Frauds—the Achilles’ heel of AePS transactions?

MSC
MicroSave Consulting

www.microsave.net

Unveiling AePS-related frauds in India

Kiran, a 28-year-old passionate business correspondent (BC) agent in rural Varanasi, Uttar Pradesh, facilitates financial transactions through the *Aadhaar*-enabled Payments System (AePS)[1]. Kiran is an ambitious woman who has her family's support. However, she faced a significant setback when a customer accused her of fraud. Radha, a middle-aged woman, visited Kiran's agent outlet to check her account balance and inquire about *Pradhan Mantri Kisan Samman Nidhi* (PM-*KISAN*) disbursements. She checked her balance and realized she had not received the PM-KISAN benefit because her bank balance was the same INR 6,300 (USD 75.53) that she had when she checked her balance previously. She left Kiran's outlet after she checked her bank balance.

A month later, Radha returned with her grandson and accused Kiran of withdrawing INR 6,300 (USD 75.53) from her account. Kiran offered to check her overdraft (OD) account statement, but the amount had not been credited. Kiran advised Radha to file a complaint with her bank and at the police station. Police registered the case under section 66 D of the Information Technology Act (IT Act 2000) and initiated the process to investigate the case. The confrontation escalated into a first information report (FIR)[2] with three charges against Kiran and threats of arrest and seizure of her agency ID.

However, further investigation revealed that an unidentified person from Hardoi, a district approximately 400 km from Varanasi, had conducted those unauthorized transactions when Radha visited Kiran's outlet for a balance inquiry. Per the police, the fraudster accessed Radha's biometrics and executed the unauthorized transactions. It later came to light that someone had approached Radha a few days earlier to reverify her *Aadhaar* number and biometrics for a subsidy program that she had enrolled in and could have cloned her biometrics. Police authorities registered an FIR and started their investigation to verify the identity of the fraudster's bank account.

This incident, however, left both Radha and Kiran frustrated. The former lost a significant amount of money, while the latter faced loss of business and social reputation.

Note: While the story of Kiran, Radha, and Gautam is based on real-life incidents, their actual names have been changed to protect their identities.

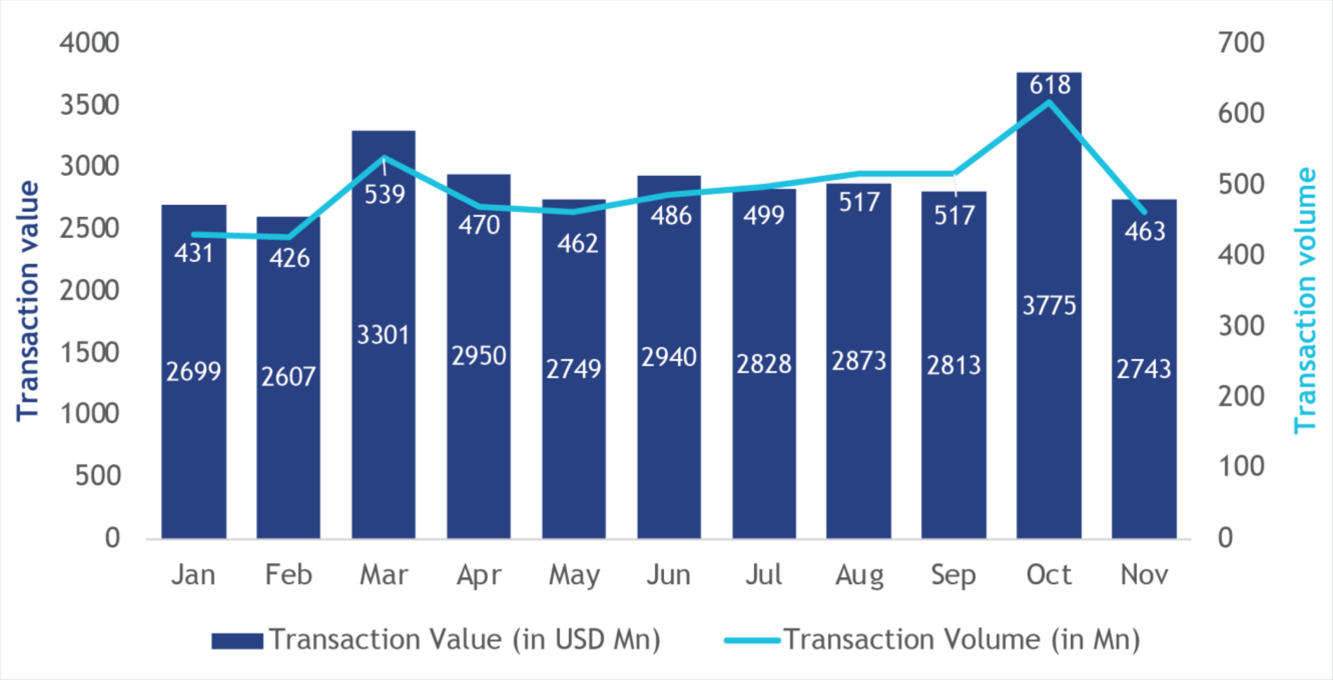
[1] AePS is a bank-led model that uses Aadhaar-based authentication to allow interoperable online transactions in Aadhaar-linked bank accounts at micro-ATMs or kiosks. To use AePS, customers need an account with a bank that supports AePS and must have their Aadhaar linked with their bank account. To transfer money through AePS, users need to put their Aadhaar number, and biometrics (fingerprint generally) to the nearest BC agent.

[2] First information report (FIR) is a written document prepared by the police when they receive information about the commission of a cognizable offense.

This unpleasant experience faced by Radha and Kiran is not an isolated case. In 2023, AePS-related frauds constituted about 11% of the total 1.13 million cyber financial fraud cases registered in India. These frauds involved INR 823.74 crore (USD 98 million) and were mostly committed in and originated from Bihar and Jharkhand. The amount lost to fraud per case is usually reported to be approximately between INR 5,000 to INR 6,000 (USD 60 to 72).

AePS plays a critical role in delivering payment services in India. During COVID, AePS emerged as a critical cash-out medium for migrants, daily wagers, and other informal sector workers. In 2024 (Jan to Nov'24), ~400 million customers conducted 5.4 billion and USD 32.27 billion AePS transactions in volume and value, respectively.

Figure: 1 Volume and value of AePS transactions in 2024.



Source: NPCI website

To know the latest insights and trends on digital payments in India, visit MSC's PIN Rails website.

Most AePS users belong to the low- and moderate-income (LMI) segments, who have limited understanding and awareness of payment systems and technology, which makes them more susceptible to fraud.

What is AePS fraud? How do we define it?

Though AePS fraud lacks a standard definition, most financial service providers (FSPs) typically consider an AePS transaction as a fraudulent transaction if it meets any of the following conditions:

i. The transaction is conducted outside the permissible geography. The permissible geography is the area radius as assigned by the provider where a BC agent is authorized to conduct transactions for customers;

ii. The transaction traceability is compromised. This means that the transaction cannot be traced or verified at the provider's backend system linked to the AePS device;

iii. The agent is untraceable after a suspected fraud transaction or during an inquiry of suspected fraudulent transactions;

iv. The BC agent (or anyone else involved) misrepresents the truth or conceals a material fact to mislead someone into acting against their own interest.

The financial fraud incident with Radha and Kiran is a classic example of AePS fraud. The transaction was conducted outside the permissible radius, its traceability was compromised, and information about the transaction, usually sent via SMS, was concealed from the customer. A major challenge in tracing or suspecting a potential fraud is that it is recorded as a successful transaction at the backend. In most cases, customers are not around or do not receive SMS or email alerts about the transaction, which makes it difficult to trace a fraudulent transaction in real time.

Many cases arise from the unintentional sharing of sensitive information, such as one-time passwords (OTPs). However, cybercriminals increasingly use sophisticated techniques, such as silicone thumbs and deepfake technology, to exploit biometric systems. These methods allow them to replicate fingerprints with the use of biometric data from documents, such as land records, and enable unauthorized access to bank accounts. In some cases, agents are complicit in the fraud, while in others, the scammers deceive them as well.

The National Payments Corporation of India (NPCI) typically classifies frauds into four categories to determine the liability of addressing them. These include:

i. **Fake biometric fraud:** The fraudster uses victims' or customers' *Aadhaar* numbers, virtual IDs, and fake biometrics to perform a financial transaction;

ii. **Fraud through deception:** Fraudsters deceive customers to provide their *Aadhaar* number and then use it to perform financial transactions from the customer's account;

iii. **Incorrect *Aadhaar* linking or account seeding** by the issuer bank: This can also lead to the misuse of funds intentionally or unintentionally;

iv. **Others:** These include cheating fraud with the use of social engineering techniques, or instances where the CBC or BC agent is absconding, not available or not contactable after a fraud.

We have categorized these frauds into various buckets based on their origination to understand them in more detail.

Common types of AePS frauds in India

Case type A: Agent-initiated fraud

Scenarios	Presence of customers	Impact on stakeholders
Scenario 1: The agent sells their agent ID to an unauthorized person for as much as INR 10,000 (~USD 120). The unauthorized person then conducts fraudulent withdrawals, acting as the BC agent. **Scenario 2:** The agent declares a successful transaction as unsuccessful and asks the customer to attempt the transaction a second time. The agent then debits the transaction amount from the customers' account and gives them a receipt of the transaction. **Scenario 3:** The agent initiates a withdrawal transaction of a higher amount than stated by the customer. Such frauds are mostly successful in cases where the customer is illiterate and cannot understand the entries on the receipt.	Yes	**Customer:** - **Financial impact**: Customers lose their hard-earned money. - **Delayed resolution:** These frauds are hard to trace. Most customers do not even realize that money has been deducted from their accounts, which leads to delayed reporting. Customers who raised complaints reported a long turnaround time (TAT) for a resolution. However, in most cases, customers bear financial losses since the current recourse mechanism is complex and the country's recovery rate is low across different banks and FSPs. **Corporate business correspondent (CBC):** - **Procedural costs:** Providers are expected to trace the root cause of the financial fraud, blacklist the agent, and file an FIR against the agent. This involves a considerable investment of time and money. - **Financial impact:** Providers must compensate customers for the financial loss if the fraud claims are correct. This could also be paid as chargeback[3] fees, which the CBCs are liable to pay. CBCs also risk losing future business with the issuer banks.

[3] Chargeback: Chargeback refers to the reversal of funds back to the payer's (customer's) account due to a dispute against a particular transaction. This dispute can be due to the non-delivery of services to the customer or unauthorized or fraudulent transactions in the the customer's account. Please see this link for details on the NPCI's guidelines on AePS fraud chargeback.

		Bank: - **Procedural costs**: When the bank directly manages an agent who has committed fraud, it has to block such agents, file an FIR, notify the NPCI, and include such agents' details in the "negative registry." This results in direct costs and additional investment of time and money to recruit and onboard a replacement. - **Financial impact**: Banks must compensate customers for their financial loss.

Case type B: Customer-initiated fraud

Scenarios	Presence of customers	Impact on stakeholders
Scenario 1: The customer authorizes an AePS transaction at the agent point. However, after the customer noticed that the agent did not record the transaction or did not have CCTV footage to prove the transaction, they filed a complaint and flagged the transaction as fraudulent. The customers usually file such complaints after some time, typically after one to three months, to benefit from the chargeback facility. **Scenario 2:** Banks and CBCs have reported multiple cases of customer and agent collusion. The customer raises a chargeback complaint about a transaction they authorized. In this case, the agent knows the customer will file a complaint against the transaction. To benefit from the chargeback facility, they usually file such complaints close to the 90-day mark.	Yes	**Agent:** - **Financial impact:** Providers seize the agent's ID till the agent is proven innocent, which impacts the agent's business. - **Reputational impact:** Other customers do not trust the agent even after they are found innocent. This impacts their earnings and leads to income loss. **Corporate business correspondent:** - **Financial impact:** CBCs have to pay the customer the entire amount if the claims are correct. Since most BCs are managed directly by CBCs, CBCs also bear the brunt of a fraudulent transaction. **Bank:** - **Financial impact:** The acquirer bank is liable to pay the customer the entire amount in addition to the chargeback amount unless the customer is proven guilty or found complicit in the fraud.

Case type C: Third-party frauds

Scenarios	Presence of customers	Impact on stakeholders
Scenario 1: Fraudsters fabricate counterfeit customer biometrics. They use silicon cloning techniques and obtain biometric data from sources, such as land records. These falsified biometrics are then used to carry out transactions at agent points. **Scenario 2:** Fraudsters use technology to trace transactions, such as a balance inquiry transaction, and conduct a withdrawal from the customer's account. In such cases, the agent's system is hacked by clicking on unverified Android application package (APK) links, which enables hackers or fraudsters to commit fraud.	No	**Agent:** - **Financial impact:** The agent's ID gets blacklisted, and they lose business until proven innocent. - **Reputational impact:** Other customers stop trusting the agent even after they are found innocent. This impacts their earnings and leads to income loss. **Customer:** - **Protracted resolution:** These frauds are hard to trace. Most customers do not even realize that money has been taken from their accounts, which leads to delayed reporting. Customers who raise a complaint reported a long TAT to receive a resolution. Meanwhile, customers who are unaware of the grievance resolution mechanism (GRM) process bear the financial loss. - **Future risks of frauds or scams:** Leakage of personally identifiable data puts them at a higher risk of fraud in the future. **Corporate business correspondent:** - **Financial impact:** CBCs have to pay the customer the entire amount if the claims are correct. Since most BCs are managed directly by CBCs and not banks, CBCs bear most of the cost of fraudulent transactions. - **Procedural costs:** The National Payments Corporation of India's (NPCI) regulations call for a detailed investigation process whose liability primarily falls on CBCs. **Bank:** - **Procedural costs:** Providers are expected to trace the root cause of the financial fraud, blacklist the

		agent, and file an FIR against the agent. This involves a considerable investment of time and money.

Based on the originator of the fraud, the compensation's financial liability shifts between the acquirer bank[4] and the issuer bank[5]. For instance, the acquirer bank is responsible for the issues if fraud or error occurs due to the acquirer bank through its CBC, BC, or any of the customer service points (CSP). However, if the issuer bank causes fraud or error through its CBC, BC agent, CSP, or customer, the issuer bank must take responsibility. In such cases, the issuer bank cannot claim a refund from the acquirer bank and must reimburse the customer directly.

While each stakeholder is impacted significantly, CBCs seem to be the most impacted by rising fraud cases. This is because the banks deduct the contested amount from the monthly payments of the CBCs before they agree on an official recourse. CBCs are also liable for the chargeback payment. Considering the average ticket size of AePS withdrawals and the transaction limits set by banks, the chargeback liability[6] may typically fall within the range of INR 2,500 to INR 50,000 per customer, depending on how many unauthorized transactions were conducted before the fraud was detected and flagged. They are also responsible for the management of the processes and financial costs required to file an official police report and thoroughly investigate the fraud complaint.

More is less when it comes to safety and security measures to address AePS fraud.

With the rise in the number of frauds, financial institutions (FI) also struggle to track and investigate instances of fraud regularly. Our interaction with a few industry stakeholders highlighted that the RBI prescribes FIs to track certain fraud risk indicators. One such indicator is the fraud-to-sales ratio (FTS)[7]. While the prescribed ratio is 0.22, in the present scenario, some FIs have reported a ratio as high as 4.22 and are actively working to bring it down below the stipulated limit.

Recently, two parliamentary panels took note of the rise in payment fraud and have prescribed various measures to curb it. In July 2023, the parliamentary Standing Committee on Finance recommended various measures, such as bolstering oversight of financial service providers, creating a centralized cybersecurity authority, and enhancing financial infrastructure. Additional recommendations included establishing a fraud registry, streamlining victim compensation, and enforcing stricter data-sharing protocols for tech companies to safeguard the digital ecosystem. Then, in February 2024, the parliamentary Standing Committee on Communications and Information Technology Players presented its report on digital payments with observations to enhance digital transactions' security.

[4] Acquirer bank: The bank that has acquired the agent or the bank whose device has been used for the transaction.

[5] Issuer bank: The bank in which the customer holds their account and to which *Aadhaar* is mapped for conducting AePS transactions

[6] The chargeback liability would also depend on other factors, such as the total number or instances of fraudulent transactions before the fraud was reported, the fraud's origin (agent or third-party), timely reporting of the fraud, and other evidence available based on which banks and CBCs may further negotiate the liability.

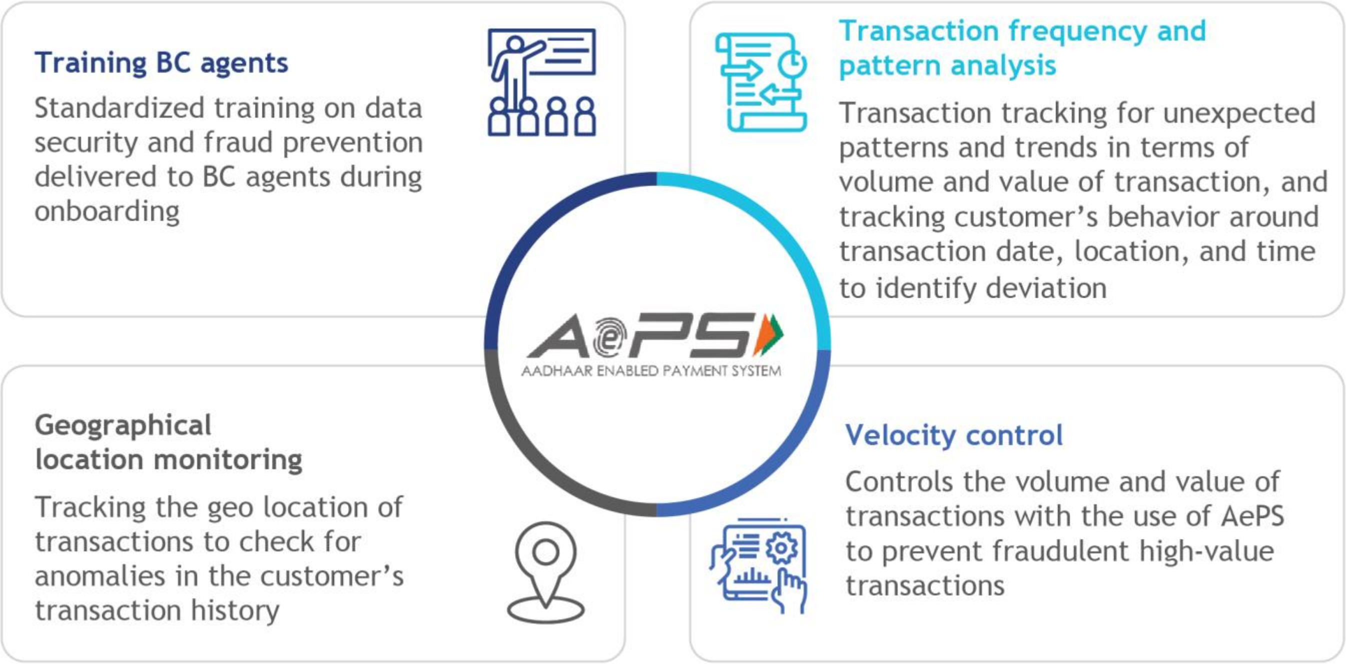
[7] FTS: Fraud-to-sales ratio refers to the total volume of fraudulent transactions reported divided by the total volume of transactions conducted in that time period.

While AePS fraud protection is an integral part of these recommendations, the stakeholders in the AePS ecosystem have also created policies, adopted regulatory measures, and are implementing new strategies to curb AePS fraud. They have adopted an approach that follows an AePS transaction throughout its lifecycle. This includes increased scrutiny in the onboarding and management of BC agents, monitoring of customers' transactions to identify and resolve anomalies, and a robust system for regulators, acquirers, and issuer banks to collaborate to resolve instances of fraud after they have occurred.

Most stakeholders have implemented a variety of measures to address AePS fraud. We have highlighted a few measures below:

1. Measures by banks and CBCs

Figure 2: Checks by providers to prevent AePS fraud



Training BC agents

Standardized training on data security and fraud prevention delivered to BC agents during onboarding

Transaction frequency and pattern analysis

Transaction tracking for unexpected patterns and trends in terms of volume and value of transaction, and tracking customer's behavior around transaction date, location, and time to identify deviation

Geographical location monitoring

Tracking the geo location of transactions to check for anomalies in the customer's transaction history

Velocity control

Controls the volume and value of transactions with the use of AePS to prevent fraudulent high-value transactions

Training BC agents

- Radha and Kiran's story highlights that Kiran's system was likely compromised earlier through an unverified APK sent to their mobile device through which she transacts. Therefore, in-depth training on fraud typology, ways to preempt fraud, and best practices for digital hygiene are key components to prevent such situations.
- Some CBCs also observed that the agents who were onboarded digitally were involved in more fraud than those who were onboarded physically. Digital onboarding processes may involve electronic know your customer (e-KYC), which, if not secure, can be exploited by fraudsters, for instance, through phishing attacks or identity theft cases. Physical onboarding is a slower process, but it may deter certain types of fraud, such as impersonation-based fraud. After this discovery, one of the CBCs switched to the physical KYC of agents and installed various geofencing software to continuously check for frauds occurring within the system.

Geographical location monitoring and alerts for customers

- Banks often monitor the geographical locations of transactions. If a transaction occurs in a location that is significantly different from the customer's usual transaction history, for instance, if a customer from Bengaluru conducts a transaction in Delhi, it can trigger an alert. The bank's support team may then verify the transaction with the customer.

Transaction frequency and behavior analysis

- Some banks use behavioral analysis to establish a baseline of their customer's typical behavior. Deviations from this baseline can raise suspicions. For example, transactions that occur during nonbusiness hours or on holidays when the customer typically does not conduct banking activities can be considered suspicious. The bank may ask for confirmation and verify the transaction with the customer. Banks analyze the frequency and patterns of transactions to identify fraudulent transactions. Unusual or unexpected transactions, such as a sudden spike in activity or a transaction the bank's customer rarely engages in, could trigger alerts.
- Similarly, banks also limit and block the usage of AePS for customers based on their internal profiling. For example, an urban customer who typically conducts transactions through debit or credit cards and Unified Payments Interface (UPI) will be blocked from conducting AePS transactions at a BC outlet. Such transactions will be deemed suspicious, which reduces the chances of fraud. Moreover, AePS services are discontinued for accounts that have not witnessed any AePS debits in the past 12 months and for accounts where the only AePS transaction in the past 12 months was deemed fraudulent.

Velocity controls by issuer banks

- Velocity controls include limits on the value and volume of transactions that can be processed. Specifically, a customer is allowed a maximum of five daily transactions at any given touchpoint. Additionally, it involves a cap of INR 10,000 (USD 118) on the total value of AePS transactions per day and a monthly limit of INR 50,000 (USD 590) for withdrawals. AePS is largely used for cash withdrawals, and the average ticket size ranges between INR 2,500 to 3,000 (USD 30 to 36). These velocity controls are vital to prevent the accumulation of high-value transactions that could be fraudulent.

PLZ PLACE YOUR
YOUR BEST FINGER
भारतीय विशिष्ट पहचान प्राधिकरण
भारत सरकार
Unique Identification Authority of India
Government of India

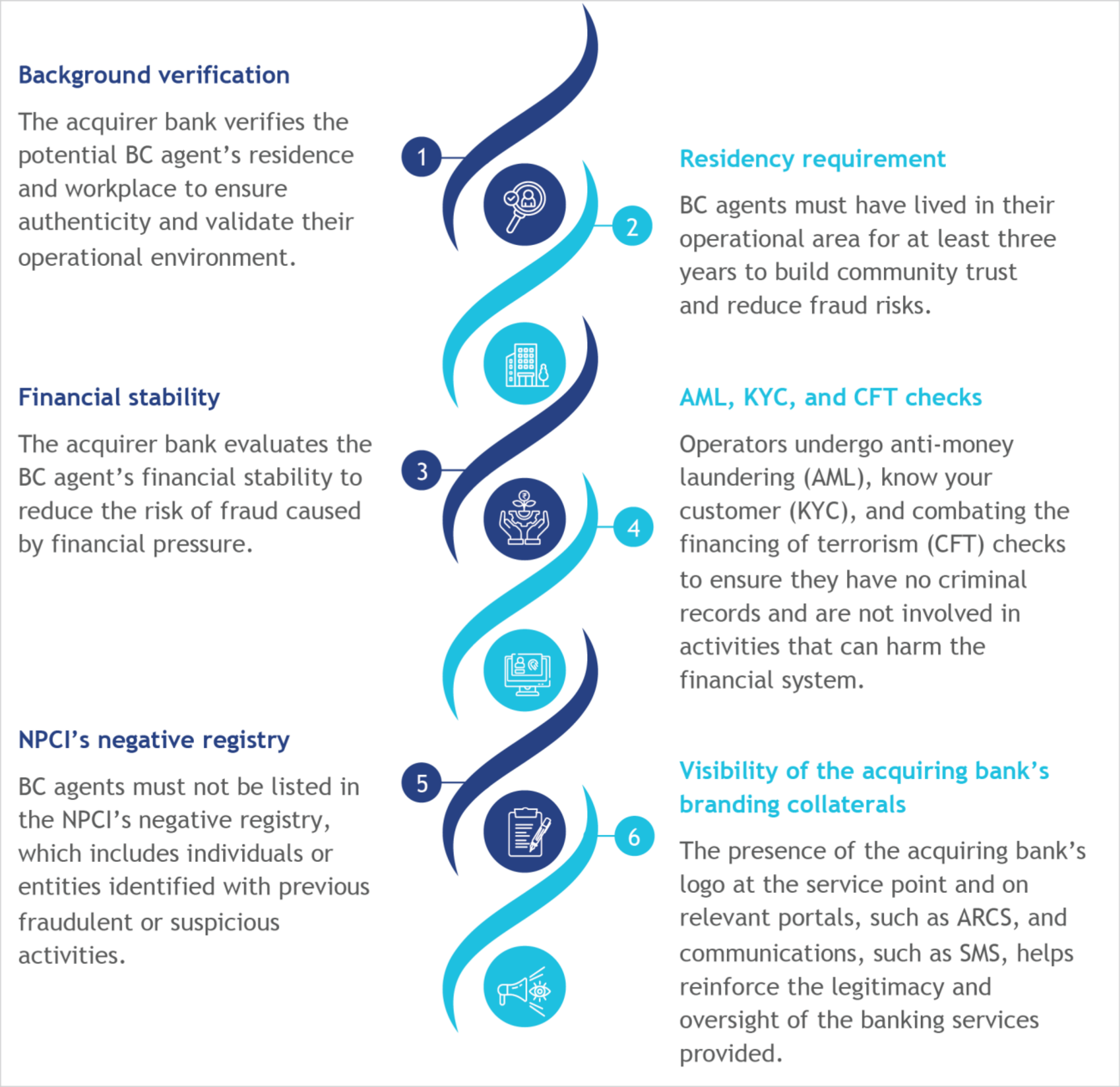
2. Measures by regulators and policymakers

Regulators and policymakers, such as the Reserve Bank of India (RBI), the Unique Identification Authority of India (UIDAI), and the NPCI, have also implemented a mix of prevention and resolution approaches to combat fraud effectively.

Background checks and due diligence in onboarding BC agents

The NPCI mandates that acquirer banks adhere to a comprehensive due diligence process before they onboard new BC agents. This process includes several critical checks, which the infographic below highlights:

Figure 3: Due diligence checklist for acquirer banks



Background verification

The acquirer bank verifies the potential BC agent's residence and workplace to ensure authenticity and validate their operational environment.

Residency requirement

BC agents must have lived in their operational area for at least three years to build community trust and reduce fraud risks.

Financial stability

The acquirer bank evaluates the BC agent's financial stability to reduce the risk of fraud caused by financial pressure.

AML, KYC, and CFT checks

Operators undergo anti-money laundering (AML), know your customer (KYC), and combating the financing of terrorism (CFT) checks to ensure they have no criminal records and are not involved in activities that can harm the financial system.

NPCI's negative registry

BC agents must not be listed in the NPCI's negative registry, which includes individuals or entities identified with previous fraudulent or suspicious activities.

Visibility of the acquiring bank's branding collaterals

The presence of the acquiring bank's logo at the service point and on relevant portals, such as ARCS, and communications, such as SMS, helps reinforce the legitimacy and oversight of the banking services provided.

RBI's draft guidelines on due diligence of AePS touchpoint operators also mandate banks to update KYC for AePS agents who have not conducted financial transactions for six consecutive months before it enables them to transact further. Moreover, a bank can onboard only one AePS touchpoint operator.

Two-factor authentication for agents

Each agent must complete biometric authentication at the beginning of every transaction. Further, to enhance security protocols, acquirer banks must establish a system that automatically blocks any agent from the AePS service for 24 hours if they fail biometric authentication three consecutive times.

However, many agents find this system counterintuitive and complex because it means they must always be present to authenticate transactions. Hence, they cannot delegate the authority to coworkers at the outlet. Moreover, if a fingerprint does not match for any reason, it is logged as incorrect or a mismatch, which can lead to the biometric devices being blocked. Nonetheless, some providers seem to believe this requirement is useful as an additional layer of security. However, no data is available to support this belief.

An agent's conundrum

Aslam, a 39-year-old agent from Tughlakabad, Delhi, shared his difficult experience of being locked out of his device due to biometric mismatches.

> The bank has issued this new guideline that requires us to verify our fingerprints before each transaction. Before, we needed to verify ourselves only a few times a day, but now they have made it mandatory for each transaction. This is becoming difficult because sometimes, I accidentally ask the customer to place their finger on the scanner first, which causes errors. Three of my devices got blocked, and I had to buy new ones. I have already lost INR 8,000 (USD 95) in this process. A training session on how to use this new verification system will be helpful.
>
> **- Aslam, an exclusive BC agent, Tughlakabad, Delhi**

Every time Aslam made an error entering his fingerprint details, the device would lock him out. Although BCNMs could have helped him regain access to his device, he was unaware of this. As a result, he kept buying new devices to resolve the problem.

Increased security in biometric data capture

The UIDAI implemented an advanced artificial intelligence or machine learning (AI or ML) technology known as the Finger Minutiae Record-Finger Image Record (FMR-FIR) modality to enhance the security of AePS transactions. It includes two key components—finger minutiae and finger image—to authenticate fingerprints more accurately during transactions. Its features include a liveness detection capability, which helps distinguish between actual live fingerprints and cloned or fake counterparts to prevent spoofing attempts.

Moreover, the introduction of facial authentication to AePS is also expected to provide customers with enhanced security and a higher transaction success rate than fingerprint authentication. Facial authentication offers an 84% success rate compared to 81% using fingerprints and can even be used by users with physical disabilities or whose fingerprints have worn off. It is also easier to deploy in sensitive environmental conditions, such as dusty weather and rain, as it only requires a smartphone camera and no additional hardware. As of now, liveness detection and advanced AI/ML capabilities have been added to facial authentication to help fight deepfake cases. This could potentially reduce instances of AePS fraud by offering better protection against biometric spoofing.

Let us return to Kiran and Radha’s story to understand the next steps after a fraud occurs. Radha followed Kiran’s advice and filed a complaint with her bank. The issuer bank adhered to the NPCI’s guidelines and reported the fraud within five working days. They documented the incident details and Radha’s account history and filed the FIR.

The acquirer bank also conducted a thorough investigation and submitted a report in five days. They confirmed that Gautam, a BC agent from Hardoi, conducted the fraudulent transaction, which cleared Kiran of any wrongdoing. The acquirer bank accepted financial liability and processed the chargeback through the *Aadhaar* Reconciliation and Chargeback System (ARCS) portal. The bank also added Gautam’s name to the NPCI negative BC registry. Further, a police case was registered against Gautam under Section 318(4) of *Bharatiya Nyaya Sanhita* and under Section 66 (C) and (D) of the

Information Technology Act, and he was eventually arrested. Radha finally received the disputed amount, and Kiran felt vindicated.

While Kiran and Radha eventually had a positive outcome, the resolution rate for most fraud-related cases remains pitifully low. MSC's study suggests that a mere 17% of complainants recovered their funds completely, with the remaining incidents being unresolved or taking considerable time to address. Identifying and locating fraudsters is particularly challenging when cases are not reported promptly, as delayed reporting reduces the likelihood of successful investigations. This gap in enforcement allows fraudsters to evade consequences, which encourages further fraudulent activities due to a perceived lack of deterrence. As a result, the absence of timely action and resolution undermines efforts to curb such incidents and encourages others to exploit vulnerabilities in the system.

The fate of AePS and the frauds that haunt this service

Despite these measures, AePS frauds continue to rise. Fraudsters are constantly innovating to develop fraud methods, which include new social-engineering methodologies, new technologies to capture and replicate fingerprints, and workarounds for liveness detection.

MSC's findings suggest that loss of funds to fraud in CICO can erode trust in digital financial services. Lack of trust acts as a barrier, much like other challenges faced by unserved and underserved customers, such as distance, cost, and strict KYC requirements, all of which hinder the broader goal of financial inclusion. The AePS ecosystem must enhance its fraud management and protect the interests of all stakeholders involved to maintain trust in the system.

Stakeholders must make concerted efforts to address the rising challenge of fraud, inhibit fraudsters, and educate customers to be more vigilant against potential fraud attempts. Regulators, banks, CBCs, and other grassroots organizations still need to undertake several focused efforts to curb AePS fraud effectively such as:

Stakeholders	Steps to strengthen
Regulators and policymakers (RBI, NPCI, UIDAI)	**Strengthen the storage of biometric data to prevent leakages:** Regulators and policymakers must ensure robust and secure storage of *Aadhaar*-linked biometric data to prevent cloning or misuse. They must define strict guidelines for biometric data collection and handling. They must ensure that all biometric data stored in government and private systems is encrypted with advanced cryptographic techniques, such as AES-256. They must enforce secure data transmission channels, such as HTTPS with TLS, to collect and transfer biometric data. **Mandate risk-based authentication:** The regulators must implement risk-based authentication for all AePS transactions to improve security and reduce reliance on biometric data alone. They should categorize transactions into low-, medium-, and high-risk levels based on factors, such as transaction amount, location, and frequency. Low-risk transactions can use minimal authentication, such as biometric verification with a fingerprint or iris scan, for activities, such as balance inquiries or low-value transfers. Medium-risk transactions should

Stakeholders	Steps to strengthen
	combine biometrics with a one-time password (OTP) or PIN for processes, such as moderate-value fund transfers or sensitive account information updates. High-risk transactions should require multifactor authentication, which includes biometrics, OTP, and device-based confirmation, for high-value transfers or changes to *Aadhaar*-linked account details. **Develop** anti-cybercrime toolkits: This can boost fraud prevention through FSPs' readiness assessment, real-time threat alerts, streamlined reporting via a centralized and unified fraud reporting platform built with AI or ML capabilities, and equipping law enforcement with cutting-edge tools and training to counter evolving cyber threats. For example, the Philippines has been using AI-powered fraud prevention tools to combat cyber crimes. **Fast-track the investigation** of the identified cyber crimes and impose rigorous punishment under the new criminal laws to deter future cases. Moreover, regulators should introduce policies that mandate a minimum complaint resolution rate and impose penalties for noncompliance, especially in cases where complaints remain unresolved for extended periods. **Enhance the customer awareness campaign efforts beyond awareness**: The regulators must design campaigns to raise affective awareness[8] to help individuals overcome the emotional biases and imbalances that influence their decisions when they encounter fraud. It should help people recognize the emotional triggers that scammers exploit, such as urgency or fear. For example, the UK's "Take Five" initiative effectively addresses this by acknowledging that victims may not lack awareness but struggle to act when overwhelmed by a "hot state." The campaign encourages strategies, such as pausing to reflect before responding, questioning the legitimacy of the situation, and contacting their bank or authorities for assistance if fraud is suspected. **Increase customer awareness about AePS and channels to raise grievances:** Regulatory bodies should raise awareness about digital hygiene practices. They can promote the use of masked *Aadhaar*, enable biometric locks, update PIN regularly, and closely monitor SMS alerts, particularly those from banks. Additionally, they can educate customers on how to report suspicious activities or fraudulent transactions easily through a CBC or bank or file a complaint on the National Cyber Crime Reporting Portal. The RBI's data on recent campaigns in India show that these campaigns have successfully encouraged people to file complaints, voice concerns, and seek resolution more effectively.
Banks	**Enhance biometric security**: Banks must use advanced biometric technologies with liveness detection to prevent the use of cloned

[8] Affective awareness: Affective awareness refers to the ability to recognize and understand the emotional responses or states that influence one's thoughts, decisions, and behaviors.

Stakeholders	Steps to strengthen
	fingerprints. Banks and CBCs can explore the possibility of integration of more advanced fingerprint capture methodologies to create systems that are resistant to spoofing. These include advanced fingerprint capture methods with the use of high-resolution scanners to capture detailed and accurate fingerprint images, capture both surface and subsurface details, combine fingerprint recognition with facial or iris recognition, and use AI algorithms to distinguish between genuine and artificial fingerprints. **Monitor transactions in real time**: Banks must implement real-time fraud detection systems with the use of machine learning and behavioral analytics that monitor transactions in real time and flag suspicious activities based on set thresholds, such as multiple failed attempts, unusual transaction sizes, or frequency. **Improve identification system**: Banks must ensure BC agents can be identified in transaction records in passbooks or bank statements by highlighting details about the BC agent, such as their ID and location. **Streamline reporting mechanisms**: Along with better communication on fraudulent transactions, banks must ensure customers have easy access to report fraud and understand the steps to take when they suspect fraudulent activity. Banks can strengthen and simplify the grievance resolution process for customers with a user-centric design approach, automatic escalation of grievances, and relevant status updates of the grievance on the bank portal. **Conduct effective customer education and awareness campaigns**: Banks must launch targeted campaigns, such as Airtel's latest campaign in India, to educate customers about scam calls and common fraud tactics. They must use multiple communication channels that use local languages to reach a wider audience. They should educate customers about linking their mobile numbers with bank accounts and encourage customers, especially vulnerable segments, to opt for SMS alerts to prevent fraudulent transactions. The creation of better communication mechanisms to identify and inform fraudulent transactions will help sustain customers' trust in AePS transactions. Banks should use phygital medium[9], such as online media—WhatsApp, Instagram, and Facebook—coupled with offline modes—billboards and posters—for wider outreach. Another critical component of customer education is content type. Banks should update customers about new methods of fraud and scams, such as video calls and the usage of AI for voice cloning.
Corporate BCs	**Strengthen internal checks and monitor BC agents strictly:** CBCs must implement internal checks and controls to reduce fraud. While some interventions are unique to the CBC, such as BC geo-location tracking,

[9] Phygital mediums: **Phygital (physical plus digital**) is a marketing term that describes blending digital experiences with physical ones.

Stakeholders	Steps to strengthen
	transaction limits based on the CBC's vintage, and agent onboarding criteria, others are common across the industry. - Create a mandatory checklist of the checks and controls that must be implemented regularly, such as training on fraud typology, strategies to preempt fraud, and promotion of best practices for digital hygiene to reduce fraud cases further. - Use a geofencing mechanism to establish specific geographies where agents can perform transactions. Transactions initiated outside these zones can be flagged or blocked in real time. - Deploy mobile device management (MDM) systems to enable remote locking or wiping of devices. These features can be activated when the device is tampered with or unauthorized access is detected. - Implement stringent monitoring and accountability measures for BC agents, which include measures, such as SIM card binding.[10] **Ensure greater transparency at the agent outlet:** CBCs must conduct regular audits to ensure that all agents display their agent ID at the outlets, disclose transaction fees, and inform customers about the GRM mechanism. - Design systems to store tamper-proof digital receipts for all AePS transactions conducted by the agent. These receipts should be accessible only through two-factor authentication—biometrics and OTP—upon request by a bank or regulatory body, particularly in transaction disputes or suspected fraud. - Implement a voice box system at agent outlets to instantly announce transaction amounts to customers. This system can verbally confirm the transaction amount and provide customers with clear and immediate visibility into the transaction details. **Conduct customized training programs for BC agents:** CBCs must continuously train BC agents on the latest fraud detection techniques and secure transaction practices. They must ensure they are well-equipped to identify and report potential fraud. The current BC agent network landscape consists of traditional, bank-linked BC agents and new-age FinTech-onboarded retailer agents. A standardized, in-depth training curriculum must be developed and delivered to all BC agents before the services are activated on their portals. **Real-time notification and control**: CBCs must ensure that customers are immediately notified about transactions conducted from suspicious locations. These alerts empower customers to take prompt action, such as

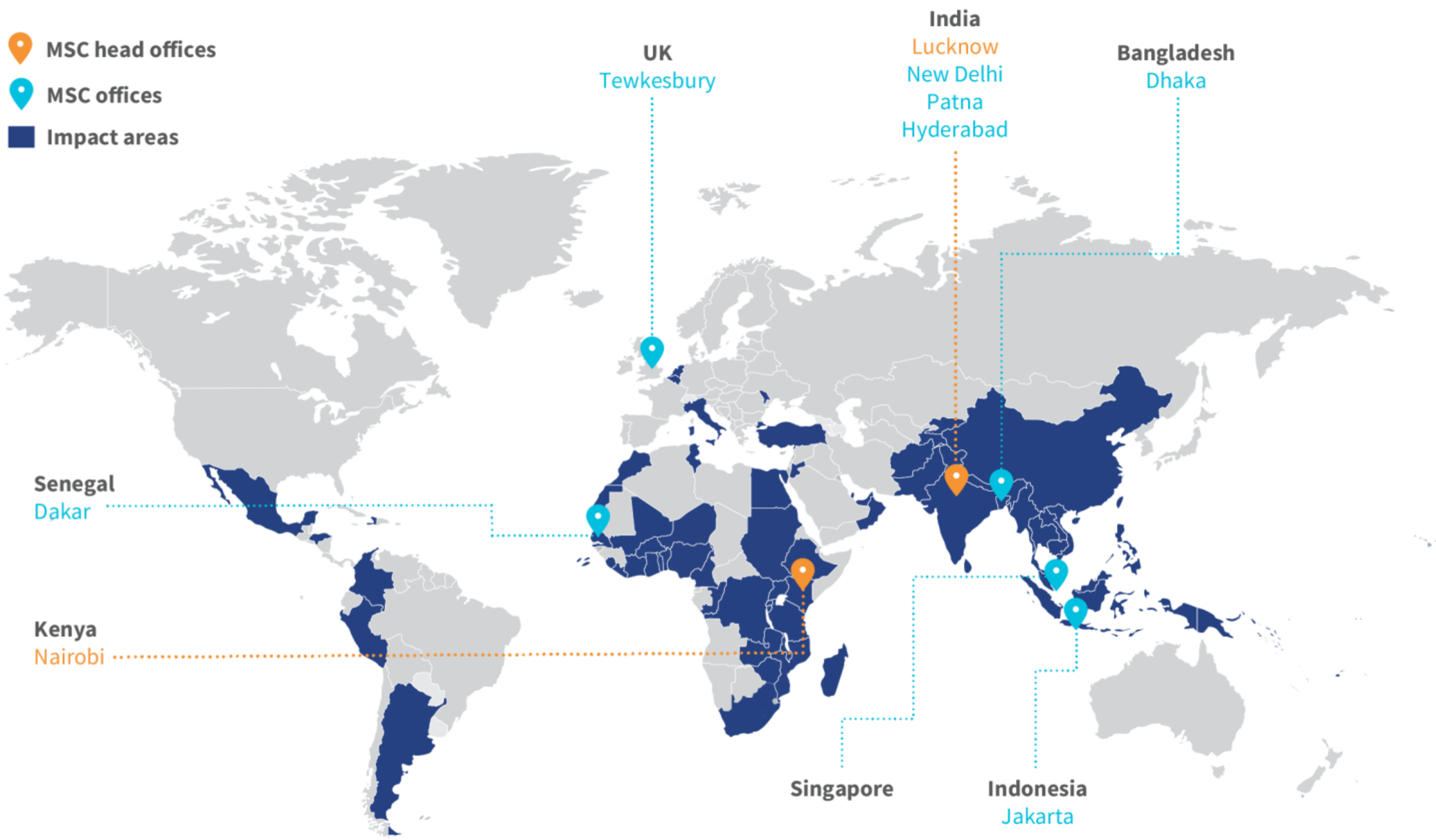
[10] SIM binding: It is a security feature designed to link a specific mobile application or service to the subscriber's SIM card on their mobile device. SIM binding helps ensure that only the registered device and SIM can access the service by associating a user's account with their unique SIM card. It adds an extra layer of protection against unauthorized access and fraud. Click here to learn more.

Stakeholders	Steps to strengthen
	reporting unauthorized activities or temporarily blocking their accounts, to prevent potential fraud.
Others (NGOs, grassroots organizations)	**Bolster customer education and awareness activities:** Grassroots organizations have already made efforts to educate customers about digital transactions and ways to prevent fraudulent transactions. For instance, the National Bank for Agriculture and Rural Development works with local communities to raise awareness about financial inclusion and secure banking practices. These organizations must organize workshops and community events where BC agents can interact directly with local communities, address their concerns, and build trust. Collaborate with government-run initiatives, such as common service centers (CSCs), to establish local training hubs focused on digital fraud protection. **Drive policy advocacy to improve digital transactions' safety:** Some grassroots organizations have also engaged in policy advocacy efforts to drive improved security in digital financial transactions. **For instance,** the Bihar Rural Livelihoods Promotion Society (BRLPS) has been advocating for the integration of security features in digital financial systems to protect rural consumers from fraud. The organization has worked on policies to promote secure digital financial practices across the state. **Promote financial literacy and transparency:** Grassroots organizations must run educational campaigns to raise awareness about the role and benefits of BC agents and banks and ensure transparency and understanding. These organizations should raise awareness about the steps customers should take if they suspect fraud or encounter a fraudulent transaction. Led by Malaysian banks and regulatory authorities, the campaign "Jangan Kena Scam" helped raise awareness about common online scams in Malaysia. A 2023 survey found that 56% of respondents acknowledged the campaign's role in helping them avoid falling victim to fraud. The initiative also highlighted a broader effort to boost digital financial literacy and reflected positive outcomes, such as a noticeable drop in scam encounters nationwide. **Localized helpline and GRM:** Establish a local helpline or community-based grievance resolution mechanism (GRM) to support customers in rural areas. This can enable them to register complaints and follow up on resolutions. For instance, SaferNet, a Brazilian NGO, partners with the Federal Public Ministry to combat internet crime and offers a helpline to report online scams, which include mobile money fraud.
Customers	**Safeguard their *Aadhaar* transactions:** Customers should lock their biometrics on the UIDAI portal, download masked *Aadhaar* from the my*Aadhaar* portal, and use it.

Stakeholders	Steps to strengthen
	Fraud reporting: If a customer suspects fraud, they should report it to the UIDAI through various channels, which include a helpline, email, the *Aadhaar Mitra* chatbot, or by filing a complaint on the *Aadhaar* website. Customers can also file complaints on the National Cyber Crime Reporting Portal (NCRP). **Monitor transaction notifications**: Customers must link a bank account to a mobile number and regularly check all SMS notifications, especially transaction alerts. **Verify transaction details**: Customers must confirm the transaction amount and details before they authorize any payment. They should always request a receipt after the completion of each transaction. **Always check the agent's credentials**: Customers must ensure that the agent that helps with the transaction is authorized. They should always request the agent's ID and verify it, particularly when they transact at a new or unfamiliar BC outlet or with an unknown agent.

Various stakeholders, which include the government, banks, and regulatory bodies, have taken steps to address AePS-related fraud, with opportunities for further improvement, as noted earlier. While these steps are important to mitigate immediate risks, their long-term efficacy in reducing fraud will take time to assess. Some measures, such as the integration of advanced biometric authentication and real-time fraud detection systems, require widespread adoption and rigorous testing before their impact becomes evident. The success of these efforts hinges on continuous improvement, collaboration, and the active participation of all stakeholders to foster a secure AePS ecosystem.

MSC
MicroSave Consulting



Asia head office

28/35, Ground Floor, Princeton Business Park, 16 Ashok Marg,
Lucknow, Uttar Pradesh, India 226001
Tel : +91-522-228-8783 | Fax : +91-522-406-3773

Africa head office

Landmark Plaza, 5th Floor, Argwings Kodhek Road
P.O. Box 76436, Yaya 00508, Nairobi, Kenya
Tel: +254-20-272-4801/272-4806

Email: info@microsave.net | Website: www.microsave.net