Improving Cash Benefit Transfers - The Role of Biometric Authentication Failures

Authors: Laveesh Bhandari and Sumita Kale[1]

Abstract

India’s Direct Benefits Transfer programme has achieved phenomenal coverage and success in reaching beneficiaries, however gaps do remain. One of the challenges in withdrawing cash from the beneficiary account is failure in biometric authentication, which results in significant inconvenience and loss to the beneficiaries. This paper focuses on this critical gap that mars the objective of seamless delivery of cash benefits to the targeted beneficiaries. The paper notes that with improved training and monitoring, some investment in maintenance and superior scanning equipment, and effective grievance redressal mechanisms, a large share of failures can be eliminated. However, the first step towards improving the delivery of cash benefit transfers lies in identifying the precise causes of authentication failure and putting out detailed data on failures in the public domain. Improved public monitoring of this critically important and growing national service is essential.

[1] Laveesh Bhandari and Sumita Kale are with the Indicus Centre for Financial Inclusion. The authors would like to acknowledge inputs from Pranav Kumar and Anand Raman. This paper however contains the views of the authors who can be contacted at laveesh@indicus.org and sumita@indicus.org

1. Introduction

The Direct Benefit Transfers (DBT) programme in India has been evolving since its launch in January 2013, from the initial pilots covering 27 schemes to 312 with a record 980 million beneficiaries receiving cash transfers and 819 million receiving benefits in kind in 2020-21[2]. Despite its phenomenal coverage and success in reaching beneficiaries, gaps do remain[3], both in the direct transfer of cash benefits to the beneficiaries' accounts and its withdrawal by them. One of the primary causes of the latter is failure in biometric authentication, which results in significant inconvenience and loss to the beneficiaries[4]. This White Paper focuses on this critical gap that mars the objective of seamless delivery of cash benefits to the targeted beneficiaries.

It is important to flag at the outset that transaction failures do not always translate into denial of dues to beneficiaries. However, there is significant time and cost to the beneficiary in resolving the issue[5]. Moreover, a weak redressal mechanism results in some issues remaining unresolved and some taking a long time to get resolved. In any case, grievance redressal takes time and expenses, which are costly for low-income beneficiaries. Biometric authentication failures in accessing cash benefits through the Aadhaar-enabled Payment System reportedly stand at around 20 percent of transactions[6]. Though this figure is not based on any adequate nationally

[2] Data from https://dbtbharat.gov.in/

[3] See ICFI White Paper, "Direct Benefit Transfer: Status and Challenges Ahead", July 2021.

[4] See Appendix for some non-biometric challenges that need to be addressed.

[5] Transactions failures do not automatically result in exclusion, as the transaction may go through in subsequent attempts. In order to determine the extent of exclusion due to transaction failures, as well as estimation of the time and expense spent by the poor in resolution of the problem, the government should institute a nation-wide large sample survey.

[6] Economic Times, dated August 26, 2020. Also see Mint, 8th May 2020 on AePS failure rates

representative survey, the possibility that a fifth of the transactions failed at least once due to a biometric related reason, calls for deeper study.

A recent study by Dvara Research (2022) focusing on exclusion risk has looked at all stages in the DBT pipeline.[7] When it came to cash withdrawal from the account, biometric authentication failures was among the top three causes. The study reported that 20.7% of the respondents attributed cause of failure to access their cash to be biometric mismatch. The recourse stated was to visit the nearest Aadhaar Enrolment Centre to update the biometrics, but only 45.6% of those who faced the issue reported successful resolution of the problem. The study admittedly only provides indicative results, since the underlying survey was not nationally representative; however, the failure rates and reasons are a cause of concern.

A performance audit by the Comptroller and Auditor General India (CAG)[8] of the functioning of the Unique Identification Authority of India (UIDAI) revealed that the UIDAI did not have the data to ascertain the reason behind authentication failures. However, it did indicate that in cases of failure of fingerprint authentication in the first attempt, subsequent attempts may succeed. And that related to (at least partially) address connectivity issues, buffer authentication had been allowed[9].

[7] Initiative, Social Protection, 2022. "State of Exclusion -Delivery of Government-to-Citizen Cash Transfers in India." Dvara Research. Available at https://www.dvara.com/research/wp-content/uploads/2022/06/State-of-Exclusion-Delivery-of-Government-to-Citizen-Cash-Transfers-in-India.pdf

[8] Comptroller and Auditor General of India, Report No.24 of 2021 - Union Government (Ministry of Electronics and Information Technology), Performance Audit on Functioning of Unique Identification Authority of India, available at https://cag.gov.in/en/audit-report/details/116042

[9] As per Aadhaar Authentication API Specification - Version 2.0 (Revision 1) February 2017, "AUAs can buffer authentication requests and send it to Aadhaar authentication server to support occasional lack of network connectivity on the field. Maximum time up to which requests can be queued (buffered) will be defined by UIDAI policy. Currently, this will be configured to 24 hours and may be changed as per policy. All

In the absence of available analysis for the reasons behind authentication failures, the CAG looked at the number of voluntary up-dation requests of biometrics by Aadhaar holders[10]. It concluded:

> *"the need for biometric update could arise on account of authentication failures (called "false rejects"- where a correct resident with a valid Aadhaar Number is incorrectly rejected) due to incorrect biometric capture or poor biometric quality captured at the time of enrollment. Thus, a significantly high percentage of voluntary biometric updates indicated occurrence of a high volume of authentication failures, which compel Aadhaar number holders to update their biometrics."*

In this paper we study the role played by biometric authentication in transaction failures, the protocol for ensuring that each beneficiary gets their due and conclude with some solutions for resolving the existing issues that mar the process.

2. Biometric Authentication and DBT

Biometric information such as fingerprint, finger vein patterns, iris scan, and facial and even voice recognition help in capturing unique identification details pertaining to an individual. As no two individuals have the same biometric details, it is accepted as the most scientific method to prove identity. In practice, however, there are various gaps and glitches in implementation, and also technological challenges, that can lead to less-than-optimal performance of the biometric authentication mechanism. In the Indian context the biometric

requests with "ts" value older than this limit will be rejected." Available at https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf

[10] Out of the successful updates in 2018-19, 0.81 Crore (26.55 per cent) were mandatory and the remaining 2.23 Crore (73.45 per cent) were voluntary updates. Comptroller and Auditor General of India Report No. 24 of 2021

based Aadhaar has undoubtedly contributed immensely to the success of India's financial inclusion objective. Aadhaar captures fingerprints, iris, and photograph of the individual, along with some proof of name and residence at the time of enrolment.

The wide coverage of Aadhaar[11] set the stage for the opening of bank accounts through the Pradhan Mantri Jan Dhan Yojana (PMJDY) for the underprivileged, mainly in rural areas, thus providing infrastructure for direct transfer of cash to the beneficiaries. Once cash is transferred to the accounts, beneficiaries access the funds, through banks and banking correspondents. This involves authenticating their identity by submitting their Aadhaar number and their biometrics, mainly fingerprints. At the Proof-of-Concept (POC) stage in 2012, the accuracy of biometric authentication was placed at 98% and 99% for fingerprint authentication and iris authentication respectively[12].

However, these figures are from a POC, and real-world implementation has many issues that are not operating at that stage. Recognizing the possibilities of authentication related errors, and trying to minimize them, the UIDAI and DBT Mission have put in place a protocol for addressing the issue of failure. However, protocols themselves are not always followed. An error at the biometric data collection stage creates additional interaction with the system necessitating perhaps multiple visits to the bank branch/ Business Correspondent outlet/Aadhaar enrolment centre and costing the beneficiaries in time and expenses, as well as potential exclusion.

[11] Aadhaar saturation of adult population stands estimated at 100.88% on 31st March 2022 Some states like Gujarat, Jharkhand still lag, with less than 98% saturation. https://uidai.gov.in/images/Aadhaar_saturation_report-as_on_31-03-2022.pdf

[12] Rajya Sabha unstarred question No. 400, 20th July 2018, https://uidai.gov.in//images/rajyasabha/RSPQ400(Unstarred).pdf

The key question that arises is, given the relatively successful spread of Aadhaar and a robust banking network across India, what are the reasons behind biometric authentication failure that prevent beneficiaries from accessing their government given benefits with ease? And how can these be reduced.

3. The Biometric Challenge

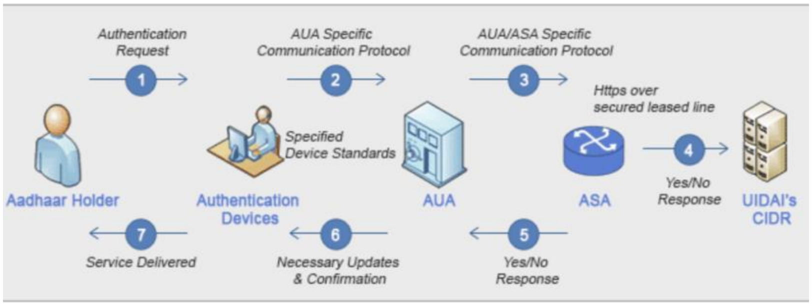
Biometric failures can occur for many different reasons related to poor quality of the underlying body part (e.g. fingerprint, or iris), poor quality of instrument, poor practices followed, network failures, technical failures, etc. Since there are multiple agencies involved – Banks, Business Correspondents (BCs), National Payments Corporation of India (NPCI), UIDAI, telecom company, etc., it is critical to (a) identify specific causes of the failure and (b) intimate the specific cause to the concerned stakeholders. This process is fairly weak currently, and therefore there is inadequate information in the public domain on the relative importance of various failures.

This section first looks at the authentication platform, the NPCI, and follows that with the underlying biometric platform, the UIDAI. It then briefly discusses the alternatives and their challenges and ends with a discussion on the need for a comprehensive and easily accessible customer grievance redressal mechanism.

3a. The Authentication Platform

As an Authentication Service Agency, the National Payment Council of India (NPCI) operates two platforms that play an important role in the government's Direct Benefit Transfer programme. The first is the Aadhaar Payments Bridge (APB) through which transfers are made from the government's account to the individual account which is linked to the beneficiary's Aadhaar number. There is no biometric authentication needed at this stage for the money to reach the beneficiary account. The second, that comes into play sequentially, is the Aadhaar Enabled Payment System (AePS) which enables the beneficiary to withdraw cash from her account using biometric authentication through Micro ATMs at BCs.

Figure 1 Aadhaar Authentication Process Flow


Authentication Request
1
AUA Specific Communication Protocol
2
AUA/ASA Specific Communication Protocol
3
Https over secured leased line
4
Specified Device Standards
Aadhaar Holder
Authentication Devices
AUA
ASA
Yes/No Response
UIDAI's CIDR
7
Service Delivered
6
Necessary Updates & Confirmation
5
Yes/No Response

Source: https://uidai.gov.in/ecosystem/authentication ecosystem/operation-model.html
Note: AUA - Authentication User Agency; ASA – Authentication Service Agency; CIDR- Central Identities Data Repository

It must be noted that previous policy action has led to significant improvements at the APB stage. That is, coordinated action between the MoF/DBT mission, RBI, NPCI and banks has led to a standardization of responses for APB returns resulting in identification of the cause of the failure thereby reducing transaction failure rates in the APB or the first stage of the mechanism.[13] However such efforts have not yet occurred in the AePS platform resulting in continued challenges at identifying causes behind transaction failures. We discuss these later.

Currently, NPCI classifies transaction failures in AePS under two categories [14], (a) Business Declines, which are due to errors by stakeholders, such as insufficient balance in the account,

[13] Arun Sharma, "Transaction Returns/ Failures in DBT Payments", July 21, 2020, available at https://www.linkedin.com/pulse/transaction-returns-failures-dbt-payments-arun-sharma/

[14] See NPCI Circular on AePS transaction failure codes https://www.npci.org.in/PDF/AePS/circular/2018-19/NPCI2018-19AEPS008.pdf

incorrect PIN etc, and (b) Technical Declines that are due to technical shortcomings like connectivity issues, switch unavailability, invalid response etc. From data available in the public domain, as of October 2018, NPCI had identified 197 reasons for failures under AePS, of which 108 codes were assigned under different causes of Technical Declines and 89 codes under Business Declines. Failures due to biometric issues are classified under either category depending on the specific causes.

Unfortunately, there is limited data in the public domain on the more precise reasons for failure; and it is not even clear how this code-level data is shared between policy-making and regulatory bodies. However, we can still glean some insights from other data. Approved transactions under AePS and share of Business Declines and Technical Declines are available for 50 banks monthly since August 2021. The latest figures for March 2022 are presented in Table 2 below for the top ten banks which account for three quarters of the aggregate volume of 50 banks. While the failure rates vary across the banks, it is clear that Business Declines are significantly higher than Technical Declines. While there is no granular data available in the public domain for individual reasons under the categories, this appears to match anecdotal reports cited earlier[15] that biometric authentication under AePS has significant failure rates, approximating 20% of failures.

[15] Dvara Research, 2022, Economic Times, dated August 26, 2020. Also see Mint, 8th May 2020 on AePS failure rates,

Table 1 AePS Top 10 Bank Statistics for March 2022

Sr No	Issuer Bank Name	Total Volume of Transaction (Mn)	Approved %	Business Declines %	Technical Declines %
1	State Bank of India	84.14	74.52	20.85	4.07
2	Punjab National Bank	29.12	79.59	15.81	4.02
3	Union Bank of India	25.85	77.48	13.33	8.64
4	Bank of Baroda	25.54	63.35	34.57	1.51
5	Indian Bank	23.78	67.74	16.25	15.48
6	Central Bank of India	21.92	80.89	15.9	2.6
7	Baroda Uttar Pradesh Gramin Bank	16.87	70.92	23.87	4.52
8	Bank of India	15.21	74.51	17.03	7.86
9	Canara Bank	10.56	82.58	15.57	1.36
10	India Post Payment Bank	8.06	65.78	19.96	13.72

Source: NPCI https://www.npci.org.in/statistics/bd-td-and-uptime

As more granular data may be confidential and therefore difficult to put in the public domain, other avenues of information sharing between the different players need to be evolved. The DFS/DBT mission, NPCI, Indian Banks Association (IBA) and RBI would need to develop a coordinated approach on this issue of data sharing especially related to transaction failures.

3b. The Biometric Platform

Currently Aadhaar authentication can take place in four modes (See Box) – demographic authentication, One Time Pin (OTP), Biometric-based authentication of fingerprint or iris and a combination of any other three.

Box: Modes of Authentication through Aadhaar

1. **Demographic authentication**: The Aadhaar number and demographic information are obtained from the Aadhaar number holder and matched with her demographic information in the Central Identities Data Repository (CIDR).
2. **One-time pin-based authentication**: A One Time Pin (OTP), with limited time validity, is sent to the mobile number and/ or e-mail address of the Aadhaar number holder registered with the Authority. The Aadhaar number holder provides this OTP along with his Aadhaar number during authentication and the same are matched with the OTP generated by the Authority.
3. **Biometric-based authentication**: The Aadhaar number and biometric information submitted by an Aadhaar number holder are matched with the biometric information of the said Aadhaar number holder stored in the CIDR. This may be fingerprints-based or iris-based authentication or other biometric modalities based on biometric information stored in the CIDR.
4. **Multi-factor authentication**: A combination of two or more of the above modes may be used for authentication.

Source: https://uidai.gov.in/ecosystem/authentication-ecosystem.html

According to data from the Aadhaar Authentication dashboard[16] , which is not exclusively for DBT, 96% of the authentications are from fingerprint, 2% from OTP, 1% from demographic authentication, and iris is less than 1%[17].

[16] Data is for authentication for all purposes, not exclusively for DBT https://uidai.gov.in/aadhaar_dashboard/

[17] These figures are from 1st to 14th April 2022 and therefore only indicative of the share of various authentication options.

Biometrics from the customer are captured initially at the stage of being registered for Aadhaar, and subsequently at the cash out point. The UIDAI has stipulated that only registered devices are used for the capturing biometric information, and this is critical to ensure accuracy of the data collected. Device suppliers are also certified by the UIDAI. However, in the absence of appropriate audit[18], it is not clear whether older un-registered devices are also being used, impacting efficiency and security.

The authentication requesting entities have a choice between iris and fingerprint for biometric authentication, however fingerprint scanners are used more often as they have moderate costs, and rate high on usability and accuracy. Iris scanners also rate high on security and accuracy, and high on usability, but their costs are significantly higher.

While there can be issues of normal wear and tear and need for calibration of the instrument that affect both fingerprint and iris scanning, industry discussions suggest that authentication failures typically arise in the case of fingerprint scanning. Since iris scanners are relatively costlier, most agencies only use the fingerprint scanning facility offered by Aadhaar.

For instance, fingerprints are not captured well with unclean or dry hands, or due to age and physical work fingerprints may be worn, etc. Cleaning the fingers, repeat scanning, and scanning of other fingers and not just thumbprint, are the first level solutions. There are also the abovementioned challenges related to poor maintenance of scanners. And these may occur at Aadhaar enrolment stage (under the ambit of UIDAI), or at the cash out point (BCs). Both entities need to ensure the following of protocols to minimize these failures. From what the available data suggests, it is apparent that the mechanism

[18] Comptroller and Auditor General of India, Report No.24 of 2021 - Union Government (Ministry of Electronics and Information Technology), Performance Audit on Functioning of Unique Identification Authority of India, available at https://cag.gov.in/en/audit-report/details/116042

needs to improve. Better management and strict monitoring and enforcement of protocol of the scanning process is critical to further reduce failures.

Yet there are increasing calls for incorporating other forms of authentication over and above that of fingerprint and iris. In August 2020, the government, NPCI and UIDAI began looking to test authentication through facial matching. While the UIDAI has reportedly asked intermediaries to increase deployment of iris scanners, the use of facial matching had moved to the Proof-of-Concept stage last year (Lok Sabha, 28th July 2021).

It is obvious that to better understand where India's priorities in terms of biometric authentication lie, it is critical to have data on where the transaction failures are occurring in the whole chain of information flows from the beneficiary to the UIDAI and back. Having said that, we discuss the characteristics of other forms of authentication within the Indian context.

3c. Biometric Alternatives

Facial matching, especially real time facial matching has two key advantages. First, it does not require a specialized scanner like that for fingerprint and iris. Any decent camera-based smartphone would be adequate for the purpose at hand. Second, since it is real time, and visible, there is no need for the beneficiary/customer to visit the bank branch (or the outlet of any Authentication User Agency (AUA) physically. In other words, it can help create and open up a whole new market for a range of financial products and services.

However, facial matching is not without its own challenges, including but not limited to, quality of camera, light conditions, changing facial characteristics etc. Therefore, we need to develop the right set of guidelines and best practices, and also ensure that legal issues related to customer protection are addressed. Simultaneously a mechanism of close monitoring, quick identification and rapid enforcement must be in place.

And therefore, while piloting this is a good idea, a rapid scale-up is not advisable without identifying and putting in place appropriate checks and balances.

The OTP based authentication has not scaled up in usage in the DBT domain. This requires the mobile number to be connected with the Aadhaar. While many have connected the two, and numbers are steadily increasing, there are many complications that need to be better understood. The first is related to frequently changing cell numbers of those at the bottom of the pyramid and difficulty in accessing the Aadhaar Permanent Enrolment Centres to update the number. Another associated issue is that in many households, many members share the same mobile. Telecom connectivity failures can also sometimes get in the way. And therefore, OTP authentication does not necessarily address the problem of transaction failures due to use of biometrics and can further complicate access.

To summarize therefore, in our view, the superior option before us is to continue focusing on perfecting the existing fingerprint authentication mode and enhancing the use of iris authentication as a backup. The non-biometric based OTP is also inadequate for those at the bottom of the pyramid. Moreover, facial authentication may have great potential, but requires intensive piloting and study.

3d. Self-Corrective Mechanisms

Stable and mature ecosystems by definition have well-functioning mechanisms to identify hurdles in the smooth working of their various parts, provide such data and information to the right set of stakeholders, and have well defined ways of ensuring corrective action.

The first such mechanism is related to informing a customer (and in this case also the BC) of the failure and the specific reason behind it. This currently does not occur. An even better customer-oriented solution would also inform within the same message of the right entity to connect with to ensure corrective action can be taken promptly.

The second such mechanism is a well-functioning grievance redressal mechanism. Studies including those conducted by the authors[19] have previously laid out the challenges and solutions in having a good customer grievance redressal mechanism in the financial inclusion domain. In the case of biometric authentication failures, the BC, Bank, NPCI, UIDAI, RBI and the DBT Mission are the key players that would have to coordinate.

The third possible tool is allowing for a manual over-ride for a high enough functionary in the DBT payments chain. This will also benefit those who have physical disabilities or are bed-ridden. However manual over-ride could also be misused if not designed and implemented well in terms of efficient checks and balances.

4. Way Forward

To summarize, lack of specific information/data available within the ecosystem on the reasons behind the authentication and transaction failure, prevents any entity from identifying the corrections required. At the ground level, lack of monitoring and implementation of best practices and SOPs related to scanning of biometrics may be behind a significant proportion of failures. At the systemic level, coordination failures between multiple overseeing entities including regulators, government departments, key platform providers and banks further impacts the ability of the system to identify and correct the errors. Finally, weaknesses in the customer redressal mechanism prevent the necessary information and demand from the beneficiaries for such failures.

[19] ICFI Policy Brief, Consumer Grievance Redressal in a Digital World, August 2017, available at https://www.indicus.org/admin/pdf_doc/Policy-Brief-August-2017.pdf.pdf

4a. Improving Coordination to Smoothen Systemic Issues

Better coordination and integration: The NPCI is a key service provider in the ecosystem and has doubtlessly been able to rapidly build a well-functioning payments platform. Increasingly, as the challenge is more towards ensuring superior service quality, inputs from diverse stakeholders need to be made available for ongoing improvements in the NPCI platform. And therefore, representatives from UIDAI, BCs and even consumer interest groups need to be included in the NPCI steering committee.

SOPs for AePS transactions: The Ministry of Finance needs to lead the coordination between the DBT Mission, NPCI and UIDAI to put in place SOPs for AePS transactions. An exercise that enabled coordination between the DBT Mission, RBI, NPCI and banks led to standardisation of responses for APB returns[20]. This has resulted in the identification of the precise cause for failure in the movement of funds from the government to beneficiary bank account component of the chain.[21] A similar exercise is required for AePS transactions where Banks and BCs are also included in the coordinated approach.

4b. Improved Data Capture and its Availability

SOPs for AePS transactions: Without very specific data, the root cause of failure will remain unknown, and resolution cannot take place. Standardizing error codes across the system is needed for the AePS transactions. The DBT Mission, NPCI and UIDAI must coordinate to put in place SOPs, along with the banks and BCs.

[20] Arun Sharma, "Transaction Returns/ Failures in DBT Payments", July 21, 2020, available at https://www.linkedin.com/pulse/transaction-returns-failures-dbt-payments-arun-sharma/

[21] Data from the DBT Mission (Arun Sharma *ibid*) showed that the transaction failure rate rose during the first three months of the Covid lockdown, as a larger proportion of the DBT payouts were going directly to the accounts, rather than through the Aadhaar-based system.

Making data public: As much as is possible, data on reasons behind failures need to be made public on an ongoing basis by NPCI. The greater the geographical granularity (subject to confidentiality issues) of such data, the greater would be its effectiveness.

4c. Training, Awareness and Capacity Improvements

Training of BCs and Bank staff: It is critical that training at the last mile includes detailed SOPs and exception handling mechanisms already articulated by UIDAI and the DBT Mission. This includes a) best practices under Best Finger Detection, cleaning the fingers, cleaning and maintaining the scanner etc. as well as b) protocol for exception handling for Aadhaar based problems. Typically, market forces lead to improvements in service quality, but since market forces are not working in this case, it will need to be enforced top down. Two possibilities exist, either the RBI work from the regulatory side to ensure that Banks and BCs comply, or the DBT does so.

Improving Scanners for Biometrics: Reportedly the UIDAI is currently working on standardising specs for micro-ATMs and scanners to update from the 2013 standards. However, past experience shows that improved SOPs need to be supplemented by actions to implement them including training of BCs and awareness building measures. RBI as the key financial regulator must ensure that banks upgrade and ensure compliance in the field on an ongoing basis.

Iris Scanner in Every Bank Branch: Though it may not be feasible to place an iris scanner with every BC agent, in case of situations where a person's fingerprints cannot be captured well, the alternative of iris scanning should be available in the vicinity of all.

4d. Transactional and Tactical Issues

Ease of mobile number up-dation: UIDAI should facilitate easy up-dation of mobile number with the Aadhaar number, ideally at the touch point in the village – currently it is restricted to Primary Enrolment Centres, which may not always easily accessible to villagers.

Customer grievance mechanism: DBT Mission must put out first a white paper on the need for a grievance redressal mechanism along with basic structure related to assigning accountability to multiple entities involved in the process. It is critical that the agent on the ground and the beneficiary, both must be aware of the process in place for resolution of an issue – whom to contact, service resolution time, escalation process in detail etc.

Informing customers about reasons for failure: Reasons for failure must be communicated to the beneficiary and the BC/agent. This would require updating the code and software related to transaction failure. It must also include contacts of relevant entity to contact.

Manual over-ride: The DBT Mission can put in place guidelines for manual over-ride to ensure delivery of benefit if the Aadhaar authentication fails. The SOPs can include a) availability of fingerprint, iris and face authentication at all touch points, b) mobile OTP-based verification, c) identifying a responsible authority in the village for those beneficiaries who have disabilities, d) authentication at the door for those beneficiaries who are bed ridden. It is however critical that such over-ride is governed by a mechanism of checks against misuse.

To conclude, therefore, there are many tactical, informational, capacity and systemic issues that directly or indirectly lead to biometric authentic failures and by extension payment failures. We suggest specific action points by which they can be reduced. We argue that it is more important to address these underlying issues rather than identify other forms of biometrics to replace the current Aadhaar based fingerprint and iris authentication. This is because many of the current problems will remain irrespective of the type of biometric being used. While OTP is one such alternative that is growing rapidly, it has serious challenges related to those at the bottom of the pyramid, namely, sharing of a single mobile between many, and high turnover of mobile numbers among the poor. Facial matching does get around that problem and also that of inappropriate instrumentation and skills, but it has serious dangers of being misused. Therefore piloting, data collection, its analysis, and building appropriate checks and balances at scale are critical before it can be implemented on a national scale. Meanwhile with improved training and monitoring, some investment in maintenance and superior scanning equipment, and grievance redressal mechanisms, a large share of failures can be eliminated. Finally, detailed data on failures should be put in the public domain on an ongoing basis for improved public monitoring of a critically important and growing national service – the DBT.

***

Appendix: Selected Non-biometric Challenges

A. Removing 'dark spots' in DBT access

The RBI has already issued a framework for geotagging of payment system touch points with end customers.[22] When completely implemented this would enable the identification of specific areas or 'dark spots' where access options are missing or not commensurate with the population/potential customers. These 'dark spots' will then need to be brought under the BC ambit.

B. Network failures

The DFS needs to coordinate with the TRAI/DoT for putting in place a mechanism for monitoring, identifying and communicating to the Telcos specific points of network failures for their quick resolution. These issues have also been discussed in greater detail in earlier work[23].

C. Inter-Bank and Intra-Bank transactions

There is one more class of challenges related to when the acquiring bank and issuer bank are the same (ON-US AePS transactions), and when the acquiring bank and issuer bank are different (OFF-US AePS transactions). One, there are reportedly higher failure rates on OFF-US transactions compared to ON-US transactions. This issue was also highlighted in the Economic Survey 2016-17[24] where the decline rate for Aadhaar-enabled

[22] March 2022
https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=12260&Mode=0

[23] ICFI White Paper Direct Benefit Transfer: Status and Challenges Ahead July 2021 available at https://www.indicus.org/admin/pdf_doc/Direct-Benefit-Transfer-Status-and-Challenges-Ahead.pdf; ICFI Policy Brief Service Quality Standards in Telecom Connectivity for Financial Inclusion November 2015, available at https://www.indicus.org/admin/pdf_doc/20151203085012.pdf

[24] https://www.indiabudget.gov.in/budget2017-2018/es2016-17/echapter.pdf

payments under OFF-US transactions was nearly 56 percent, almost double that for ON-US transactions. This is a natural outcome of multiple organizations not following interoperable processes. Second, while Jan Dhan accounts have been opened predominantly by Public Sector Banks, the BC network has spread largely through private channels. As private banks and BCs moved in to benefit from the interchange fees, the share of OFF-US transactions in AePS increased from 4% in September 2016 to 51% in September 2021 as reported by SBI EcoWrap November 2021[25]. The RBI must take the lead in coordinating between NPCI, IBA, UIDAI and DBT Mission towards sharing data at a granular level for failures of ON-US and OFF-US transactions. The persistent difference in failure rates between ON-US and OFF-US transactions must be investigated in depth.

D. Splitting transactions

Some BCs, in a bid to earn more commissions from the interchange fees began to split a single transaction into multiple transactions. To reduce this practice, the NPCI advised issuer banks to put in appropriate "per user per day and per month, volume and value transaction limits"[26]. NPCI also advised issuer banks to put in a maximum limit of five transactions "per Aadhaar per terminal ID per day" as a best practice to prevent fraud. While the intent of these guidelines is to reduce fraud and enable a level playing field for issuer banks, the limits may in some cases also be leading to failures for beneficiaries to access their cash.

[25] As stated in the SBI Ecowrap November 2021, "The account opening bank pays an interchange fee to the operator of the BC/CSP when a customer makes a transaction at micro-ATM that does not belong to the account opening bank (i.e. OFF-US transaction). At present the interchange fee is 0.5% of transaction amount (min Re 1 and max Rs 15) for an OFF-US financial transaction and Rs 5-7 for nonfinancial transaction." https://www.sbi.co.in/documents/13958/10990811/08112021_Ecowrap_20211108.pdf/e1bfe492-c223-14a5-d0e7-6c9af2659162?t=1636365455515

[26] https://www.npci.org.in/PDF/AePS/circular/2019-20/Circular%2029%20Circular%20against%20the%20control%20measres%20for%20Split%20-%20standard%20investigation%20structure.pdf

E. Strengthening the legal basis of Aadhaar

Though this paper focuses on the DBT, it must be recognized that government benefit transfers are but one component of a larger ecosystem of digital financial transactions. This ecosystem needs to be held together by smooth, error free and trustworthy authentication. Aadhaar today is by far the most potent and well spread mechanism to enable that. Currently Aadhaar authentication is working under the constraints laid down in Aadhaar Act (Section 29) and the Supreme Court has also adjudicated on the matter. Aadhaar number collected for one government scheme cannot be used for another government scheme, even if under the same department. Moreover, private firms cannot use Aadhaar under UIDAI authentication. These legal challenges need to be addressed.