



Federation of National Postal Organisations

T-24, Atul Grove Road, New Delhi-110 001

Mob.: 9959538622, e-mail: sivajivasireddy@gmail.com, Web : fnpo.org



SIVAJI VASIREDDY

Secretary General

No: 1-1/Malegoan Divn/Maharastra Circle/2025

dated 12.12.2025

To
The Secretary Posts,
Department of Posts,
Dak Bhavan,
New Delhi - 110001.

Respected Madam,

Sub: - Improper fixation of responsibility on operative staff – case of Rs.1.76 Cr fraud
case – at CPC Malegaon HO – Maharastra Circle – reg.

On behalf of the Federation of National Postal Organizations (FNPO), I respectfully submit the following legal and factual points for your kind and immediate intervention in the matter relating to the alleged EFT fraud amounting to Rs. 1.76 Crores at CPC, Malegaon HO, under Maharashtra Circle.

It is submitted that the present approach of fixing accountability solely upon operative staff is contrary to the principles of natural justice, ignores binding Directorate instructions, and overlooks serious administrative, systemic, and policy-level failures which directly enabled the occurrence of the fraud. In this context, the following submissions are made in defence of the operative staff, who are in urgent need of justice:

1. Non-compliance with Directorate guidelines on wrongly migrated policies

The PLI Directorate Order No. 25-02/2020-LI dated 27.08.2020 categorically mandated that wrongly migrated policies must be identified and removed from the McCamish system by the concerned Regional/Circle Offices.

However:

- The Administrative Offices failed to implement these binding instructions.
- No monitoring mechanism or compliance reporting system was put in place.
- Wrongly migrated policies continued to remain in the system for several years.

Thus, the root cause of the fraud lies in administrative non-compliance and not in the actions of operative staff. Fixation of liability on staff who had neither jurisdiction nor authority over policy migration is violative of the settled principle under Rule 11 of the CCS (CCA) Rules, 1965, which mandates that responsibility must correspond to the powers vested.

Contd....2



Scanned with OKEN Scanner

2. Critical security lapses in McCamish – system vulnerable by design

The McCamish system is afflicted with serious security deficiencies, including:

- Allowance of multiple simultaneous logins from different terminals using the same credentials.
- Absence of mandatory password change protocols, despite Directorate Order No. 29-34/2012-LI (Vol-II) dated 02.08.2016.
- Editable POSB account number fields even at the final stage of EFT maturity processing.
- Absence of validation checks for beneficiary account numbers in sensitive financial transactions.

Further, the CAG Report on the Project for Computerization of Core Banking and Core Insurance Solution (Chapter III – Department of Posts), particularly Para 3.1.11, has flagged serious systemic and control deficiencies. These lapses constitute gross failure on the part of system administrators and technology custodians responsible for implementing cyber-security and internal control frameworks. Operative staff cannot be penalized for defects inherent in the system, especially when such vulnerabilities directly facilitated diversion of funds.

3. EFT fraud attributable to lack of system-level checks, not staff negligence

The system permitted:

- Processing of wrongly migrated policies,
- Editing of beneficiary account details at the final stage,
- Execution of EFT transactions without cross-validation of account numbers.

These are high-risk actions expressly prohibited under standard financial controls and prudential norms. Such failures amount to violation of POSB rules, AML Prevention Guidelines, and CBS operational controls, which are the responsibility of administrative and system-controlling authorities, and not CPC-level operative staff.

4. Violation of Directorate instructions on User-ID management and trained manpower

Direktorate Orders No. 39-1/2017-LI, 13-01/2023-LI, and X-20/21/2020-SPN-II clearly stipulate:

- Deployment of only trained and certified personnel for sensitive financial operations.
- Immediate deactivation of McCamish User IDs upon transfer, retirement, or cessation of duties.
- Absolute prohibition on engagement of outsiders/daily wagers for financial work.

Contd...3

Contrary to the above:

- Outsiders were engaged in CPC operations involving financial authority.
- User IDs continued to remain active beyond authorized tenure.
- Operative staff were compelled to perform duties without formal training or adequate system knowledge.

These constitute grave administrative violations. Responsibility, therefore, must be fixed at supervisory and controlling levels rather than on subordinates who acted under compulsion and institutional constraints.

5. Arbitrary and legally unsustainable fixation of responsibility on operative staff

In the present case, operative staff had:

- No authority over system configuration or access controls.
- No power to rectify or delete wrongly migrated policies.
- No role in framing or enforcing password policies.
- No control over enabling or disabling system validation mechanisms.

Holding them solely responsible violates:

- Principles of Natural Justice,
- Doctrine of Proportionality,
- Fairness requirements under Rule 14 of the CCS (CCA) Rules, 1965,
- Judicial principles laid down by the Hon'ble Supreme Court in *State of Punjab vs. V.K. Khanna*.

Any recovery or disciplinary action initiated against operative staff without addressing administrative and systemic failures is arbitrary, discriminatory, and legally untenable.

6. Prayer for relief

In view of the foregoing, it is most humbly prayed that:

- a) A comprehensive and fresh assessment of responsibility may be undertaken, duly considering administrative, supervisory, systemic, and software-related failures.
- b) Operative staff may be exempted from disciplinary proceedings and recovery actions, as the fraud was enabled by factors wholly beyond their control.
- c) Waiver of recovery may kindly be granted, since the financial loss is directly attributable to administrative non-compliance, software vulnerabilities, and breach of mandatory security protocols by supervisory authorities.

Contd....4

d) Accountability may be fixed at appropriate administrative and system-management levels, in accordance with Directorate instructions and established legal principles.

This submission is made in the interest of natural justice, institutional fairness, and accountable governance.

Thanking you Madam,

Yours faithfully,
12/12/2025
(SIVAJI VASIREDDY)
Secretary General

Copy to:

1. The Chief Vigilance Officer, Dak Bhawan, New Delhi for information and with a request to order for fresh inquiry in this case to find actual responsible officials for fixing contributory negligence.
2. The Chief Postmaster General, Maharashtra Circle, Mumbai for information and necessary action.