

Fraud Risk Management Policy

July 2024

Contents

1. Introduction and objective	3
2. Fraud definition and classification	3
3. Fraud governance structure	5
4. Fraud Prevention.....	5
5. Fraud detection	5
6. Fraud Investigation	6
7. Reporting and fraud loss assessment.....	7
8. Training and awareness.....	7

1. Introduction and objective

1.1. Objective

The Fraud Risk Management Policy ("the Policy") sets out the approach and guidelines for management of the fraud risk at ICICI Prudential Life Insurance Company Limited ("the Company"). The objective of this Policy is to safeguard the reputation and financial viability of the Company through improved management of fraud risk.

1.2. Regulatory requirement

Insurance Regulatory and Development Authority of India (IRDAI) has issued guidelines in relation to "Insurance Fraud Monitoring Framework" which emphasize the requirement to have appropriate framework to detect, monitor and mitigate occurrence of frauds.

1.3. Applicability

It is the responsibility of all relevant staff to be familiar with the contents of the Policy and to exercise sound judgment to act within the framework in their daily work. Guidance must be sought from the Operational Risk Management (ORM) team, where application of the framework described in the Policy is not clear.

1.4. Scope

The Policy sets out the roles and responsibilities and the processes to detect fraud, manage response to reported or suspected fraud, and deploy measures to prevent or minimise the risk of fraud.

The Policy may be changed only with the approval of the Board and should be reviewed as the need may arise, but atleast annually.

2. Fraud definition and classification

2.1. Actual fraud

As defined in point B of the guidelines issued by IRDAI and requirements as per Companies Act 2013, "Fraud" in relation to affairs of a company 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.

2.2. Attempted fraud

An attempted fraud is an incident where a fraudster tries perpetrating a fraud and the same is prevented by the Company's system and process controls. There is no loss to the Company or to the customer in an attempted fraud. The following conditions must be satisfied:

- (a) A 'deliberate act/omission'
- (b) Such act/omission did 'not' result in a 'wrongful gain' to any person

In case a 'wrongful gain' is established to anyone (including for a temporary period), the act ceases to be an 'attempted fraud' and falls into the category of being an 'actual fraud'. Wrongful acts committed by a staff member without any misappropriation of funds for personal use and the wrongful gain so derived from committing such acts cannot be clearly quantified and hence such instances would be treated as attempted frauds.

2.3. Fraud classification and categorisation

Frauds can be classified on the below lines;

- (a) Misappropriation of assets;
- (b) Deliberate misrepresentation or suppression of material facts;
- (c) Abuse of responsibility, position of trust or fiduciary relationship

Additionally, such frauds can be categorised based on the relationship of the Company with the individual(s) involved in the fraud:

Internal fraud - Fraud against the insurer by its employees, either individually or in collusion with others who are either internal or external to the insurer;

External fraud - Fraud against the insurer, by vendors, customers or unrelated entities to obtain wrongful payments in any form; and

Intermediary fraud - Fraud perpetuated by intermediaries (insurance agent/corporate agent/other intermediaries) against the insurer policyholders, customers or beneficiaries

2.4. Amount involved in fraud

The amount involved shall be arrived by the nature of fraud:

- (a) Amount in policy related forgery or tampering if identified before claims stage shall be the total premium paid but actual loss shall be the loss incurred by the Company;
- (b) Amount in policy related tampering if identified at claims stage shall be the sum assured but the actual loss shall be "Nil";
- (c) In case of fraud identified post issuance of a policy and subsequently the policy was repudiated or voided by the Company, the fraud amount involved shall be the sum insured but the actual loss shall be "Nil";
- (d) If the fraud has been identified post claims or redemption payment then the total amount paid shall be considered as loss;

- (e) For instances of proven cash/cheque misappropriation, the amount misappropriated shall be equal to the actual loss

3. Fraud governance structure

3.1. Roles and responsibilities

The ORM team will be responsible for periodic identification, measurement, control and monitoring of fraud risk and reporting their findings to the Executive Risk Committee (ERC). The ERC reports the key findings to the Board Risk Management Committee (BRMC) every quarter.

3.2. Root cause analysis

Analysis of actual and potential loss events above ` 1 million should be performed to identify risks. The ORM team should carry out an independent root cause analysis of such incidents and report it to the Operations Risk Committee (ORC) and the Executive Risk Committee (ERC). These loss events could either help identify inadequacies in the control measures for known risks or identify new risks which need to be addressed.

4. Fraud Prevention

4.1. Risk & control self-assessment (R&CSA)

The ORM team will periodically engage with relevant business functions to conduct an R&CSA to:

- (a) Identify potential fraud or system lacunae that may permit perpetration of fraud;
- (b) Review the efficacy of internal controls and remedial action taken to prevent recurrence of frauds;
- (c) Recommend measures to strengthen preventive measures against frauds

4.2. Know your employees and intermediaries

The Company shall ensure appropriate due diligence prior to onboarding its employees and intermediaries

4.3. Key risk indicators (KRI)

The Company should develop appropriate KRIs which would act as lead or lag indicators of fraud risk. The KRIs and their thresholds should be defined by the ORC and approved by the ERC.

5. Fraud detection

5.1. System alerts

The Company should deploy system triggers including for online business to detect any anomalies related to new business (pre-issuance), claims and payout (surrender and partial withdrawal). Additionally, internal employees, advisors, channel partners and policyholders should be encouraged to report suspicious transactions/behavior.

5.2. Whistle blower mechanism

The Company shall have a whistle-blower policy to provide a mechanism to ensure that concerns are appropriately raised, independently investigated and addressed. The purpose of the policy is to enable reporting of matters without the risk of subsequent victimisation, discrimination or disadvantage.

6. Fraud Investigation

6.1. Process management

The ORM team is responsible for the examination of a suspected fraud (or a transaction) or a customer dispute/alert. The ORM team has the authority to appoint external investigation agencies for this purpose. Operational risk managers should undergo requisite training to enhance their skills and competencies. Operational risk managers should use appropriate techniques including computer forensics and forensic accounting. Oral interviews of customers, employees, advisors and partner employees may be conducted, as necessary, to understand the background and details of the case through prescribed procedures.

The operational risk managers should ensure that investigations do not breach specified closure times for customers' complaints as per the grievance redressal guidelines.

6.2. Information sharing with other companies

To ensure effective fraud mitigation, the Company shall evaluate opportunities to exchange information with other industry members. The Company shall engage with industry bodies to create a common platform for such information exchange.

6.3. Filing of police complaint with the police and/or other law enforcement

The Company will evaluate filing of complaints with police and/or other law enforcement agencies depending on the case facts.

6.4. Recovery of fraud losses

In case of financial loss to the Company, the ORM team/Legal team may engage in the recovery process based on the case facts along with respective departments for attempts to recover the amount lost, including co-ordination with third parties, if required.

6.5. Staff Accountability

The Company's Code of Conduct defines the professional and ethical standards that all its employees and Directors need to adhere to in compliance with all applicable statutory laws, regulations and internal policies. All employees affirm compliance with the Code of Conduct every year.

To administer and ensure compliance to the Code and applicable statutory laws and regulations as maybe there, the Company has defined the Employee Service Rules (ESR) and the Whistle Blower Policy.

The ESR define the terms and conditions of appointment and service, the rules of conduct that employees need to adhere to at the workplace and the procedure of disciplinary proceedings in the event of any breach of any policy governing employee conduct at the workplace that may be defined from time to time and also any statutory or regulatory laws as may exist.

7. Reporting and fraud loss assessment

7.1. Quarterly Risk Reports

The results of risk measurement and control for fraud risk should be published in the Quarterly Risk Report to be reviewed by the ERC, which in turn must present a summary to the BRMC on a quarterly basis. The report should present:

- (a) Losses arisen on account of fraud, both in value and volume, by category of loss;
- (b) Mitigation plans for identified process weaknesses

Loss events due to fraud should be tracked. Identified loss incidents should be classified as follows:

- (a) Actual loss: An incident that has resulted in an actual financial loss;
- (b) Attempted loss: An incident that has been identified and reported but may not ultimately result in a financial loss

8. Training and awareness

8.1. Culture

The ORM team should promote risk awareness culture by improving understanding of fraud.

(a) External awareness

Potential and existing customers are informed about the Company's policy through its website stating the consequences of submitting a false statement and/or incomplete statement for making personal gain.

(b) Internal awareness

The ORM team shall facilitate training/awareness of employees on fraud prevention practices.