies and control activities.
- Ensuring that management has adequate resources at its disposal to enable Company to achieve its fraud risk management objectives.
- Ensuring that exposure to fraud is considered when introducing new, or when amending existing, systems and processes.

5.3 Fraud Control Unit ("Unit")

The Fraud Control Unit shall be responsible for the development and implementation of the Company's fraud risk management program

The Fraud Control Unit shall:

- Assist management in establishing and implementing a framework for adequate internal controls to prevent and detect fraud.
- Conduct regular monitoring activities and advise the concerned management on potential threats, fraud risks and remedial action.
- 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.
- Co-ordinate with law enforcement agencies for reporting frauds on a timely basis.
- Provide necessary reports to Management, Board and Regulator on fraud cases received and actions taken to manage fraud risks.
- Assist in laying down procedures for exchange of necessary information on frauds amongst all insurers.
- Create awareness on ways to counter fraud among the employees / policy holders at regular intervals.

5.4 Employees

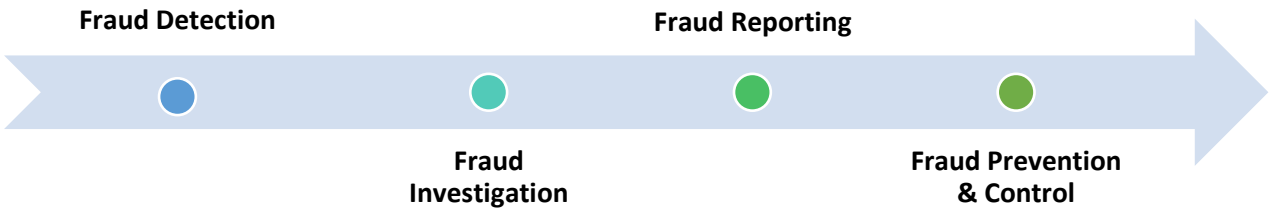
All employees are responsible for assisting the Company in safeguarding its funds and other assets, as well as protecting its reputation and business from matters involving fraud, corruption and misconduct.

All levels of employees shall:

- Have a basic understanding of fraud and be aware of red flags pertaining to their areas

- 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.
- 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 minimize the possibility 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.

Department wise anti-fraud procedures are embedded into processes such as:

- 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

The Company conducts series of proactive monitoring of processes and transactions across various functions in order to detect potential frauds or negative trends. These monitoring activities help detect anomalies or identify potential frauds. Examples of areas that may be monitored are premium payment through serial cheques, Customer contactibility and Policy delivery trends, lapsation and claims trends, Policy splitting and replacements, AML transaction monitoring, employee expense claim trends, sharing of confidential data by employees with unauthorized persons.

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 and to protect them 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 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.

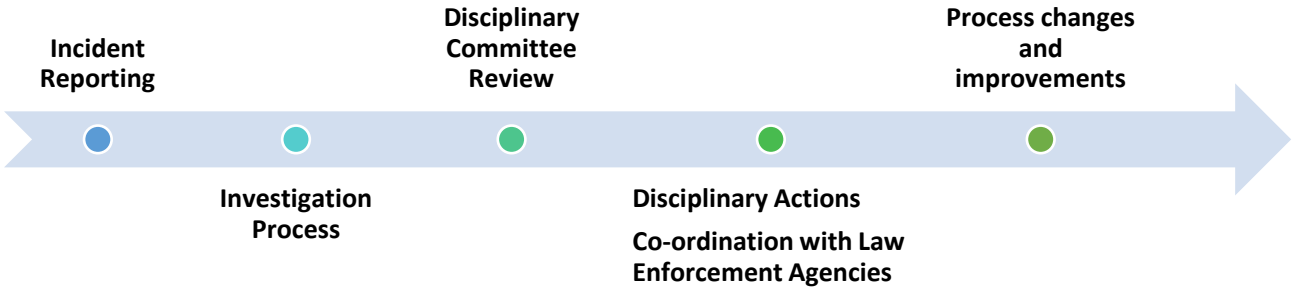
6.1.6 Customer Complaints

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 Council. 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.

6.2 Fraud Investigation Process



6.2.1 Incident Reporting:

In case of any incident of fraud / possible attempt of fraud regarding Pramerica Life Insurance Limited, kindly e-mail or write to us at the below address:
Fraud Control Unit, Pramerica Life Insurance Ltd., 7th & 8th Floor, Tower 2, Capital Business Park, Sector 48, Gurugram, Haryana – 122018
Email: fraud.control@pramericalife.in

6.2.2 Investigation Process:

The Fraud Control 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 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 into an Investigation Report. The report will include a summary of the sequence of events, evidence, if any, against individuals, Company policies that have been violated and the proposed penalties.

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 Committee Review

The Company has established a Disciplinary Committee ("Committee") sponsored by the Managing Director & CEO that shall decide and concur upon disciplinary actions to be taken against employees and intermediaries based on investigation findings.

The Committee or a Sub-Committee that it so appoints, will decide the disciplinary action(s) after reviewing and discussing the report. The Committee will evaluate each instance of misconduct in consideration of 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 and nature and severity of the violation. The decisions of the Committee will be documented.

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 Control Unit will communicate actions to relevant functions for implementation.

Human Resources 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 Control Unit for its records.

In case of disciplinary action against agents, Distribution Operations will perform the necessary administrative tasks.

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 IRDA.

The Fraud Control 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 Unit.

6.2.6 Process Gaps & Change recommendation

The Fraud Control 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. Function management is expected to implement the recommendations after due evaluation.

6.3 Fraud Reporting

6.3.1 Internal Reporting

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

The Unit will on at least a half yearly basis, update the Board or any of its Committees that it so appoints, on Fraud Risks, trends and control activities.

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 Due Diligence:

The Company will conduct appropriate background checks and/ or due diligence on new employees, agents, intermediaries and vendors. This may include checks relating to educational background, work experience, criminal records and screening against watch lists. The due diligence shall be done by the respective functions.

6.4.3 Training & Awareness :

The Company and its management will ensure that its employees and associates undergo formal and informal training on ethical conduct and fraud awareness. The objective of such training will be familiarize personnel with the Fraud Policy, raise awareness of what

constitutes fraud, how to prevent, detect and report frauds and communicate expectations from associates.

6.5 Aadhar data & EKYC Fraud prevention control measures

Aadhaar e KYC is the way of resident authentication. Aadhaar allows the residents to submit it as document verifying your identity and other particulars linked to Aadhaar number.

During Aadhaar based e KYC verification, an OTP would be sent by UIDAI for authentication purpose. This is sent on Mobile number registered with UIDAI.

Aadhaar data & EKYC process to prevent authentication related frauds by following below mentioned preventive measures

- Masking of Aadhaar data as required by regulations
- OTP information is not stored with company
- Aadhaar Authentication requests are digitally signed
- Terminal devices used shall ensure users are authenticated & devices protected
- In case of 4 consecutive failed authentication attempts, user access would be blocked to prevent unauthorized access

Fraud control measures

- Carrying out onsite vendor reviews for designated vendors wherein fraud risk exposure is high / which are responsible for execution of such controls
- Review of work allocation to vendors to minimize the possibility of vendor favoritism in applicable areas
- System event and activity log monitoring
- Provide communication channels and mechanisms, specified through this policy as well as in the whistle-blower policy, for relevant stakeholders including employees, Board of directors and customers to report matters pertaining to fraud.
- Regular reviews carried out by the internal audit function to identify fraud events that may not get reported or identified in the normal course of business
- Usage of anti-fraud solutions as implemented by the Company from time to time

Aadhaar data & EKYC process to prevent authentication related frauds by following below mentioned measures (indicative not exhaustive)

- Authentication and transaction logs capture requisite details as required by the regulation
- Such logs will be retained for a minimum specified period with controlled access
- These controls must be considered and adopted by functions (wherever necessary) with guidance from the Risk Management- Fraud risk team.
- Any fraudulent event noted involving Aadhaar data/authentication related request shall be duly investigated and dealt in line with applicable provisions

<<<End of the Document>>