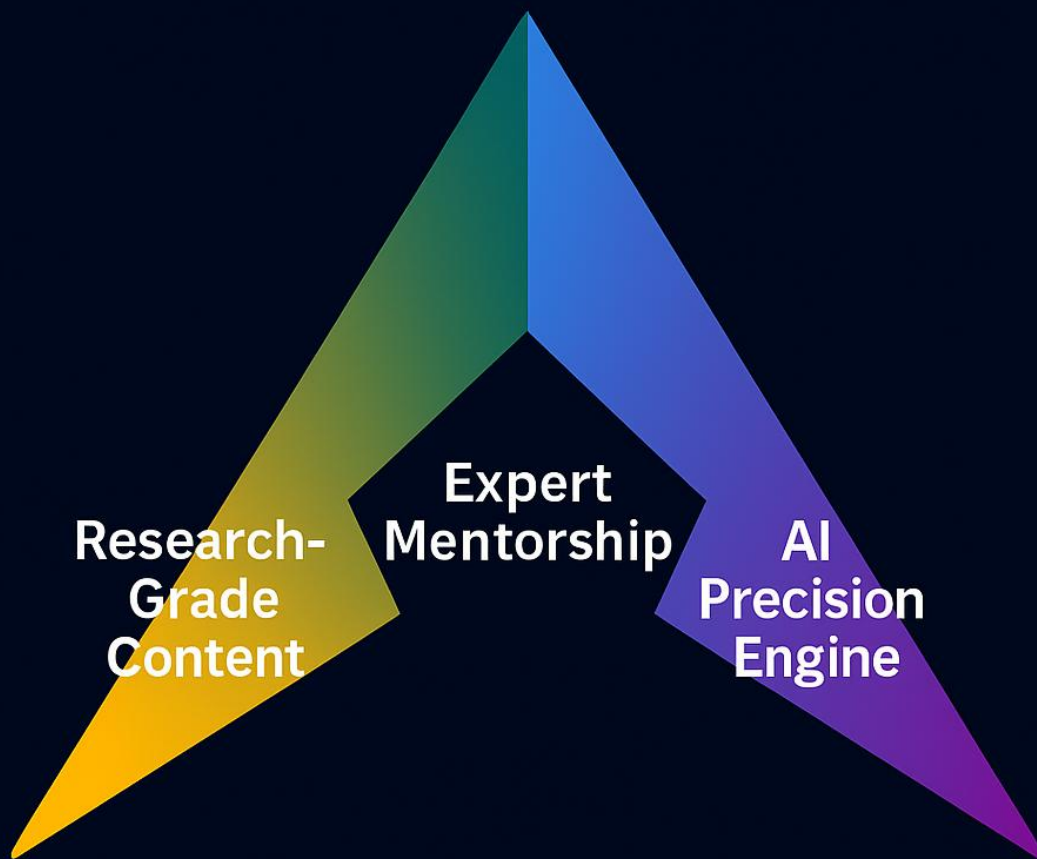


PrepAlpine

The Next-Generation UPSC Institution

Where Research Meets Mentorship & Precision



Preparation Meets Precision

A Next-Generation Learning Institution

Copyright © 2025 PrepAlpine

All Rights Reserved

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means—whether photocopying, recording, or other electronic or mechanical methods—without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain non-commercial uses permitted by copyright law.

For permission requests, please write to:

PrepAlpine

Email: info@PrepAlpine.com

Website: PrepAlpine.com

Disclaimer

The information contained in this book has been prepared solely for educational purposes. While every effort has been made to ensure accuracy, PrepAlpine makes no representations or warranties of any kind and accepts no liability for any errors or omissions. The use of any content is solely at the reader's discretion and risk.

DAILY CURRENT AFFAIRS DATED 25.06.2026

GS Paper II: Current Affairs

1. RBI's Revised Framework for Digital Fraud Compensation

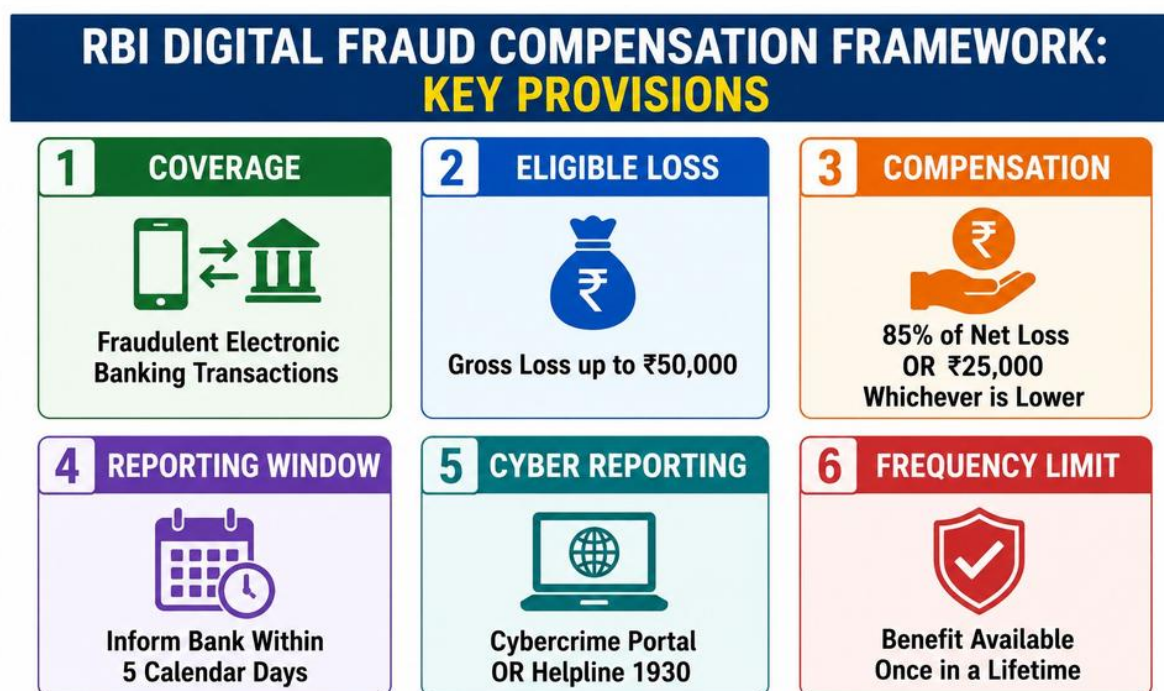
a. Introduction

India's rapid expansion of digital payments has transformed financial inclusion, convenience and the delivery of banking services. However, the same expansion has also increased exposure to cyber fraud, phishing, unauthorised transactions and social-engineering attacks.

For ordinary users, the fear of losing money through digital fraud can weaken trust in online banking and payment systems.

In this context, the Reserve Bank of India has revised the framework for limiting customer liability in fraudulent electronic banking transactions and introduced a compensation mechanism for victims of digital payment frauds. The revised framework, applicable from January 1, 2027, marks an important shift towards shared institutional responsibility in cases of digital fraud.

This makes the issue important for understanding the balance between digital financial inclusion, consumer protection and cyber-risk management.



b. Key Provisions of the Revised Framework

Scope and Objective

The revised directions apply to fraudulent electronic banking transactions carried out through bank accounts and digital banking channels.

Their objective is to:

- protect bona fide victims,
- encourage timely reporting,
- strengthen institutional accountability,
- build trust in digital banking systems.

Compensation for Genuine Victims

For genuine victims whose gross loss is up to ₹50,000, compensation will be calculated as:

- 85 per cent of the net loss, or
- ₹25,000, whichever is lower.

This benefit will be available only once in a lifetime.

Reporting Requirement

To qualify for compensation, the victim must:

- report the fraud on the National Cyber Crime Reporting Portal or through helpline 1930, and
- inform the bank within five calendar days of the occurrence.

This requirement aims to ensure quick reporting so that fraudulent transactions can be traced and funds can be frozen where possible.

Burden-Sharing for Domestic Transactions

For losses below ₹29,412 in domestic fraudulent electronic banking transactions, the burden will be shared as follows:

- Reserve Bank of India: 65 per cent,
- customer's bank: 10 per cent,
- beneficiary bank: 10 per cent.

For losses between ₹29,412 and ₹50,000, compensation will be capped at ₹25,000 and shared according to the prescribed framework.

Burden-Sharing for Cross-Border Transactions

In cross-border fraudulent electronic banking transactions, the burden-sharing pattern will be:

- Reserve Bank of India: 65 per cent,
- customer's bank: 20 per cent.

For losses between ₹29,412 and ₹50,000, compensation will again be capped at ₹25,000.

Overall, the framework moves digital fraud response away from individual victim-blaming and towards shared institutional responsibility.

c. Analysis/ Observations

Strengthening Consumer Confidence

- The revised framework is significant because it strengthens consumer confidence in digital banking.
- When users know that genuine victims of fraud may receive partial compensation, they are more likely to trust electronic banking systems. This is especially important in a country where digital financial inclusion depends heavily on public confidence.

Encouraging Timely Reporting

The framework encourages timely reporting by linking compensation to reporting within five calendar days.

Early reporting can:

- improve the chances of tracing fraudulent transactions,
- help freeze funds,
- alert banks to emerging fraud patterns,
- strengthen cybercrime response.

Recognition of Systemic Risk

- The burden-sharing design is important because it recognises that cyber fraud is not always the result of individual negligence.
- Banks, payment systems, beneficiary institutions and regulators all have a role in preventing, detecting and responding to fraud. The framework therefore treats digital fraud as a systemic risk rather than merely an individual failure.

Support for Digital Financial Inclusion

A credible compensation system can reduce fear among:

- elderly users,
- rural customers,
- first-time digital banking users,
- low-income account holders.

This can strengthen India's digital payment ecosystem and support wider financial inclusion.

Limited Coverage

- However, concerns remain. The compensation benefit is limited to gross losses up to ₹50,000.
- Many digital frauds involve higher amounts, especially where victims are manipulated into multiple transfers. Such cases may remain inadequately covered.

Once-in-a-Lifetime Restriction

- The once-in-a-lifetime condition may be restrictive because a person can become a genuine victim more than once.
- This may be especially relevant for vulnerable users who are repeatedly targeted through social engineering.

Reporting Window Challenge

The five-day reporting window may exclude digitally less-aware users, particularly:

- elderly citizens,
- rural users,
- first-time digital banking users,
- persons who do not immediately understand that a fraud has occurred.

Implementation Constraints

Implementation will depend heavily on coordination among:

- banks,
- the Reserve Bank of India,
- cybercrime portals,
- law-enforcement agencies,
- payment system operators.

Fraud investigation remains complex because tracing beneficiary accounts, identifying mule accounts, freezing funds and coordinating across jurisdictions can be difficult.

Thus, compensation is necessary, but it must be supported by strong fraud prevention, investigation and recovery systems.

d. Way Forward

Strengthen Real-Time Fraud Detection

- India must strengthen real-time fraud detection and transaction-freezing systems.
- Banks should be able to flag suspicious transactions quickly and temporarily block doubtful fund flows, especially in reported fraud cases.

Improve Institutional Coordination

- Coordination between banks, the Reserve Bank of India, the National Payments Corporation of India and cyber police must be improved.
- A seamless reporting and response system can reduce delays and improve recovery chances.

Expand Digital Literacy

Digital literacy should be expanded, especially among:

- elderly users,
- rural households,
- first-time digital payment users,
- low-income account holders.

Awareness campaigns should explain common fraud methods, safe banking practices and the importance of immediate reporting through helpline 1930 and the cybercrime portal.

Simplify Grievance Redressal

- Grievance redressal and compensation timelines should be clearly defined.
- Victims should not be forced to navigate complex procedures after suffering financial loss.

Use AI-Based Monitoring Carefully

Artificial intelligence-based risk monitoring may help detect unusual transaction patterns. However, it must be used with:

- privacy safeguards,
- clear accountability,
- auditability,
- protection against wrongful blocking of genuine transactions.

Periodic Review of Compensation Limits

- Compensation limits should be reviewed periodically as digital transaction values rise and fraud patterns become more sophisticated.
- These steps can ensure that the compensation framework becomes part of a wider digital financial protection architecture.

Conclusion

The Reserve Bank of India's revised framework marks an important shift from individual blame to shared institutional responsibility in digital fraud cases.

It can strengthen trust in digital banking and support India's digital payment ecosystem. However, its success will depend on fast reporting systems, bank accountability, effective cybercrime coordination and stronger fraud-prevention infrastructure.

In a rapidly digitalising economy, consumer protection must evolve as quickly as digital innovation itself.

Reader's Note — About This Current Affairs Compilation

Dear Aspirant,

This document is part of the PrepAlpine Current Affairs Series — designed to bring clarity, structure, and precision to your daily UPSC learning.

While every effort has been made to balance depth with brevity, please keep the following in mind:

1. Orientation & Purpose

This compilation is curated primarily from the UPSC Mains perspective — with emphasis on conceptual clarity, analytical depth, and interlinkages across GS papers.

However, the PrepAlpine team is simultaneously developing a dedicated Prelims-focused Current Affairs Series, designed for:

- factual coverage
- data recall
- Prelims-style MCQs
- objective pattern analysis

This Prelims Edition will be released separately as a standalone publication.

2. Content Length

Some sections may feel shorter or longer depending on topic relevance and news density. To fit your personal preference, you may freely resize or summarize sections using any LLM tool (ChatGPT, Gemini, Claude, etc.) at your convenience.

3. Format Flexibility

The formatting combines:

- paragraphs
- lists
- tables
- visual cues

—all optimised for retention.

If you prefer a specific style (lists → paras, paras → tables, etc.), feel free to convert using any free LLM.

4. Monthly Current Affairs Release

The complete Monthly Current Affairs Module will be released soon, optimized to a compact 100–150 pages — comprehensive yet concise, exam-ready, and revision-efficient.

PrepAlpine