Consumer Protection

Fraud and scams

This barrier refers to the range of potential negative or deceitful interactions customers may experience when using DFS, typically involving unauthorized access to personal information or tricking someone into willingly sharing their information. Financial customers—especially novice users—can and have fallen victim to fraud and scams committed by mobile money agents, for example, who request customers' pins or charge fake fees.

Why is this barrier important?

While users experience fraud and scams, and while anecdotal evidence suggests frauds and scams are on the rise in some markets, evidence does not indicate that it directly or strongly inhibits access and use of financial services. The barrier is a side effect of the proliferation of technology, especially mobile phones. The fear of making mistakes can prevent women from utilizing the full range of DFS products and services available to them, but we believe addressing other connected barriers will have a positive impact on this element of this barrier.

Connected Barriers

Cost
Non-transparent fee structures

Information Availability & Capability
Basic literacy and numeracy
Digital literacy
Unclear or unavailable info about products/ uses
Financial literacy

Product & Service Quality
Reliability and quality of in-person services

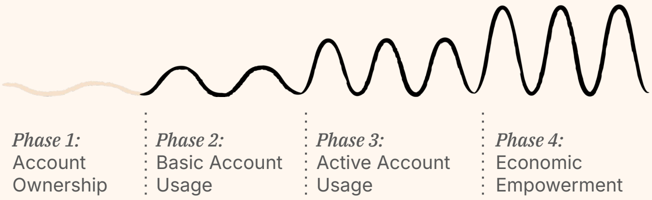
Consumer Protection
Over-charging
Fear or making mistakes
Potential (or actual) privacy violations
Predatory lending

Human Resources
Lack of female agents

Most Relevant Segments

1	2	3	4
Excluded, marginalized	Excluded, high potential	Included, underserved	Included, Not underserved

Customer Journey Relevance



Key evidence relevant to this barrier

- DFS might cause data-protection related risks where “traditionally excluded customers may be more vulnerable to the compromise of data privacy, identity theft, and fraud because they lack alternatives”. These risks are likely to cause more harm to consumers who have “low levels of financial capability” (World Bank, 2020).

- “Advances in technology have resulted in the increased digitalisation of daily life, with most consumers leaving important digital footprints behind and often being unaware of the use and misuse made by big data collection platforms of their personal/financial information, including the risk of digital profiling. Customers’ lack of knowledge of financial products and digital technologies can also make them vulnerable to abuse and other digital risks such as online fraud, phishing, social engineering scams, account hacking attacks, data theft, etc.” (OECD, 2017).

- “The global boom in e-commerce sales has also been accompanied by a multiplication of fraud activities affecting merchants, including those MSMEs that recently moved their operations online. Consequently, the relentless rise in fraud and scam cases worldwide might severely undermine MSME trust in—and subsequent reliance on—digital financial products and services.” (GFPI, 2021).

- In Kenya, respondents cited "fraud/attempted fraud" by mobile money providers (26.6% of respondents), mobile banking (9.9% of respondents), and mobile apps (4.7% of respondents) as challenges (FSD Kenya, 2021).

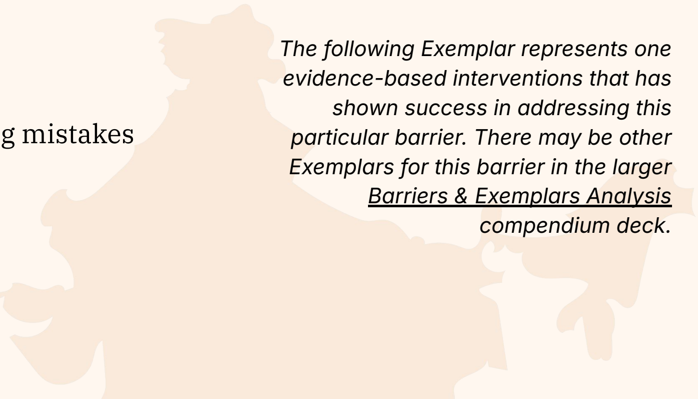
- The *Nigeria Consumer Protection in Digital Finance Survey* (2021) found that 26% of digital finance customers cited "phishing by phone or SMS" as a common challenge. This was the third most cited challenge, out of nine, among customers (MSC, 2022).

- “Fraud reduction benefited women farmers especially: Instances of repayment fraud fell 85 percent after digitization of repayments, and anecdotal reports indicate farmers (particularly female farmers) and staff feel safer because the risks of holding cash are reduced.” (BTCA, 2017).

- An IFC study covering 2,000 mobile financial services users and 2,000 non-users across Bangladesh found that “when compared to male agents, female agents were better behaved, easier to approach, more trustworthy, better at maintaining confidentiality, and could keep data secure.” (IFC, 2018).

- “Mobile agents are often very ‘male’ spaces in India. They can be intimidating for women to visit, and there is a risk of female customers’ mobile numbers being recorded and misused either by the retailer or a bystander.” (GSMA, 2018).

Consumer Protection | Fraud, scams and/or fear of making mistakes



The following Exemplar represents one evidence-based interventions that has shown success in addressing this particular barrier. There may be other Exemplars for this barrier in the larger Barriers & Exemplars Analysis compendium deck.

Exemplar

Aadhaar Project

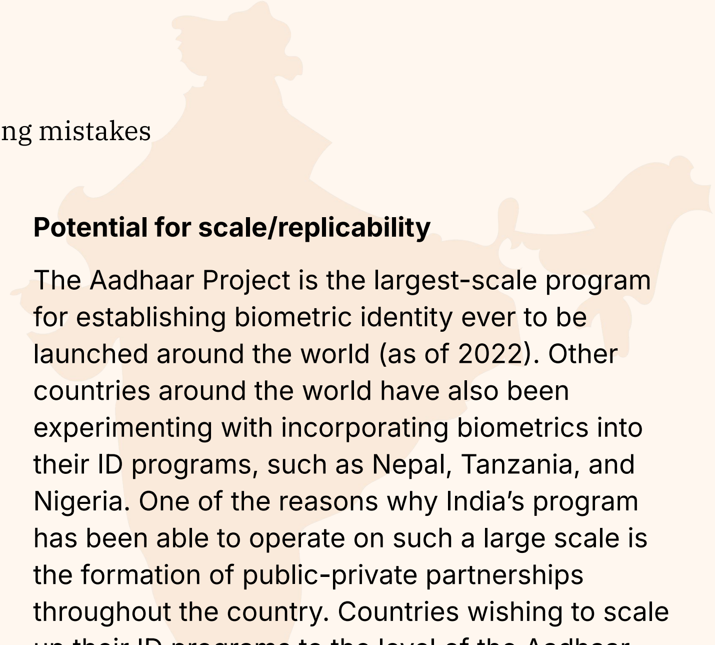
“India has a population of 1.2 billion people and approximately 400 million people are unable to prove their identity (in 2011)... The inability to prove one’s identity precludes the poor, the marginalized, and the underprivileged populations of India from gaining access to benefits and subsidies, applying for welfare benefits, accessing education, opening a bank account, or attaining employment. The goal of Indian government officials in implementing a broad identification system is to successfully address the concerns of national security, corruption, and anti-poverty efforts. There have been many documented cases of fake identities, fraud, and duplication of welfare services across the country... In order to improve the economic situation of all of its residents, the Unique Identification Authority of India (UIDAI) implemented an ambitious and innovative program known as Aadhaar. Aadhaar, which translates to ‘“support and foundation” in most Indian languages, would allow residents to prove their identity through a unique identity number provided by the officially recognized agency. The issuing of an Aadhaar number would be provided to all residents of India, whether or not they are permanent citizens.” (Chin et el., 2015).

Key activities

Enrollment is free and occurs through duly designated third-party enrollment agencies. To become an official enrollment agency, an organization is required to go through proper training and testing on procedures and use of the enrollment kit. Each kit is packed into a briefcase and includes the following: a laptop, the enrollment software, fingerprint reader, iris scanner, webcam, laser printer, and monitor. Participation in Aadhaar is voluntary for all residents. Crucially, it enables eKYC – a function which greatly enhances the efficiency of the KYC process and fosters financial inclusion. To enroll, residents can go to any authorized enrollment agency, complete an Aadhaar application form, and present current identification documents. If an enrollee does not have identification documents, they can still enroll with the help of an “introducer” – a person whose identity has already been verified. The “introducer” vouches for the enrollee, sidestepping the requirements for identification documents. The enrollee will then have their biometric data recorded and is entered into the database. The assigned Aadhaar number for an individual is connected to all biometric data collected during the enrollment process. A trained enrollment center employee photographs the enrollee, records the iris scans of the eyes, collects demographic information, and takes imprints of all 10 fingers. Each enrollee’s data is then uploaded to the Central Identification Data Repository (CIDR) for deduplication. The term “deduplication” refers to the process where the CIDR checks to determine whether or not the biometric data submitted already exists in the database. If no equivalent record exists, then a unique, randomly generated 12-digit number will be mailed to the enrollee.

Outcomes/results

- According to the UIDAI’s Aadhaar Dashboard, 1,331,920,291 Aadhaar numbers have been generated as of April of 2022. Additionally, 622,578,411 Aadhaar have been updated, and 70,711,414,709 authentication transactions have been completed.
- There 1,307,544 certified supervisors and operators, 888 active enrollment agencies, and 237 Authentication User Agencies.



Key enabling environment factors for the intervention

“Aadhaar’s ecosystem and public-private partnership structure is considered to be its greatest strength. Aadhaar’s implementation momentum does not reside entirely within the bounds of government or even within a narrow set of government and private organizations. Rather, the project has a broad array of organizations with a vested interest in its ongoing evolution and success.” (Chin et al., 2015).

Key design elements and principles that led to successful outcomes

- Enrollment is free, ensuring that users at the bottom of the pyramid can enroll in the program.
- The program is designed to be inclusive. Transgender individuals can register for this program, as well as noncitizens of India. Additionally, “multiple biometric data are recorded in order to enable the inclusion of all residents in India. Fingerprints, for example, can be worn away by physical labor. Since many of the poor residents of India have occupations that require heavy physical labor, a fingerprints-only identification scheme would continue to disenfranchise many of them.” (Chin et al., 2015).
- The program is designed to enable individuals who don’t meet the KYC requirements to enroll as long as they have the help of an “introducer” – someone whose identity has already been verified.
- The program has incorporated “anti-duplication” systems to ensure that each person is associated with one number, which minimizes the risk of fraud, scams, or identity theft.

Potential for scale/replicability

The Aadhaar Project is the largest-scale program for establishing biometric identity ever to be launched around the world (as of 2022). Other countries around the world have also been experimenting with incorporating biometrics into their ID programs, such as Nepal, Tanzania, and Nigeria. One of the reasons why India’s program has been able to operate on such a large scale is the formation of public-private partnerships throughout the country. Countries wishing to scale up their ID programs to the level of the Aadhaar project should seek to leverage partnerships with different stakeholders to improve operational efficiency and outreach.

Challenges encountered during the program

The Aadhaar Project has suffered from political divisions in the past. For example, in the 2014 national elections, some candidates questioned the safety of the Aadhaar technology and how the program’s funding was used. This raised tensions among citizens who started to distrust the program. The Supreme Court of India has also challenged the constitutionality of Aadhaar.

Recommendations from the research

Based on the concerns over security and privacy of Aadhaar, future programming should incorporate consumer protection trainings or presentations to resolve doubts that individuals may have concerning their identity and data protection. Additionally, the major strength of Aadhaar is its ability to make public-private partnerships. The program should continue leveraging these partnerships in the future to ensure that those at the bottom of the pyramid can become included via formal identification.

Additional Exemplars

BETA Savings Account in Nigeria

GRID Impact and SIA's analysis revealed that this barrier along with 11 others require further research and examination as to how they affect the customer experience, other barriers and overall WEE-FI. More in-depth analysis can be found in the larger Barriers & Exemplars Analysis compendium deck.