
	<p>रक्षा लेखा प्रधान नियंत्रक, सेना सैक्टर 9, चण्डीगढ़ - 160009</p> <p><b>PRINCIPAL CONTROLLER OF DEFENCE ACCOUNTS (Army), Chandigarh</b> Sector-9, Chandigarh-160009</p> <p>Ph: EPABX Nos: 2741611-614, 2741990, 2740445 Ext .260,263 Fax- 2742552 E-mail: npscell.pcdawc@nic.in Website : pcdawc.gov.in</p>	 <p>INTERNATIONAL YEAR OF <b>MILLETS</b> 2023</p>
---	---	--

FC/11/CHD/NPS/Circular/Vol-II/32/23-24

Dated : 02/02/2024

To

The Officer in Charge

1. AAO (Pay), Jalandhar Cantt
2. PAO (ORs) 14 GTC, Subathu
3. Pay Section (Local)
4. AN Pay (Local)
5. All AOGes under PCDA (Army) Chandigarh

**Subject:- Prevention and reporting of fraud under NPS Architecture for Govt. sector and its implementation.**

A copy of PFRDA letter No. PFRDA-09/01/0003/2023-SUP-SG dated 2.12.2023 on the subject mentioned above is enclosed herewith for information and compliance please.

PCDA has seen.

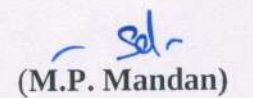


(M.P. Mandan)

Asst. Controller

Copy to

<p>The OI/C IT &amp; S Section (Local)</p>	<p>For uploading on the WAN of PCDA (Army) Chandigarh</p>
--	---



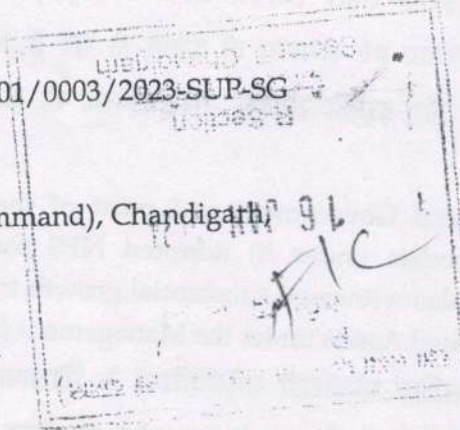
(M.P. Mandan)

Asst. Controller

File No. PFRDA-09/01/0003/2023-SUP-SG

Date: 20.12.2023

To,  
PCDA (Western Command), Chandigarh,  
Sector 9 C,  
Chandigarh,  
Chandigarh, 160009.



महोदय/महोदया,  
Dear Sir/Madam,

विषय: सरकारी क्षेत्र के लिए एनपीएस आर्किटेक्चर के तहत धोखाधड़ी की रोकथाम और रिपोर्टिंग के लिए एक नीति तैयार करने और इसके कार्यान्वयन के लिए अनुरोध।

Subject: Request for framing a policy for Prevention and Reporting of Fraud Under NPS Architecture for Government Sector and its implementation.

आपको ज्ञात ही होगा कि, 1 जनवरी 2004 को या उसके बाद सेवाओं में शामिल होने वाले केंद्र सरकार के कर्मचारियों (सशस्त्र बलों को छोड़कर) के लिए एनपीएस अनिवार्य है। इसके बाद, अधिकांश राज्य सरकारों ने भी अपने कर्मचारियों के लिए अलग-अलग तिथियों पर एनपीएस को अपनाया है।

You may be aware that, the NPS is mandatory for Central Government employees (except armed forces) joining services on or after 1st January 2004. Subsequently, most of the State Governments have also adopted NPS at different dates for their employees.

2. डीओपी/पीडब्ल्यू द्वारा 30.03.2021 को अधिसूचित केंद्रीय सिविल सेवा (राष्ट्रीय पेंशन प्रणाली का कार्यान्वयन) नियम, 2021 में एनपीएस आर्किटेक्चर के तहत नोडल कार्यालयों की विशिष्ट भूमिकाओं और जिम्मेदारियों का प्रावधान है, जिसमें किसी भी विचलन के मामले में दंड प्रावधान भी शामिल हैं।

The Central Civil Services (Implementation of National Pension System) Rules, 2021 notified on 30.03.2021 by DoP&PW, provides for specific roles and responsibilities of nodal offices under the NPS architecture, including the penal provisions, in case of any deviation.

3. केंद्र सरकार और अधिकांश राज्य सरकारों (इसके तहत स्वायत्त निकायों सहित) ने अपने अंतर्निहित कर्मचारियों के लिए एनपीएस को अपनाए हुए लगभग दो दशक हो गए हैं और इस क्षेत्र ने प्रबंधन (एयूएम) के तहत अभिदाताओं और इसकी संबद्ध परिसंपत्तियों की संख्या के संदर्भ में भी पर्याप्त वृद्धि देखी है।

It is almost two decades since the Central Government and most of the State Governments (including Autonomous bodies under it) adopted NPS for their underlying employees and the sector has also witnessed substantial growth in terms of the number of Subscribers and its associated Assets under the Management (AUM).

4. अभिदाताओं का कोष भी बढ़ गया है और इसलिए धोखाधड़ी गतिविधियों के खिलाफ अधिक सतर्कता की आवश्यकता है। धोखाधड़ी की गतिविधियों में धन के दुरुपयोग से लेकर पहचान की चोरी और व्यक्तिगत एनपीएस खातों तक अनधिकृत पहुंच तक पहुंच शामिल हो सकती है। इन कार्यों से अभिदाताओं और पेंशन प्रणाली दोनों के लिए गंभीर वित्तीय नुकसान हो सकता है।

The corpus of individuals has also grown and hence the need for greater vigilance against fraudulent activities. Fraudulent activities can range from misappropriation of funds to identity theft and unauthorized access to individual NPS accounts. These actions can lead to severe financial losses for both individuals and the pension system as a whole.

5. इन जोखिमों से निपटने और एनपीएस की अखंडता को बनाए रखने के लिए, केंद्र/राज्य सरकार के नोडल कार्यालयों (इसके तहत स्वायत्त निकायों सहित) के लिए "एनपीएस आर्किटेक्चर के तहत धोखाधड़ी की रोकथाम और रिपोर्टिंग के लिए रूपरेखा" की स्थापना की तत्काल आवश्यकता है।

To address these risks and uphold the integrity of the NPS, there is an urgent necessity for the establishment of the "Framework for Prevention and Reporting of Fraud Under NPS Architecture" for Nodal offices of Central/State Government (including autonomous bodies under it).

6. उपर्युक्त को ध्यान में रखते हुए, आपसे अनुरोध है कि सरकारी क्षेत्र के लिए एनपीएस संरचना के तहत धोखाधड़ी की रोकथाम और रिपोर्टिंग के लिए एक नीति तैयार करने और इसके कार्यान्वयन के लिए अपने संबंधित प्रशासनिक विभाग/मंत्रालय के साथ मामले की जांच करें और इसे उठाएं।

In view of the above, you are hereby requested to examine and take up the matter with your concerned Administrative Department/Ministry for framing a policy for the Prevention and Reporting of Fraud Under NPS Architecture for the Government Sector and its implementation.

7. उपर्युक्त "धोखाधड़ी विरोधी नीति" का उद्देश्य आपके प्रशासनिक नियंत्रण कार्यालयों, कानून प्रवर्तन एजेंसियों और प्राधिकरण को धोखाधड़ी की रोकथाम और रिपोर्टिंग के उपायों के रूप में दिशानिर्देश निर्धारित करना है। इस ढांचे का उद्देश्य अन्य बातों के साथ-साथ निम्नलिखित को प्राप्त करना होगा:

The objective of the above-mentioned "Anti-fraud Policy" is to set guidelines as measures of prevention and reporting of fraud to your administrative controlling offices, Law enforcement Agencies, and Authority. The framework shall *interalia* aims to achieve the following:

- I. धोखाधड़ी की रोकथाम: धोखाधड़ी को स्पष्ट रूप से पहचानने और इकाई के भीतर धोखाधड़ी के जोखिम को कम करने के लिए तेज और प्रभावी तंत्र को लागू करने के लिए तंत्र विकसित करना। इसमें आंतरिक रूप से धोखाधड़ी की रोकथाम की एक मजबूत संस्कृति को बढ़ावा देना, मजबूत नियंत्रण लागू करना और सभी हितधारकों के बीच जागरूकता बढ़ाना शामिल है।

Fraud Prevention: Evolve mechanisms to clearly Identify fraud and implement swift and effective mechanisms to mitigate the risk of fraud within the entity. This involves internally promoting a strong culture of fraud prevention, implementing robust controls, and raising awareness among all stakeholders.

- II. समय पर पता लगाना: इकाई के भीतर धोखाधड़ी गतिविधियों का जल्दी पता लगाने की सुविधा के लिए निगरानी, डेटा एनालिटिक्स और रिपोर्टिंग तंत्र को बढ़ाएं।

Timely Detection: Enhance monitoring, data analytics, and reporting mechanisms to facilitate the early detection of fraudulent activities within the entity.

- III. अभिदाता संरक्षण: एनपीएस आर्किटेक्चर के भीतर, मध्यस्थों द्वारा उच्च नैतिक मानकों का पालन करना और अभिदाताओं के हितों की रक्षा करना सुनिश्चित करके अभिदाताओं और लाभार्थियों के हितों की रक्षा करना। इस उद्देश्य का उद्देश्य अभिदाताओं के विश्वास को बढ़ाना और अखंडता बनाए रखना है। इसके अलावा, धोखाधड़ी के व्यापक प्रभाव को रोकने के लिए तत्काल उपाय किए जाने चाहिए ताकि एक बार इसका पता चलने के बाद और अधिक निगरानी हानि को रोका जा सके।

Subscriber Protection: Safeguard the interests of subscribers and beneficiaries by ensuring that intermediaries within the NPS Architecture adhere to high ethical standards and diligently protect the interest of the subscriber. This objective aims to enhance subscriber confidence and maintain integrity. Further, immediate measures are to be taken to stop the cascading impact of fraud to contain further monetary loss, once it is detected.

IV. वसूली और क्षतिपूर्ति: धोखाधड़ी के कारण होने वाले मौद्रिक नुकसान की वसूली के लिए प्रावधान स्थापित करना और प्रभावित पक्षों को क्षतिपूर्ति करने का प्रावधान करना।  
Recovery and indemnification: To establish provisions to recover the monetary loss caused on account of fraud and provision for indemnifying the affected parties.

V. नियामक अनुपालन: पीएफआरडीए अधिनियम 2013 के प्रावधानों, समय-समय पर प्राधिकरण द्वारा जारी नियमों, विनियमों और दिशानिर्देशों के अनुपालन को बढ़ावा देना। इसका उद्देश्य यह सुनिश्चित करना है कि प्रणाली के भीतर काम करने वाली सभी संस्थाएं धोखाधड़ी से प्रभावी ढंग से निपटने में अपने दायित्वों और जिम्मेदारियों को पूरा करती हैं।

Regulatory Compliance: Promote compliance with provisions of the PFRDA Act 2013, rules, regulations, and guidelines issued by the Authority from time to time. The objective is to ensure that all entities operating within the system fulfil their obligations and responsibilities in effectively combating fraud.

VI. निरंतर सुधार: धोखाधड़ी जोखिमों, तकनीकी प्रगति और उभरते उद्योग प्रथाओं के जवाब में ढांचे की नियमित रूप से समीक्षा और अद्यतन करके निरंतर सुधार की संस्कृति को बढ़ावा देना।

Continuous Improvement: Foster a culture of continuous improvement by regularly reviewing and updating the framework in response to evolving fraud risks, technological advancements, and emerging industry practices.

VII. धोखाधड़ी की रिपोर्टिंग: पता लगाने के बाद धोखाधड़ी को आपके प्रशासनिक नियंत्रण कार्यालयों, कानून प्रवर्तन एजेंसियों और "प्राधिकरण के निगरानी और जांच विभाग" को सूचित किया जाना है। इस संबंध में, पीएफआरडीए को धोखाधड़ी की सूचना देने के लिए विचारोत्तेजक प्रारूप और औचित्य नीचे दिए गए हैं।

एसएल	रिपोर्ट का विशेष आवृत्ति	प्रारूप
1	वास्तविक और संदिग्ध धोखाधड़ी का पता चलने के 3 सप्ताह के भीतर धोखाधड़ी का विवरण (एफएमआर 1)	अनुलग्नक-I
2	बकाया धोखाधड़ी के हर साल वित्तीय वर्ष की समाप्ति के 30 दिनों के भीतर मामलों का विवरण (एफएमआर 2)	अनुलग्नक-II

92

3	बंद धोखाधड़ी के हर साल वित्तीय वर्ष की एनेक्शन-III मामलों का विवरण समाप्ति के 30 दिनों के भीतर (एफएमआर 3)
---	---

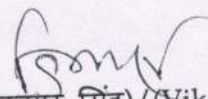
Reporting of Fraud: The fraud after detection is to be reported to your administrative controlling offices, Law enforcement Agencies, and "The Surveillance and Investigation Department of Authority. In this regard, the suggestive format and frequency for reporting fraud to PFRDA are as below.

SL	Particular of Reports	Frequency	Format
1	Details of actual and suspected fraud (FMR 1)	within 3 weeks of the detection of fraud	Annexure-I
2	Details of outstanding fraud cases (FMR 2)	of every year within 30 days of the close of the financial year	Annexure-II
3	Details of closed fraud cases (FMR 3)	every year within 30 days of the close of the financial year	Annexure-III

8. पीएफआरडीए के तहत मध्यस्थों के लिए धोखाधड़ी जोखिम प्रबंधन नीति की एक प्रति (हिंदी और अंग्रेजी में) पीएफआरडीए वेबसाइट पर उपलब्ध है तथा इसका अंग्रेजी संस्करण तत्काल संदर्भ के लिए संलग्न है। यदि आवश्यक हो तो हमें कोई स्पष्टीकरण प्रदान करने में खुशी होगी।

A copy of the Fraud Risk management Policy for Intermediaries (in Hindi and English) is available on PFRDA website and English version of the same is attached herewith for ready reference please. We would be glad to provide any clarification, if required.

सादर,  
Yours sincerely,

  
(विकास कुमार सिंह) / (Vikas Kumar Singh)  
मुख्य महाप्रबंधक / Chief General Manager

**PENSION FUND  
REGULATORY AND  
DEVELOPMENT  
AUTHORITY**

(FRAMEWORK FOR PREVENTION AND  
REPORTING OF FRAUD UNDER NPS  
ARCHITECTURE) GUIDELINES, 2023

PFRDA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS ARCHITECTURE) GUIDELINES, 2023

Contents	
CHAPTER- I- SHORT TITLE, COMMENCEMENT, OBJECTIVE AND APPLICABILITY	2
1. Short title and commencement	2
2. Objective	2
3. Applicability	3
CHAPTER-II-DEFINITION AND CLASSIFICATION	3
4. Definition	3
5. Classification of Fraud	4
CHAPTER-III-GENERAL DIRECTION	4
6. General Direction	4
CHAPTER-IV- OBLIGATIONS OF THE ENTITIES UNDER NPS ARCHITECTURE AND ESTABLISHMENT OF AN ANTI-FRAUD POLICY	5
7. Obligations of the entities under NPS architecture	5
8. Establishment of an Anti-Fraud Policy	6
CHAPTER-V- REPORTING PROCESS	8
9. Reporting Process of Financial Fraud to Law Enforcement Agencies	8
CHAPTER-VI -FRAUD MONITORING REPORTS	9
10. Fraud Monitoring Reports ("FMR") to Authority	9
11. Reports to the Board of the entity	9
12. Delays in Reporting of Frauds	9
CHAPTER-VIII-ANNEXURES	10
Annexure-I- FRAUD MONITORING REPORT-1 (FMR 1)	10
Annexure-II- FRAUD MONITORING REPORT-2 (FMR 2)	12
Annexure-III- FRAUD MONITORING REPORT-3 (FMR 3)	14



PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY  
(FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS  
ARCHITECTURE) GUIDELINES, 2023

CHAPTER- I- SHORT TITLE, COMMENCEMENT, OBJECTIVE AND  
APPLICABILITY

1. Short title and commencement.

- 1.1. These guidelines may be called the Pension Fund Regulatory and Development Authority (Framework for Prevention and Reporting of Fraud Under NPS Architecture) Guidelines, 2023.
- 1.2. The guidelines are issued under section 14 of the Pension Fund Regulatory and Development Authority Act 2013 ("PFRDA Act 2013").
- 1.3. These guidelines shall come into effect on the day, they are placed on the official website of the Pension Fund Regulatory and Development Authority ("PFRDA" or "Authority").
- 1.4. These guidelines are to be construed and acted upon, together with any other guidelines on fraud prevention, as may be applicable in the organization or which it is obliged to follow.

2. Objective:

The objective of the " Framework for Prevention and Reporting of Fraud Under NPS Architecture Guidelines" is to suggest a set of guidelines and measures for the prevention and reporting of fraud to the Board of the entity, Law enforcement Agencies, and Authority. These guidelines are not exhaustive on the subject and every care should be taken by entities under NPS architecture to evolve best practices to detect, prevent, and contain fraud. The framework *interalia* aims to achieve the following objectives:

- 2.1. Fraud Prevention: Evolve mechanisms to clearly Identify fraud and implement swift and effective mechanisms to mitigate the risk of fraud within the entity. This involves internally promoting a strong culture of fraud prevention, implementing robust controls, and raising awareness among all stakeholders.
- 2.2. Timely Detection: Enhance monitoring, data analytics, and reporting mechanisms to facilitate the early detection of fraudulent activities within the entity.
- 2.3. Subscriber Protection: Safeguard the interests of subscribers and beneficiaries by ensuring that intermediaries within the NPS Architecture adhere to high ethical standards and diligently protect interest of subscriber. This objective aims to enhance subscriber confidence and maintain the integrity.
- 2.4. Regulatory Compliance: Promote compliance with provisions of the PFRDA Act 2013, rules, regulations, guidelines issued by Authority on time to time. The objective is to ensure that all entities operating within the system fulfil their obligations and responsibilities in effectively combating fraud.

## PFRDA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS ARCHITECTURE) GUIDELINES, 2023

2.5. Continuous Improvement: Foster a culture of continuous improvement by regularly reviewing and updating the framework in response to evolving fraud risks, technological advancements, and emerging industry practices.

### 3. Applicability

These guidelines shall apply to all intermediaries registered with the Authority or any entity associated with such intermediaries in relation to any activity under NPS, besides other entities empanelled with the Authority (hereinafter referred to as "the entities/entities/entities under NPS architecture"). These guidelines shall be applicable in respect of all the schemes regulated and administered by PFRDA.

## CHAPTER-II-DEFINITION AND CLASSIFICATION

### 4. Definition of Fraud

4.1. "Fraud" shall include any act of commission or omission or distortion or any concealment of facts or suppression of information or practising deception or any acts of undue influence, misrepresentation with a view to cause any unjust enrichment or gain to any person (whether monetary or otherwise) or any wrongful loss or any detriment suffered by another, without there being any necessity to prove any such gain or loss. Some of the instances of fraud shall include whether in a deceitful manner –

- Making of any statement or furnishing any document which he knows 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.
- wilfully 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 having civil or criminal ramifications or both.;
- Failure to segregate moneys of the client or use the client for self of for any other client

4.2. There shall be no requirement of proving any financial or non-financial harm or loss having been caused to any person, under these guidelines, on account of any fraudulent activity.

## 5. Classification of Fraud

A list of acts/conduct which may be classifiable as fraud is listed below which is not exhaustive but only illustrative: -

- Breach of trust
- Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts.
- Cheating and forgery.
- Embezzlement or Misappropriation of funds, securities, supplies, or other assets
- Forgery or alteration of any document, record, or account or any destruction of documents
- Forgery or alteration of a cheque, bank draft, account, or any other financial instrument
- Incorrect financial reporting with a view to deceive
- Mis-utilization of office funds for personal purposes
- Unauthorised destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment;
- Making false written or oral statements or representations with respect to organisation activities
- Impropriety in the handling or reporting of money or financial transactions
- Profiteering as a result of insider knowledge of the organisation's activities
- Disclosing confidential and proprietary information to unauthorised parties
- Bribery or kickbacks
- Wilful suppression of facts/deception in matters of appointment; placements; submission of reports
- Omitting to give true and correct information of a material nature
- Any other type of fraud not coming under the specific heads as above

## CHAPTER-III-GENERAL DIRECTION

### 6. General Direction

6.1. The Managing Director/Chief Executive Officer (MD/CEOs) of intermediaries shall have the obligation to lay down a policy to deal with fraud and its prevention and reporting in accordance with these guidelines -

6.1.1. To provide focus on the prevention and reporting of fraud to the Board of the entity, Law enforcement Agencies, and Authority.

## PFRDA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS ARCHITECTURE) GUIDELINES, 2023

- 6.1.2. To frame an Anti-Fraud Policy for fraud risk management and investigation.
- 6.1.3. To clearly demarcate the functions, roles and responsibilities of each employee.
- 6.2. Also, in order to adequately protect itself from the financial and reputational risks posed by frauds, the entities under NPS architecture shall have in place an appropriate framework to detect, monitor, and mitigate the occurrence of such frauds within their organization. The said framework shall, *inter-alia* include measures to protect the entity from the threats posed by the following broad categories of fraud:
  - 6.2.1. 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.
  - 6.2.2. Intermediary/ Entity fraud - Fraud perpetuated by an intermediary / Agent/ Business Correspondent under the NPS System/or by subscriber/ potential subscriber.
  - 6.2.3. Internal Fraud – Fraud/misappropriation against the intermediary/ by its Director, Key Personnel and /or, any other officer or staff member.
  - 6.2.4. Digital fraud - spam, scams, spyware, identity theft, password theft, phishing, or internet banking fraud.

### CHAPTER-IV- OBLIGATIONS OF THE ENTITIES UNDER NPS ARCHITECTURE AND ESTABLISHMENT OF AN ANTI-FRAUD POLICY

7. Obligations of the entities under NPS architecture:
  - 7.1. Compliance with the regulatory norms: The entities under NPS architecture shall comply with all applicable laws, and provisions of the PFRDA Act 2013, including rules, regulations, and guidelines issued thereunder, at all times. Further, these guidelines shall also be part of regulatory compliance and its reporting by the entities under NPS architecture.
  - 7.2. Risk Assessment: The entities under NPS architecture are required to conduct periodic regular risk assessments to identify potential areas of vulnerability to financial fraud. These assessments should evaluate internal control systems, operational processes, customer due diligence, and transaction monitoring capabilities.
  - 7.3. Internal Procedures: The entities under NPS architecture must establish and maintain internal procedures to prevent financial fraud. These should include but are not limited to:

- 7.3.1. Fraud Prevention Measures: Implementing controls, checks, and balances to mitigate fraud risks across all business functions and operations related to NPS.
  - 7.3.2. Know Your Customer (KYC) and Subscriber Due Diligence (SDD): Conduct thorough customer due diligence, verify customer identities, and implement ongoing monitoring measures to detect and prevent fraudulent activities.
  - 7.3.3. Reporting Suspicious Activities: Establish mechanisms for employees to report suspicious activities internally.
  - 7.3.4. Training and Awareness: Regular training programs to enhance employees' awareness about financial fraud risks, prevention measures, and reporting obligations to foster a culture of integrity and ethical behavior within the organization.
  - 7.3.5. Whistle-blower Protection: Implement a whistle-blower protection framework that encourages employees to report potential financial fraud without fear of retaliation.
  - 7.3.6. Incident Response and Investigation: Develop protocols for handling and investigating suspected financial fraud incidents promptly and thoroughly.
  - 7.3.7. Surveillance and Monitoring: Implement surveillance and monitoring systems to identify unusual patterns, suspicious transactions, or red flags indicative of financial fraud.
  - 7.3.8. Policy for Identification: To have a policy for identification of sensitive functions and rotate officials performing such functions.
  - 7.3.9. Reporting: Timely reporting mechanism (both in-house and to external agencies) upon detection of fraud and for taking immediate measures to mitigate harm/loss caused.
  - 7.3.10. Periodic Review: Review of fraud detection and prevention mechanism periodically and report to the Board of the organisation about the same.
8. Establishment of an Anti-Fraud Policy
- 8.1. The entities under NPS architecture, subject to Board approval to establish an Anti-Fraud Policy for fraud risk management and investigation. This policy should adhere to governance standards and accountability, and consider the organization's structure, services, and technology. A comprehensive approach is to be adopted to identify, measure, control, and monitor fraud risk, with tailored risk management policies and procedures across the organization.
  - 8.2 Key components of the Anti-Fraud Policy shall be as under
    - 8.2.1. Policy Statement:
      - Clearly define the organization's commitment to preventing, detecting, and combating fraud.
      - Outline the purpose and objectives of the anti-fraud policy.

PFRDA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS ARCHITECTURE) GUIDELINES, 2023

- Emphasize the organization's zero-tolerance approach towards fraud.
- 8.2.2. Risk Assessment
- Identify and assess potential fraud risks specific to organization's area of activities/ functions
  - Evaluate internal and external factors that may contribute to fraud, such as operational processes, system - hardware and software, people, procedure, customer interactions, and regulatory compliance.
- 8.2.3. Detection Mechanisms:
- Implement robust monitoring and detection systems to identify suspicious activities and anomalies in transactions, account behavior, or customer interactions.
  - Conduct periodic audits and reviews to assess the effectiveness of controls and identify potential vulnerabilities.
  - Establish clear escalation procedures for reporting and investigating suspected fraud cases.
- 8.2.4. Prevention Measures:
- Establish internal controls and procedures to deter fraud, including segregation of duties, access controls, and authorization protocols
  - Provision for regular employee training programs to raise awareness of fraud risks and provide guidance on fraud prevention techniques
  - Promote a strong ethical culture within the organization to discourage fraudulent behavior.
  - Encourage anonymous reporting channels for employees to report suspected fraudulent activities.
  - To take immediate measures to stop the cascading impact of fraud to contain further monetary loss, once it is detected.
- 8.2.5. Co-ordination with Law Enforcement Agencies
- Lay down procedures to coordinate with law enforcement agencies for reporting frauds on a timely and expeditious basis and
  - follow-up processes thereon.
- 8.2.6. Reporting and Communication:
- Establish a reporting framework to document and communicate fraud incidents internally and, if required, externally
  - Develop protocols for timely reporting of suspected fraud to management, stakeholders, and regulatory authorities, as mandated by applicable laws and regulations.

PFRDA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS ARCHITECTURE) GUIDELINES, 2023

- Maintain confidentiality and privacy of sensitive information throughout the reporting and communication process.
- 8.2.7. Recovery and indemnification:
- To establish provisions to recover the monetary loss caused on account of fraud and provision for indemnifying the affected parties.
  - To establish provisions in public interest to ensure that the suitable action is taken against the guilty persons, apart from recovery of the amount involved.
- 8.2.8. Review and Continuous Improvement:
- Regularly review and update the anti-fraud policy to align with changing fraud risks, industry best practices, and regulatory requirements.
  - Conduct periodic assessments of the policy's effectiveness and make necessary improvements based on lessons learned from fraud incidents.
  - The Board shall review the Anti-Fraud Policy on at least an annual basis and at such other intervals as it may be considered necessary.

#### CHAPTER-V- REPORTING PROCESS

#### 9. Reporting Process of Financial Fraud to Law Enforcement Agencies

To effectively report financial fraud to law enforcement agencies, the following steps may be followed:

- 9.1. **Recognizing and Documenting Fraud:** The first step in reporting financial fraud is to recognize the signs of fraudulent activity. This may include unauthorized transactions, identity theft, money laundering, or other fraudulent practices. Once you suspect financial fraud, it is crucial to document all relevant details, including dates, times, amounts involved, and any supporting evidence such as bank statements, emails, or communication records.
- 9.2. **Internal Reporting:** Individuals who become aware of financial fraud should report it to the designated authority within their organization, as per anti-fraud policy.
- 9.3. **Reporting to Authority:** The fraud detection may immediately be reported to Surveillance and Investigation Department of the Authority followed by detailed reports as prescribed under Fraud Monitoring Reports-1(FMR-1) to it also.
- 9.4. **Contacting the Law and Enforcement Agencies/ Local Police Station:** To report financial fraud by the entity as per the prescribed parameters of an anti-fraud policy of organisation to enforcement agencies/local police stations and provide them with a clear and comprehensive account of the fraudulent activities, including all the documented evidence to help them better understand the nature of the fraud and initiate an investigation.

PFRDA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS ARCHITECTURE) GUIDELINES, 2023

9.5. **Seeking Legal Advice:** It may be prudent to seek legal advice for guidance for the legal process to protect the rights, and advise on how to navigate the complexities of the case. This may also help in proceedings.

CHAPTER-VI -FRAUD MONITORING REPORTS

10. Fraud Monitoring Reports ("FMR") to Authority

10.1. The Managing Director/Chief Executive Officer (MD/CEOs) of intermediaries shall have the obligation to submit all the returns referred to in this document.

10.2. The fraud monitoring report containing information on fraudulent cases that come to light and action taken thereon are to be submitted to the Authority in the prescribed format under as per below categories and frequencies:

SL	Particular of Reports	Frequency	Format
1	Details of actual and suspected fraud (FMR 1)	within 3 weeks of the detection of fraud	Annexure-I
2	Details of outstanding fraud cases (FMR 2)	every year within 30 days of the close of the financial year	Annexure-II
3	Details of closed fraud cases (FMR 3)	every year within 30 days of the close of the financial year	Annexure-III

11. Reports to the Board of the entity:

The entities under NPS architecture to ensure that all frauds are reported promptly to its Board. Such reports should, among other things, 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.

12. Delays in Reporting of Frauds

The entities under NPS architecture should ensure that the reporting system is suitably streamlined so that delays in reporting of frauds, and submission of delayed and incomplete fraud reports are avoided. The entities under NPS architecture must fix staff accountability in respect of delays in reporting fraud cases to the Authority.



CHAPTER-VIII-ANNEXURES  
Annexure-I- FRAUD MONITORING REPORT-1 (FMR 1)  
(Details of actual and suspected fraud)

1	Details of the Entity	
(a)	Name of the Office/ Branch	
(b)	Branch type	
(c)	Place	
(d)	District	
(e)	State	
2	Details of Subscriber/Prospective Subscriber	
(a)	Name of the Subscriber	
(b)	Permanent Retirement Account Number (PRAN)/ Application No.	
(c)	Area of operation where the fraud has occurred	
3	Details about fraud	
(a)	Nature of Fraud	
(b)	Whether the computer is used in committing the fraud?	
(c)	The total amount involved (in Rs.)	
(d)	Date of occurrence	
(e)	Date of Detection	
(f)	Reasons for delay, if any, in detecting the fraud	
(g)	Brief history	
(h)	Modus operandi	
4	Fraud committed by	
(a)	Employee/Staff	(Yes/No)
(b)	Subscriber	(Yes/No)
(c)	Outsiders	(Yes/No)
5	Other details	
(a)	Whether internal inspection/ audit was conducted during the period between the date of the first occurrence of the fraud and its detection?	(Yes/No)
(b)	If yes, why the fraud could not have been detected during such an inspection/audit?	
(c)	What action has been taken for non-detection of the fraud during such inspection/audit	

PFRDA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS ARCHITECTURE) GUIDELINES, 2023

6	Details about action taken/proposed to be taken	
(a)	Whether any complaint has been lodged with the Police/CBI?	(Yes/No)
(b)	If yes, name of office/ branch of CBI/ Police	
(c)	Date of reference	
(d)	The present position of the case	
(e)	Date of completion of Police/CBI investigation	
(f)	Date of submission of the investigation report by Police/CBI	
(g)	If not reported to Police/CBI, the reasons therefor	
7	Details of staff-side action	
(a)	Whether any internal investigation has been/is proposed to be conducted	(Yes/No)
(b)	If yes, the date of completion	
(c)	Whether any departmental enquiry has been/is proposed to be conducted	(Yes/No)
(d)	If yes, give details as per the format given below:	
(e)	If not, reasons therefor	
8	Steps were taken/proposed to be taken to avoid such incidents	
(a)	Total amount recovered	
(b)	Amount recovered /parties concerned	
(c)	From other sources	
(d)	Extent of loss	
(e)	Amount written off	
9	Suggestions for Consideration of Authority	

Format for Staff-side action

No.	Name	Designation	Whether suspended/Dt. of suspension	Date of issuance of charge sheet	Date of commencement of the domestic inquiry	Date of completion of inquiry	Date of issuance of final orders	Punishment awarded	Details of prosecution/ conviction/ acquittal, etc.

PFDA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS ARCHITECTURE) GUIDELINES, 2023

Annexure-II- FRAUD MONITORING REPORT-2 (FMR 2)  
(Details of outstanding fraud cases)

Name of entity:

Report for the year ending :

Part I

Frauds Outstanding

Sl. No.	Description of Fraud	Unresolved Cases at the beginning of the year		New cases detected during the year		Cases closed during the year		Unresolved Cases at the end of the year	
		No.	Amount involved	No.	Amount involved	No.	Amount involved	No.	Amount involved
	Total								

Part II

Statistical details: (unresolved cases as of the end of the year)

Sl. No.	Description of Fraud	No. of Cases	Amount involved
	Total		

Part III

Preventive and Corrective steps taken during the year

Sl.No.	Description of the fraud	Preventive/Corrective action taken

PFRA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NIS ARCHITECTURE) GUIDELINES, 2023

Part IV

Cases Reported to Law Enforcement Agencies

Sl. No.	Description	Unresolved Cases at the beginning of the year		New cases reported during the year		Cases closed during the year		Unresolved cases at the end of the year	
		No.	Rs. in lakh	No.	Rs. in lakh	No.	Rs. in lakh	No.	Rs. in lakh
1	Cases reported to Police								
2	Cases reported to CBI								
3	Cases reported to Other agencies (specify)								
	Total								

CERTIFICATION

Certified that the details given above are correct and complete to the best of my knowledge and belief and nothing has been concealed or suppressed.

Date:

Place:

Signed/-

Annexure-III- FRAUD MONITORING REPORT-3 (FMR 3)  
(Details of closed fraud cases)

Fraud Cases closed during the year:

Name of the Entity:

Report for the year:

SL No.	Basis of closing a case	Number of cases closed#
1.	The fraud cases pending with CBI/Police/Court were finally disposed of	
2.	The examination of staff accountability has been completed.	
3.	The amount involved in the fraud has been recovered.	
4.	The amount paid back to the affected subscriber.	
5.	The entity has reviewed the systems and procedures; identified the causative factors; has plugged the lacunae; and the portion has been taken note of by the appropriate authority of the entity (Board, Committee thereof)	
6.	The entity is pursuing vigorously CBI for the final disposal of pending fraud cases, and staff side action is completed. The entity is vigorously following up with the police authorities and/or court for final disposal of fraud cases	
7.	Fraud cases where:  The investigation is on or challan/ charge sheet not filed in the Court for more than three years from the date of filing of the First Information Report (FIR) by the CBI/Police; or  Trial in the courts, after filing of charge sheet/challan by CBI / Police has not started or is in progress	

CERTIFICATION

Certified that the details given above are correct and complete to the best of my knowledge and belief and nothing has been concealed or suppressed.

Date:

Place:

Signed/-

PFRDA (FRAMEWORK FOR PREVENTION AND REPORTING OF FRAUD UNDER NPS ARCHITECTURE) GUIDELINES, 2023

Note: # Closure of Fraud Cases:

For reporting purposes, the entity should report only such cases as closed where the actions as stated below are complete.

1. The fraud cases pending with CBI/Police/Court are finally disposed of.
2. The examination of staff accountability has been completed
3. The amount of fraud has been recovered.
4. The entity has reviewed the systems and procedures, identified the causative factors, and plugged the lacunae and the fact of which has been taken note of by the appropriate authority (Board / Audit Committee of the Board)

Entities should also pursue vigorously with CBI for final disposal of pending fraud cases especially where the entities have completed the staff side action. Similarly, entities may vigorously follow-up with the police authorities and/or court for final disposal of fraud cases and/or court for final disposal of fraud cases.