Anti-Fraud Policy

January 2024

Contents

1 Introduction

1.1 Background

In accordance with the PFRDA Framework for Prevention and Reporting of Fraud under NPS Architecture Guidelines 2023 (hereinafter referred to as "the Framework"), SBI Pension Funds Private Ltd (hereinafter referred to as "the Company") is required to have in place an Anti-Fraud Policy(hereinafter referred to as "the Policy"), duly approved by the Board of Directors.

Further, as laid down in the PFRDA (Framework for Prevention and Reporting of Fraud under NPS architecture) Guidelines dated 19th December, 2023, the Managing Director/Chief Executive Officer (MD/CEOs) of the pension funds have the obligation to lay down a policy to deal with fraud and its prevention and reporting in accordance with these guidelines.

Accordingly, the Policy has been formulated considering the various types of frauds that the Company can be exposed to. This Policy hasbeen further devised to ensure that the fraud detection framework is in line with therequirements as laid down under the Framework, as well as it recognizes the principle of proportionality and reflects the nature, scale and complexity of the business of theCompany and risks to which it is exposed. The Policy shall also provide guidance with respect to the prevention, detection, mitigation and investigation into fraudulent activities under NPS architecture.

1.2 Objective

The Policy is established to detect, monitor, mitigate and report occurrence of fraud under NPS architecture to the Board of the Company, Law enforcement Agencies and Authority. It would facilitate development of processes to prevent, detect and contain frauds. Further it will also ensure development of control measures at an organizational level and conducting investigations. and frauds. The company is committed to conducting business in an environment of fairness and integrity and will strive to protect itself from any fraud emanating from its operations.

The Company adopts a "Zero-Tolerance" approach to fraud and will not accept any dishonest or fraudulent act committed by internal / external stakeholders.

1.3 Applicability

This Policy applies to any fraud or suspected fraud involving employees and Director of the Company as well as shareholders, consultants, vendors, contractors, outside agencies doing business with the Company and/or any other parties having a business relationship with the Company including Agent/ Business Correspondent of the Company. The policy would also be applicable to NPS subscribers and beneficiaries and potential subscriber. Any investigation activity required will be conducted irrespective of the suspected wrongdoer's length of service, position/title, or relationship to the Company.

1.4 Review and approval of the policy

The policy will be reviewed by **Risk Management Committee of the Board** and will be recommended to the Board of Directors for approval, at least on an annual basis **or if any requirement is notified by the regulators, the policy shall be amended immediately to give the effect to that even before the due date of annual review.**

Risk Management Department and Fraud Monitoring Cell shall assist in the review process and recommend necessary changes in the policy. Policy may be reviewed based on the newly released changes to Acts, regulatory requirements, independent audits and/ or internal review.

2 Policy Requirements

2.1 Roles and Responsibilities

- **Board of Directors** – **The Board is responsible for approval of the policy, periodic review and ongoing monitoring of adherence to the Policy**. The Board may delegate this responsibility to the Risk Management Committee.
- **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 the first line of defence i.e. the concerned process owner / business / line function.
- **Second Line of Defence** – **The Compliance and Risk Management Department** are the second line of defence, who are responsible for reviewing and challenging the completenessand accuracy of the first line's risk identification, measurement, management, monitoring and reporting.
- **Third Line of Defence** – Audit is the third line of defence. The auditor is responsible for conducting an impartial evaluation of the efficacy of the fraud controls framework's design and operation. Their duty extends to communicating findings and apprehensions to both the Management and the Audit and Risk Committees of the Company.

Detailed roles and responsibility of various stakeholders is detailed in the Company's Fraud Response and Monitoring Procedures.

2.2 Procedures for Fraud Monitoring

The Company will have well defined procedures to identify, detect, investigate and report frauds. The Risk Management Department and Fraud Monitoring Cell will develop /manage systems & framework and analytical tool methodologies to identify potential fraud areas / red flags.

Through sampling methodology, the team will identify patterns / trends to review processes and will put in place preventive and corrective measures and report to the Managing Director / CEO which oversees the Fraud Monitoring functions. It also spreads awareness regarding fraud prevention across the Company to develop a culture of zero tolerance to fraud.

- The Chief Operating Officer (COO) is in-charge of centralized investigation. All incidents and complaints with suspected fraudulent activity are investigated and analysed. Queries are generated to initiate the investigation and post investigation conclusions after due validation of evidences are put up to the Disciplinary Authority for taking appropriate punitive action.

- All Functional Heads are primarily responsible for day to day management of activities and in charge of maintaining, implementing and improving their systems, processes & controls so that they minimize the possibility of frauds and on a timely basis mitigate the impact of an identified fraud.

- Heads of various departments of the Company and in-charge of branch office will submit a quarterly report regarding identification and reporting of fraud, if any, in their respective functional area/location.

2.3 Identification and reporting of Suspected/ Actual frauds

Any employee who suspects or detects dishonest or fraudulent activity should report through email or in writing immediately, in any case, within 48 hours of its detection. While the reporting can be done by any employee / person who suspects / detects the fraud, Head of the Department / Office / Branch is responsible to ensure that the fraud is reported within the aforesaid timelines. Complete information as available should be provided at the time of reporting.

In case the Department / Office has conducted a preliminary investigation of the fraud, the investigation report should be annexed at the time of incident reporting. If there is any doubt as to whether an action constitutes fraud, the Risk Management Department and Fraud Monitoring Cell may be contacted for guidance.

Employees and other individuals should not attempt to personally conduct investigations or interviews / interrogations related to any suspected fraudulent act.

Disciplinary action may be initiated against the employee(s) for not reporting or withholding information related to suspected or actual fraud.

The Company urges its intermediaries, vendors, subscribers, beneficiaries & all concerned to act in a lawful & proper manner and to report allegations or irregularities in respect of any fraud to the Organisation.

In case of any incident of fraud / possible attempt of fraud regarding SBI Pension Funds Private Limited is detected/observed, then it shall be reported via email/ or letter to the below mentioned:

SBI Pension Funds Private Limited
Risk Management and Fraud Monitoring Cell
1904, 19th Floor, Parinee Cresenzo,
G-Block, Bandra Kurla Complex (BKC),
Bandra East, Mumbai – 400 051.
Email: risk@sbipensionfunds.com

2.4 Security to individuals who report fraud

The Company actively promotes a culture of reporting fraudulent activities, emphasizing the importance of individuals coming forward. It unequivocally denounces any form of unfair treatment and is committed to safeguarding individuals who, in good faith, report suspected incidents of fraud, ensuring they face no repercussions.

However, any abuse of this protection (e.g. any false or bogus allegations made by an individual knowing them to be false or bogus or with a mala fide intention) will warrant action as deemed necessary by the Company.

2.5 Confidentiality

All fraud investigations and related information will be treated confidentially. Investigation results *will not be disclosed or discussed* with anyone other than those against whom investigation is done and to the management.

2.6 Fraud Response and Monitoring Procedures

The Company ensures that all suspected / actual fraud incidents are investigated, the root cause is analyzed, appropriate action as per disciplinary matrix is taken, and mitigating controls are implemented to avoid recurrence of such incidents in future.

The Company has defined a detailed 'Fraud Response and Monitoring Procedures' which details procedures and approach to be taken to handle cases of frauds whether internal or external and both confirmed or suspected.

2.7 Disciplinary Measures

Based on the investigation findings, staff accountability and complicity disciplinary measures will be decided. Efforts will be made to recover the loss amount fully. Based on the nature of the fraud, an internal Committee may decide on suitable penal action as per the grid defined or pursue the matter with other law enforcement agencies for appropriate action against the concerned person(s).

2.8 Coordination with Law Enforcement Agencies

The Company may coordinate with various law enforcement agencies for fraud reporting on timely and expeditious basis and follow-up processes thereon. Reporting to CBI / Police and other law enforcement agency will be done on case to case basis.

2.9 Loss Monitoring and Recovery

The Company shall keep a track of all losses to be recovered from the fraudsters and monitor the same periodically.

2.10 Framework for Exchange of Information

The Company may exchange requisite information on frauds with other pension funds through NPS Trust as and when required. The Company shall aid in setting up coordination platforms through Trust or any other Forum to establish information sharing mechanism.

2.11 Due Diligence

The Company should ensure that there are adequate procedures in place at various departments for carrying out due diligence on the various entities / people with whom the Company carries out its business before entering into agreement/ or their appointment, for e.g. Personnel, agent, business correspondent, intermediary, TPA, vendors / consultants, etc.

The Risk Department shall obtain confirmation from each and every department that due diligence process and procedures are in place.

2.12 Regular Communication Channels

Risk Management Department and Fraud Monitoring Cell shall generate fraud mitigation communication within the Company at periodic intervals or on adhoc basis, as may be required. It must also ensure information flow to concerned departments with respect to frauds.

2.13 Preventive Mechanism

The Company will inform stakeholders about its Anti Fraud Policy. The Company will incorporate necessary caution in the agreements /contracts / relevant documents duly highlighting the consequences of submitting a false statement and /or incomplete statement, for the benefit of subscribers, claimants and beneficiaries.The Company will proactively identify and monitor frauds on an ongoing basis.

2.14 Fraud Awareness

An ongoing awareness program is a key enabler to convey fraud risk management expectations, as well as an effective preventive measure. Awareness of fraud and misconduct schemes should be developed through periodic assessment, training, and frequent communication.

3 Exception handling

Any exception with respect to the Policy shall be reviewed by the Board. The exception request shall be submitted to the Risk Management Department and Fraud Monitoring Cell in the form of a Note addressing the Board with complete description of the said exception.

4 Reporting

Internal Reporting:

Fraud events are reported and presented at relevant Committees and to the Board of the Company held periodically. Such report should, among other things (statistics of fraud cases, summary on key cases identified, loss amount, resolution etc), take note of the failure on the part of the concerned officials and controlling authorities and give details of action initiated against the officials responsible for the fraud.

Concerned department is responsible for reporting of frauds in the format / template and within the timelines prescribed.

External Reporting:

The Company submits annual report on various fraudulent cases to PFRDA in forms FMR 1 – Details of actual and suspected fraud, FMR 2 – Details of outstanding fraud cases and FMR-3 – Details of closed fraud cases as required by the regulator.

In addition to the above, the Company shall adhere to any other requirements / directions for reporting of frauds as may be issued by PFRDA from time to time.

5 Record keeping

All fraud related information / documents shall be preserved for a period as specified in the applicable regulations or as defined in the Record Retention Policy of the Company.

6 Appendices

6.1 Definition of Fraud

As per PFRDA Circular No.PFRDA/2023/36/SUP-CGSG/01 on "Framework for Prevention and Reporting of Fraud under NPS Architechure" Guidelines dated 19th December 2023 "Fraud" means an act of commission or omission or distortion or any concealment of facts or suppression of information or practicing deception or any acts of undue influence, misrepresentation with a view to cause any unjust richment or gain to any person (whether monetary or otherwise) or any wrongful loss or any detriment fuffered by another, without there being any necessity to prove any such gain or loss.

This may, for example, be achieved by means of:

- Making of any statement or furnishing any document which he know or has reason to believe to be false or incorrect in any material particular.
- Omitting to state any material fact knowing it to be material.
- Willfully altering, suppressing or destroying any document which is required to be furnished.
- Any misrepresentation of the truth or concealment of material facts so as to induce the other person to act to his detriment;
- A promise or allurement made by a person without any intention of performing it.
- Any representations or warranties made, without due care and caution based on which another person acts or is likely to act or omits to act or is prevented from acting based on informed consent.
- Any acts of omission or commission classifiable as fraud under any other law in force, whether civil or criminal ramifications or both.
- Failure to segregate moneys of the client or use the client for self of for any other client.

6.2 Broad Categories of Fraud:

- **Subscribers Fraud and Claimant Fraud** – Fraud by the subscriber at the time of joining NPS Architecture, contribution to the Scheme including fraud at the time of exit, premature withdrawal and partial withdrawal including the frauds by the claimant in case of death claim settlement.
- **Intermediary / Entity Fraud** – Fraud perpetuated by an intermediary / Agent / Business Correspondent under the NPS system/ or by subscriber/ potential subscriber.
- **Internal Fraud** – Fraud/ misappropriation against the intermediary/ by Director, Key Personnel and / or any other officer or staff members.
- **Digital Fraud** – spam, scams, spyware, identity theft, password theft, phishing, or internet banking fraud.

6.3 Related Policies and Procedures

This policy should be read in conjunction with the following Policies and Procedures:

- Anti-Money Laundering Policy;
- Whistle-blower Policy;
- Risk Management Policy;
- HR Policy; and
- **Fraud Response, Monitoring and Reporting Procedures.**

6.4 List of Abbreviations used in the policy

- CBI - Central Bureau of Investigation
- PFRDA - Pension Funds Regulatory and Development Authority
- RMC - Risk Management Committee