Pramerica | LIFE INSURANCE

ANTI FRAUD POLICY

VERSION: 2.0

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 **Insurance Fraud Monitoring Framework Guidelines, 2025** 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

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 and Scope

3.1 Definition of Fraud - Fraud may be defined as any act or omission, whether attempted or actual, intended to obtain a dishonest or unlawful advantage for the party committing the fraud or for any related party. Such acts or omissions may be carried out through, but are not limited to, the following means:

- Misappropriation of assets
- Deliberate misrepresentation, concealment, suppression, or non-disclosure of one or more material facts relevant to a financial decision or transaction
- Abuse of responsibility, position of trust, or fiduciary relationship

3.2 Scope of Applicability - This Policy shall apply to all employees of the Company, including members of Management and the Board of Directors. The Policy shall also apply to all external parties and stakeholders who conduct business with or on behalf of the Company, including but not limited to insurance agents, corporate agents, brokers, consultants, contractors, suppliers, vendors, subcontractors, partners and other service providers.
The Policy further covers fraudulent acts committed through direct digital channels, including policies sourced through the Insurance Self-Network Platform (ISNP) or any other insurer-owned or insurer-operated platform

3.3 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.

3.4 Cyber or New Age Fraud means any insurance fraud carried out using digital or new age technologies.

3.5 Distribution Channels includes insurance agents, intermediaries or insurance intermediaries, and any persons or entities authorized by the IRDAI to involve in sale and service of insurance policies

4. Classification of Fraud

Frauds can be broadly classified into:

4.1 Policy Holder and/ or Claims Fraud – Fraud against the Company by a client or policy holder or any other external party other than Distribution Channel 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

4.2 Distribution Channel Fraud – Fraud perpetrated by Distribution Channel 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

4.3 Internal Fraud – Fraud/ Misappropriation against the Company involving internal staff, including employees and / or senior management

Such frauds include but are not limited to –

- Intentional non-disclosure or misrepresentation of education or past employment information
- Frauds listed under “Distribution Channel Fraud” as applicable to sales employees
- Misappropriation of Company, policyholder, Distribution Channel 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

4.4 External Fraud – Fraud committed against the Company by external parties' / service providers / vendors etc.

Such frauds include but are not limited to –

- Medical Service Provider Fraud like Fabricated Medical Records, Collusion with Policyholders
- Investigation Agency & Field Vendor Fraud like Fake Field Investigation Reports, Collusion with Claimant, Inflating or Fabricating Expenses
- Diagnostic Lab Fraud

4.5 Affinity Fraud or Complex Fraud – Fraud involving collusion among one or more fraud perpetrators in the above categories.

5. Roles and Responsibilities

The following section highlights the roles and responsibilities of our Board of Directors, Managing Director & CEO & Management Team, Fraud monitoring Committee, Fraud monitoring 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.

5.2 Risk Management Committee (RMC)

RMC shall be responsible for following:

- Effective implementation and oversight of the fraud risk management framework
- Monitor reports provided by Fraud Management & Disciplinary Committee on Fraud risk, policies and control activities

5.3 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.

5.4 Fraud Monitoring and Disciplinary Committee (FM&DC)

FM&DC shall be headed by a Key Management Person and include senior representatives from relevant departments, such as underwriting, claims, legal or any other department as deemed necessary, while avoiding conflicts of interest in it's composition and functioning and would be responsible for following:

- Operationalizing the Fraud risk management framework and oversee activities, as appropriate, to ensure fraud deterrence, prevention, detection, reporting and remedying through Fraud monitoring Unit or any other mechanism as deemed fit.
- Recommend and regularly update, based on experiences, appropriate measures on fraud risk management to various functions.
- 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.
- Conduct an Annual Comprehensive Fraud Risk Assessment to identify potential vulnerabilities across business lines and activities for fraud, using past experiences, emerging trends & Red Flag Indicators (RFIs), etc.
- Identify areas for improvement and adaptation of the Fraud Risk Management Framework.
- Submit regular reports to RMC and Audit committee as applicable.
- May form subcommittees, as required, for its effective functioning.
- The FM&DC or a sub-Committee that it so appoints, will decide the disciplinary actions, pertaining to the incidents of fraud.

5.5 Fraud Monitoring Unit (FMU)

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

The Fraud Monitoring Unit shall:

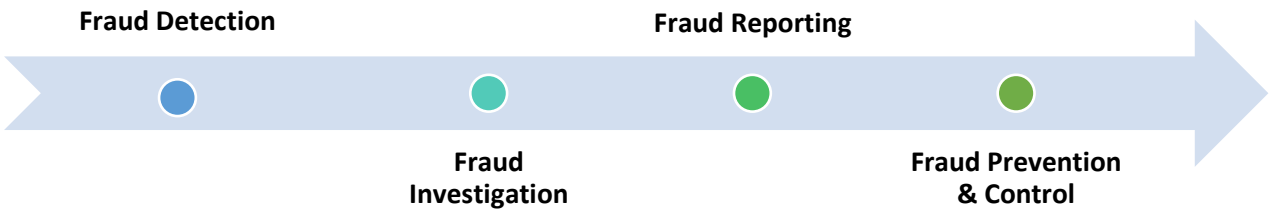
- Support FM&DC in discharging its functions and effective implementation of Fraud Risk management Framework
- Oversee and/or execute investigations as warranted by matters reported by employees and stakeholders.
- Oversee execution of all actions recommended by FM&DC.

5.6 Employees

All levels of employees shall:

- 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.
- 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 or Fraud Monitoring Unit
- 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 Distribution Channel, partners, vendors and service providers of the Company adhere to the standards and principles of this Policy.

6. Fraud Management Framework



6.1 Fraud Detection, Mitigation and Monitoring

Fraud Detection is the identification of an actual or potential fraud. Frauds may be detected through various onsite inspections of processes, employees, documents or Red Flag Indicators. 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 Indicators (RFI) and Controls measures

The Company conducts series of proactive monitoring of processes and transactions across various functions in order to detect potential frauds or negative trends through established red flag indicators and control measures. The parameters for RFIs are dynamic and may vary depending on:

- Evolving fraud typologies,
- Changes in business processes or distribution models,
- Emerging technology and cyber risks, and
- Observed trends, internal incidents and industry intelligence.

Without limiting the scope of RFIs, the following table provides illustrative examples of broadly defined RFIs across fraud categories. These indicators are indicative in nature and subject to periodic review.

Fraud Category	Illustrative Red Flag Indicators
1. Internal Fraud	Adverse finding in background verification report during employee on-boarding
	Indicators of misuse or unauthorized access to confidential data
2. Distribution Channel Fraud	identify and categorize high-risk cases identified based upon adverse findings from IIB / Internal checks
	Adverse inputs received through market intelligence regarding insurance application
	Claims, Cancellations and mis-selling trends
3. Policyholder and / or Claims Fraud	Inconsistencies observed during policy payout checks or suspicious transactions report
	Early claims
	Adverse inputs received through market intelligence regarding claim
4. External Fraud	Inconsistencies or abnormal patterns in vendors such as diagnostic lab centre, investigation agencies, etc.
	Repetitive use of common identifiers in vendor payments (such as bank accounts, registration numbers or invoices)
5. Affinity / Complex (Collusive) Fraud	Patterns indicating possible collusion between internal or external entities

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, distribution channel, vendors and service providers or those routed through regulatory bodies and law enforcement agencies.

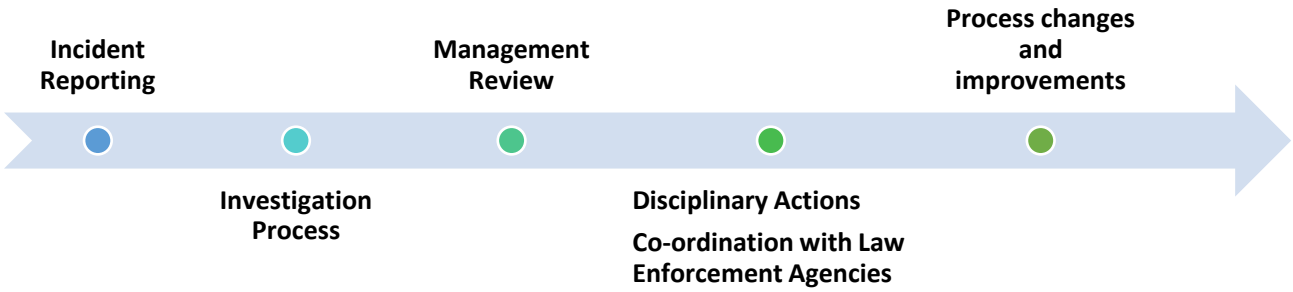
6.1.6 Customer Complaints

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

6.1.7 Fraud Monitoring Technology Framework of IIB

The Company shall participate in the Fraud Monitoring Technology Framework made available by the Insurance Information Bureau (IIB) to help the industry to combat fraud. 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 Monitoring 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 Monitoring Unit will review relevant information relating to the report/ complaint and conduct detailed investigations with all related internal and external parties to collect evidence and establish the facts of the case.

During the investigation all employees and associates related to the case or that are interviewed would be required to maintain confidentiality of the proceedings and provide information completely and accurately. The investigations team may request written reports or statements from those involved in the case.
The FMU 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 investigation shall be completed within a reasonable timeframe commensurate with the complexity and severity of the case.

6.2.3 Management Review

The Fraud Management and Disciplinary Committee or a Sub-Committee that it so appoints, shall decide and concur upon disciplinary actions in the incidents of frauds based on investigation findings.

6.2.4 Disciplinary Actions

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

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, recommend training re-enforcement, process improvements or changes, where applicable. 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.

As per the decision of the FM&DC, the Fraud Monitoring 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 Monitoring Unit for its records.

In case of disciplinary action against Distribution Channel, 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.

The Fraud Monitoring Unit will consult or seek assistance from the Legal Team while submitting or following-up on such disclosure and complaints.

6.2.6 Process Gaps & Change recommendation

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

6.3 Fraud Reporting

6.3.1 Internal Reporting

The Fraud monitoring committee shall:

- Submit quarterly reports to the RMC on its activities, findings, and recommendations including the financial impact of fraud on the insurer.
- Submit report of the Annual Comprehensive Fraud Risk Assessment before the Board of Directors through RMC.
- Report to the Audit Committee, in addition to the RMC, in case of all internal frauds.

6.3.2 External Reporting

- The Company shall file annual returns with Authority in forms FMR-1 within 30 days of close of the financial year
- In the event of fraud committed by distribution channels registered by IRDAI, the insurer shall promptly escalate and report the matter to IRDAI without delay.

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 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, distribution channel 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 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 Company will also ensure that its employees, the senior management including the board members and distribution channel shall undergo periodic fraud prevention training.

6.5 Cyber /New Age Fraud prevention control measures

- The Company has a robust cybersecurity framework and processes to protect against cyber or new age frauds and evolving technology-enabled threats.

- The Company shall continuously monitor and strengthen systems and processes for cyber fraud risk management, including incident databases, customer and intermediary verification mechanisms and access control.

6.6 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>>