CYBER CENTRE OF EXCELLENCE

Gujarat Police

AADHAAR AePS FRAUD

The Silent Withdrawal From Your Bank Account

■ *Lock it. Mask it. Monitor it.*

A Public Awareness Guide

Cyber Crime Helpline: 1930 | cybercrime.gov.in

What Is Aadhaar AePS Fraud?

The **Aadhaar enabled Payment System (AePS)** is a banking channel that lets a person withdraw cash, check balance, or transfer funds using only their Aadhaar number and a fingerprint — no debit card, no PIN, no OTP. It was built to bring banking to rural India through micro-ATM operators. But the same simplicity has made it the easiest gateway for criminals to drain bank accounts silently.

Fraudsters obtain Aadhaar numbers from leaked databases or publicly available records (land registries, property documents, EPFO records) and lift biometric impressions from sub-registrar offices, fake fingerprint clones, or silicone replicas. With these two pieces, they impersonate the victim at a micro-ATM and withdraw money. The victim usually finds out only when an SMS arrives — sometimes hours after the cash is gone.

The single most important fact:

AePS fraud needs **no OTP, no card, and no consent message** to your phone. The first SMS you receive is often the debit confirmation — by then, the money has already left. The only real defence is to **lock your Aadhaar biometrics** at uidai.gov.in before fraud occurs, not after.

The Scale of the Problem

₹459 Cr
Lost to UPI & AePS-linked frauds reported via I4C in FY 2023–24

3.7 Bn+
AePS transactions processed in India in FY 2023–24 (NPCI)

1930
Report cyber crime 24×7 All India, toll-free

The Reserve Bank of India and NPCI have repeatedly warned that AePS biometric authentication is being misused through stolen fingerprints lifted from registered documents. UIDAI has since launched the **Aadhaar Biometric Lock** facility and rolled out fingerprint liveness detection, but these protections work only if citizens enable them.

How the Fraud Happens

AePS fraud follows a recognisable five-stage pipeline. Understanding each stage can help you spot where the protection points lie:

1

Aadhaar Number Harvested

Criminals collect Aadhaar numbers from leaked KYC databases, photocopied Aadhaar cards in shops, hotel registers, gas-connection forms, or public records on government portals. An unmasked Aadhaar number is the first key.

2

Biometric Impression Lifted

Fingerprints are extracted from property registration documents (where buyers press a thumb on a register), fake biometric devices at retail shops, or silicone clones produced from high-resolution photos. Investigations in Bihar, Jharkhand, and Haryana have uncovered organised gangs operating exactly this way.

3

Micro-ATM Withdrawal

Using a portable AePS device sold to small retailers as a banking correspondent kit, the fraudster keys in the victim's Aadhaar number, places the cloned fingerprint on the scanner, and selects 'cash withdrawal'. The bank's server authorises the transaction — because the biometric matches.

4

Money Routed Through Mules

Cash withdrawn at the micro-ATM is split between the operator and the syndicate. Online AePS-to-wallet transfers are routed through a chain of mule accounts opened with stolen identities, making recovery extremely difficult once funds leave the originating bank.

5

Victim Receives an SMS

The first hint of trouble is an SMS: "Rs. 10,000 debited via AePS." The victim has never visited an ATM, never received an OTP, never given consent. By the time they reach a bank branch, the fraud chain is several hops deep. Reporting to **1930** within the first hour is the single biggest factor in fund recovery.

How To Protect Yourself

✔ DO THIS

✔ **Lock your Aadhaar biometrics** at **uidai.gov.in** or on the mAadhaar app. Unlock only at the moment you need to authenticate, then lock again.

✔ Use a **Masked Aadhaar** (downloadable from uidai.gov.in) wherever possible — it hides the first 8 digits of your number.

✔ Register for **SMS & email alerts** on every bank account so any debit reaches you instantly.

✔ Check your bank statement at least weekly for unfamiliar AePS or NACH debits.

✔ Use a Virtual ID (VID) on the UIDAI website for Aadhaar authentication where required.

✔ When buying or selling property, ask the sub-registrar's office about **biometric protection** — many states now offer covered scanners.

✔ If you notice a suspicious debit, call **1930** immediately and file a complaint at **cybercrime.gov.in** within the golden hour.

✘ NEVER DO THIS

✘ Never share a clear photocopy of your Aadhaar card with shops, hotels, or telecom dealers — always insist on masked Aadhaar.

✘ Never place your thumb on any biometric scanner you are unsure about, especially handheld devices at small retail outlets.

✘ Never ignore an SMS about an unknown debit — even ₹1 unauthorised debit can signal a larger attack in progress.

✘ Never assume your bank will detect the fraud automatically. The authentication looks valid to the bank — you must report.

✘ Never publicly post pictures of your Aadhaar card, PAN, or any government ID on social media, WhatsApp status, or matrimony sites.

✘ Never delay reporting. AePS withdrawals are nearly impossible to reverse once cash has been disbursed at a micro-ATM.

Remember:

You do **not** need to wait for fraud to happen. Lock your Aadhaar biometrics today — it takes under two minutes on uidai.gov.in and is completely reversible. Locked biometrics cannot be used by anyone, even with your number and a perfect fingerprint clone. This single step blocks the entire AePS fraud chain at its core.

How to Report — Step by Step

1930

Toll-free | 24×7 | All India

The Reporting Process

1

Call 1930 Immediately

The first hour after a fraudulent debit is the **golden hour**. The operator will record your transaction details and trigger a hold request to the recipient bank to freeze the funds before the mule withdraws or transfers them further.

2

Report to Your Bank

Inform your bank's fraud helpdesk in writing (email + branch visit). Under the RBI's "Limited Liability of Customers" circular, if you report unauthorised electronic transactions **within 3 working days**, your liability is zero for third-party breaches.

3

File at cybercrime.gov.in

Log in and file a complaint under 'Financial Fraud → AePS / Banking Fraud'. Upload bank SMS screenshots, account statement showing the fraudulent entry, your Aadhaar (masked), and a copy of your last legitimate transaction.

4

Lock Your Aadhaar Biometrics Now

Visit **uidai.gov.in** → "Lock/Unlock Biometrics" — or use the mAadhaar app — to lock immediately. This blocks any further AePS attempt while the investigation is ongoing.

5

Follow Up With Your Complaint Number

After filing, you receive an acknowledgement number. Track progress at cybercrime.gov.in. Visit your local cyber police station with printed evidence and request an FIR if one has not already been registered.

Family Safety Checklist

Senior citizens, rural account holders, and pensioners are the most heavily targeted. Walk through this checklist with every member of your household:

- Lock the Aadhaar biometrics of **every adult family member** on uidai.gov.in — especially elderly parents who rarely use them.
- Save **1930** and the bank's fraud helpline on every phone in the household.
- Enable **SMS & email alerts** on every linked bank account, including dormant Jan Dhan accounts.
- Replace all Aadhaar photocopies kept in wallets and files with **masked Aadhaar** copies.
- Check the bank passbook or app statement of pensioner family members at least once every week.
- Never let a stranger scan a family member's fingerprint at a kiosk, shop, or roadside camp.
- Discuss AePS fraud with the household monthly — many victims are unaware the system even exists until they are robbed by it.
- If a bank account is no longer in use, formally close it — dormant accounts linked to Aadhaar are a common attack target.

Real Cases Reported in India

Haryana — Pensioner, ₹1.2 lakh (2024)
A 68-year-old retired schoolteacher in Karnal received four AePS debit SMSes within an hour totalling ₹1.2 lakh. He had recently signed a land registration document where his thumb impression was openly captured. Police traced the withdrawal to a banking correspondent in a neighbouring state. Locking his Aadhaar biometrics immediately after reporting prevented two further attempts the next day.

Bihar — Mass AePS Attack on Jan Dhan accounts (2023)
In a coordinated operation across districts in Bihar, more than 200 villagers reported small AePS withdrawals (₹2,000–₹10,000 each) from accounts most had not used in months. Investigators recovered cloned silicone fingerprints from the gang and traced the source data leak to a property registration office. NPCI subsequently tightened biometric liveness checks across micro-ATMs.

Gujarat — Avoided Loss After Locking (2025)
An Ahmedabad-based salaried professional noticed her Aadhaar number had been photocopied at a hotel during travel. The same evening she locked her biometrics on the mAadhaar app. Two weeks later, a failed AePS attempt was logged at a micro-ATM in another state — the lock had blocked the transaction. She reported the incident to 1930 and supplied the failed-attempt SMS as evidence.

Important Contacts & Resources

Service	Contact
National Cyber Crime Helpline	1930 (24×7, toll-free)
National Cyber Crime Reporting Portal	cybercrime.gov.in
Lock / Unlock Aadhaar Biometrics	uidai.gov.in | mAadhaar app
UIDAI Helpline	1947 (toll-free)
Download Masked Aadhaar	uidai.gov.in → My Aadhaar
RBI Sachet (unauthorised entities)	sachet.rbi.org.in
Banking Ombudsman (RBI)	cms.rbi.org.in
Report fraudulent SMS / call	sancharsaathi.gov.in (Chakshu)
Police Emergency	112
CERT-In (incident reporting)	incident@cert-in.org.in

Five Things to Remember

1. **AePS fraud needs no OTP.**
   Unlike UPI or card payments, AePS bypasses every consent step you are used to. Your phone gives you no warning until the money is already gone.

2. **Locking your biometrics is free, fast, and reversible.**
   It takes under two minutes on uidai.gov.in. Locked biometrics cannot be used by anyone, anywhere — even with a perfect fingerprint clone.

3. **An unmasked Aadhaar number is half the attack.**
   Always share masked Aadhaar. Never let a shop photocopy your Aadhaar card with all 12 digits visible.

4. **The first hour after fraud is decisive.**
   Call 1930 immediately. Funds frozen within the golden hour are recovered far more often than those reported even a day later.

5. **Awareness in the family stops the attack.**
   Elderly parents and rural relatives are the most targeted. One conversation can lock the door before a fraudster ever knocks.

If you remember only one number: **1930**.
If you remember only one website: **uidai.gov.in**.
If you remember only one rule: **lock your biometrics today.**