Dvara Research's Submission in Response to RBI Draft Directions for Comments on Due Diligence of AEPS Touchpoint Operators

In response to concerns of fraud perpetrated through the Aadhaar enabled Payments System (AePS), the RBI has issued (draft) directions[1] to all banks and to the NPCI for onboarding and ongoing due diligence of AEPS touchpoint operators.[2] The RBI's efforts towards making the AePS system safer and more secure for its users are welcome, as AePS frauds are a pressing concern from a customer protection standpoint. In addition to requiring banks and the NPCI to comply with due diligence protocols[3] and regular KYC updating for dormant operators, the rules state that *the NPCI and acquiring banks must ensure that any AePS touchpoint operator is onboarded only by one acquiring bank*.

RBI's decision, back in 2010, to not permit more than one acquiring bank for an AePS touchpoint operator[4], was taken based on the circumstances at that point, the nature of connectivity, the tech-preparedness (or lack of) for the levels of monitoring and scrutiny that banks had over their AePS touchpoint operators, among others. However, over more than a decade after the RBI decision, our observations from field research in 2022-23[5] indicate that the stringent requirement for AePS operators to only be associated with a single acquiring bank is not serving as a customer friendly practice overall. We find that this rule continues to cause inconvenience to both the customer and the AePS operator.

Frequent server downtime was reported as a persistent issue

Dvara Research has been studying the lived experiences of Customer Service Points (CSP) – these are the last-mile spokes of an extensive network of touchpoints across the country for the BC operations that are managed either directly by banks themselves or by BC network managers. Our interactions with CSPs revealed that transaction failures are a very common lived experience in offering cash-in cash-out services (CICO). While transactions may fail for reasons like insufficient balance, biometric mismatch, etc. CSPs are particularly troubled by frequent occurrences of server downtime or failure which cause transactions to fail. The NPCI, publishes statistics on unscheduled downtime of the AePS servers and on downtime incident by bank.[6] It reports data for instances where a volume of over 3 lakh transactions is declined for durations longer than 30 minutes. A narrower definition and an analysis of such incidents across geographies would help to understand the extent of server failure issues that prevent uninterrupted CICO from manifesting for the customer (an issue that has been established anecdotally from the ground).

---

[1] Aadhaar Enabled Payment System – Due Diligence of AePS Touchpoint Operators – DRAFT, RBI, July 31, 2024. Accessed from https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4475.

[2] These include Bank Mitras of any bank, and customer service points (CSPs) of banks or corporate business correspondent (BC) network managers, who use Aadhaar authentication.

[3] as laid out in the Customer Due Diligence procedure for individuals, stipulated in Part – I, Chapter – VI of the Master Direction – KYC, 2016.

[4] 6 Reserve Bank of India. (2010). Financial Inclusion by Extension of Banking Services – Use of Business Correspondents (BCs). Accessed from https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=6017.

[5] The field research was conducted as part of a study to update our understanding of India's Cash In, Cash Out (CICO) environment. Field interviews of 30 CSPs were conducted across 3 states between December 2022 – January 2023. This work is documented fully in the report published March 2024 titled Uninterrupted Cash In Cash Out: An Agent Success Model.

[6] See statistics published by NPCI at Declined (BD/TD) & Uptime.

When transactions fail, customers must be turned away from the service and agents lose the potential earnings on those transactions.

Agents operate multiple licenses[7] to avoid loss of business and trust due to server downtime

As a workaround for the recurring issue of server downtime causing AePS transaction failure, agents acquire CSP licenses from multiple providers at a time. This is a practice that has been observed by our researchers on the ground for many years now and has been corroborated by other stakeholders we have spoken to. Holding more than one license allows CSPs to switch servers and access the infrastructure of a second bank when the original acquiring bank is experiencing downtime incidents. As per RBI's guidelines on Financial Inclusion by Extension of Banking Services (2010), CSPs are not allowed to do this – they may not represent more than one bank at the point of customer interface. However, by doing so, CSPs ensure continuous availability of AePS withdrawal services to customers who approach them.

Server issues cause difficulty for the customer and CSP agent alike. In cases where money is debited from the customer, but the transaction fails due to server downtime, customers become distressed. Though these failures almost always result in an automated reversal to the customer's account, customers may not be aware of the same or may be worried about when such reversal will take effect. This is an important consideration as delays in reversals are common. CSPs reported that customers often question them regarding the validity of a transaction failure and accuse them of fraud. For agents, this is especially worrying as they take great efforts to cultivate trust and reputation within their communities over time. CSPs greatly value this trust and legitimacy and try to avoid it being broken.

We humbly submit that the practice of CSPs 'multi-homing' themselves by using the services of more than one acquiring bank makes for a more flexible AePS environment, providing continuity of services to the user. That said, the practice has evolved over the past few years and become a routine approach by which CSPs service their customers – this is evidence of the flexibility and customer convenience that the practice provides.

Fraud is still a concern that needs to be urgently addressed – but how?

The issue of fraud is significant and customer stories from the field reveal that the experience of bad service leaves the customer hapless and unable to find recourse in an effective, fair, dignified, and quick manner.

Some bad actors among CSPs may cheat customers of their money using the pretext of server failure or thumbprint mismatch. Several contextual factors may be implicated in their modus operandi, such as targeting customers who do not have mobile phones or access to the mobile number linked to their bank account, elderly and illiterate customers, and so on. Arguably, requiring AePS touchpoint operators to be onboarded only by one acquiring bank may not be able prevent such instances of fraud. A CSP holding even a single license can defraud customers by claiming a transaction failed and not handing over money after a successful debit.

Far more concerning are the large-scale fraud incidents which tend to emerge far upstream of the AePS environment. For instance, when biometric data is leaked by improper data handling practices of unrelated other entities, it is then acquired by bad actors who then pose as genuine customers and withdraw from bank accounts of victims at CSP operator touchpoints. The UIDAI

[7] We use the word 'license' in this note to depict the contract the CSP gets into with the acquiring bank/ BC Network Manager.

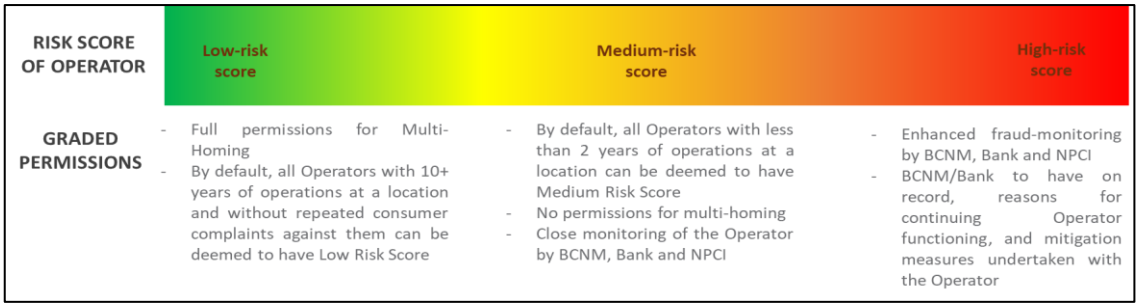
has now implemented liveness checks to reduce the incidence of such fraud[8]. Requiring AePS touchpoint operators to only be onboarded through one acquiring bank may be effective in preventing organised fraud perpetrated by bad actors posing as CSPs. But for CSPs who genuinely want to service customers and make a viable business of it, they can quite easily find a workaround to this rule by operating multiple licenses obtained in the names of their family members.

We understand that balancing customer protection against flexibility and customer convenience is an important prerogative for the RBI and NPCI. While the NPCI's proactiveness in trying to plug system-level gaps that lead to fraud is appreciated, we humbly submit that the RBI and NPCI may consider alternative approaches which could allow for multi-homing but be effective at curbing fraud. The time is opportune for revisiting and updating the regulatory and supervisory design aspects of the BC model in light of the many technological developments in the system but also the evolving needs of customers and of the CSPs themselves.

A risk-based approach to non-exclusivity of acquiring bank for CSPs

In an ideal scenario where CSPs could operate as white-label entities, they could formally leverage whichever bank's server provides them with the highest possibility of a successful transaction. As per the Mor Committee's recommendation, *"the White Label BC should be fully inter-operable and will have the ability to work with multiple banks at the back-end".*[9] In this manner, inefficiencies for both agents and customers due to failed transactions can be resolved, leading to much better outcomes for uninterrupted CICO services across the length and breadth of the country. White labelling of the CSPs delinks the transaction status from the ability of the acquiring bank infrastructure to complete a transaction, and this can become a possibility provided appropriate safeguards are upheld. ***Non-exclusivity may be enabled by requiring banks and the NPCI To adopt a graded, risk-based approach.***

There is precedence for this in RBI's recently released Draft Framework on Alternative Authentication Mechanisms for Digital Payment Transactions (2024) where RBI has stipulated that issuers may adopt a risk-based approach in deciding the appropriate alternative factor of authentication for a transaction, based on the risk profile of the customer and / or beneficiary, transaction value, channel of origination, etc. Also, the draft directions under question already requires such a risk-based approach for monitoring the activities of AePS touchpoint operators in relation to transaction limits to be set for AePS touchpoint operators based on their risk profile.



[8] UIDAI. (2023). New 'liveness' check to be done for Aadhaar fingerprint scans: Centre. Accessed from https://uidai.gov.in/ml/media-resources-ml/media-ml/aadhaar-in-prints-ml/13827-new-liveness-check-to-be-done-for-aadhaar-fingerprint-scans-centre.html

[9] Report of the Committee on Comprehensive Financial Services for Small Businesses and Low Income Households, Chair: Dr. Nachiket Mor, RBI, 2014

There is great value in leveraging the real-time data being generated through the AePS network to monitor activities of AePS operators. For instance, using geo-tagged transaction level data can help to discover patterns indicative of both innocuous multi-homing as well as real fraudulent activity. The same data may be used to allow for a risk-based approach which can determine select last-mile CSPs to operate in a non-exclusive manner. For instance, operators who have been regularly active, have a long history of undertaking CICO transactions in the exact location, operators who do not appear in the NPCI blacklist, who do not have a history of customer complaints, etc can be assessed by acquiring banks as well as by NPCI itself, depending on where the data for each layer rests. Those agents who have a higher risk score may be disallowed from accessing the AePS servers through any bank other than the one which shows more prominent activity for. The risk rating mechanism may also incorporate the corporate BC's inputs on the given CSP operator. The score can be updated on a convenient cadence to allow for genuine operators to expand their business and customer-convenience offerings. Such a system would make for improved fraud monitoring in addition to an overall more flexible and customer friendly CICO environment.