Navigating the Digitalisation of Finance

User experiences of risks and harms

April 2025

Centre for Internet & Society

Contributors (in alphabetical order)

Research design and/or report writing
Amrita Sengupta
Chiara Furtado
Garima Agrawal
Nishkala Sekhar
Puthiya Purayil Sneha
Vipul Kharbanda

Research advice and/or review
Antara Rai Chowdhury
Janaki Srinivasan
Nayantara Sarma
Palak Gadhiya
Pallavi Bedi
Sameet Panda
Semanti Chakladar
Shashidhar K J
Shweta Mohandas
Taranga Sriraman

Research and/or data analysis support
Chetna V M
Pallavi Krishnappa
Yesha Tshering Paul

Data analysis
Chiara Furtado
Garima Agrawal
Nishkala Sekhar

Research tool translation
Aravind R (Kannada)
Balaji J (Tamil)
Bhaskar Bhuyan (Assamese)
Nettime Sujata (Bangla)
Suresh Khole (Marathi)

Research tool pilots
Raveenaben (Megha Cooperative, SEWA)
Sunaben (Megha Cooperative, SEWA)
Raja Mouli N

Data collection (survey)
D-Cor Consulting

Data collection (focus group discussions)
Association of People with Disability, Bengaluru
D-Cor Consulting
Jnana Prabodhini, Pune
Transgender Rights Association, Chennai
Subodh Kulkarni

Suggested citation

Amrita Sengupta, Chiara Furtado, Garima Agrawal, Nishkala Sekhar, Puthiya Purayil Sneha, and Vipul Kharbanda (equal authorship). 2025. 'Navigating the Digitalisation of Finance: User experiences of risks and harms.' Centre for Internet and Society.

Acknowledgements

We are deeply grateful to the survey respondents, focus group discussion participants, and key informant interviewees who participated in our study, for generously sharing their time, experiences, and insights with us.

The published material is part of work housed at the Centre for Internet and Society, India (CIS) between 2022 and 2025. This work was supported, in whole or in part, by Google.org from 29/11/2022 to 28/02/2025, and Mozilla Foundation from 01/12/2024 to 28/02/2025. From 01/03/2025 to 08/04/2025, this work was supported by domestic funds at CIS.

Analysis, discussion, and recommendations expressed in this publication do not necessarily reflect views of the donors.

Typeset in: Libre Baskerville, Nunito
Cover image: Geranimo on Unsplash
Report design: Chiara Furtado, Nishkala Sekhar

Centre for Internet & Society

⚠ Trigger warning

This report discusses various aspects of social and economic harms associated with digital financial services, and some content may be distressing and potentially triggering for readers.

Contents

List of figures

List of abbreviations

AEBA	Aadhaar Enabled Bank Account
AePS	Aadhaar enabled Payment System
APBS	Aadhaar Payment Bridge System
API	Application Programming Interface
APP	Authorised Push Payment
ATM	Automated teller machine
B2B	Business-to-business
BBPS	Bharat Bill Payment System
BC	Banking Correspondent
BHIM	Bharat Interface for Money
CBO	Community-based organisation
CFCFRMS	Citizen Financial Cyber Fraud Reporting and Management System
CIS	Centre for Internet and Society
CSO	Civil society organisation
CSP	Customer Service Point
DBT	Direct Benefit Transfer
DFS	Digital financial services
DIP	Digital Intelligence Platform
DPI	Digital Public Infrastructure
EMI	Equated monthly installment
ePOS	Electronic Point of Sale
FGD	Focus group discussion
FRM	Fraud Risk Monitoring and Management

GSM	Gender and sexual minorities
I4C	Indian Cyber Crime Coordination Centre
IAMAI	Internet and Mobile Association of India
IBA	Indian Banks Association
IBSA	Image-based sexual abuse
IMPS	Immediate Payment Service
ISL	Indian Sign Language
IVR	Interactive voice response
JAM	Jan-Dhan, Aadhaar, and Mobile
KII	Key informant interview
KYC	Know Your Customer
LGBTQIA+	Lesbian, gay, bisexual, transgender, queer or questioning, intersex, asexual, and other gender and sexual minorities
MDR	Merchant Discount Rate
MeitY	Ministry of Electronics and Information Technology
MGNREGA	Mahatma Gandhi National Rural Employment Guarantee Act
MNRL	Mobile Number Revocation List
NACH	National Automated Clearing House
NBFC	Non-banking financial company
NETC	National Electronic Toll Collection
NFHS	National Family and Health Survey
NFS	National Financial Switch
NLP	Natural Language Processing
NPCI	National Payments Corporation of India
NSAP	National Social Assistance Programme
P2M	Person-to-merchant
P2P	Person-to-person

PF	Provident Fund
PII	Personally identifiable information
PM KISAN	Pradhan Mantri Kisan Samman Nidhi
PMGKY	Pradhan Mantri Garib Kalyan Yojana
PMJDY	Pradhan Mantri Jan Dhan Yojana
PMUY	Pradhan Mantri Ujjwala Yojana
PPI	Prepaid Payment Instrument
PSP	Payment service provider
PSR	Payment Systems Regulator
QR code	Quick-response code
RBI	Reserve Bank of India
RTGS	Real Time Gross Settlement
SBI	State Bank of India
SEBI	Securities and Exchange Board of India
SHG	Self-help group
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TRAI	Telecom Regulatory Authority of India
UDID	Unique Disability ID
UIDAI	Unique Identification Authority of India
UPI	Unified Payments Interface
VPA	Virtual Payment Address

Executive summary

The last couple of decades have seen significant changes in the financial ecosystem in India, both within the fintech sector and with respect to digital financial inclusion. The rapid growth in the reach of banking services to previously unbanked citizens through the Pradhan Mantri Jan Dhan Yojana has been followed by digitalisation in financial and public services.

However, a commensurate increase in digital and financial literacy has not followed, and rates of access to digital devices and the internet are still growing for many user groups, like rural women and regional language speakers. From the proliferation of fraudulent schemes and cybercrime to regulatory loopholes and inadequate consumer protections, the landscape of online financial services in India presents numerous risks. Factors such as weak cybersecurity measures, data breaches, lack of awareness among users, and the absence of comprehensive regulations create a fertile ground for financial scams. Simultaneously, rapid digitalisation of financial services, especially post demonetisation and the COVID-19 pandemic, has also brought to the fore concerns around omissions and exclusion of sections of users from databases, and a steep learning curve in adapting to this new digital ecosystem.

These combined factors open up users to a range of potential financial risks and harms, with differential impact on specific marginalised and vulnerable groups. With this understanding, we use the term digital financial harms to refer to adverse financial outcomes and other related detrimental consequences in the use of digital financial services.

Through this study, we aim to situate these experiences in a continuum of harms within a rapidly digitalising financial ecosystem. By exploring questions of access, accessibility and language we hope to bring aspects of cybersecurity, digital and financial literacy and design justice into conversation with each other. While some research has aimed to understand technology-facilitated gender based violence, financial fraud, misinformation, and other forms of digital risks in siloes, the correlations between these risks online remain severely understudied. In this report, we focus on the experiences of groups long marginalised within the financial system, to recommend that their needs are centred in shaping digital financial services.

Key questions guiding our research were:

- How were digital financial risks understood and experienced by users of digital financial services across groups? What factors have amplified risks for marginalised and at-risk user groups?
- What potential vulnerabilities, risks and harms have emerged relating to digital financial services around device and internet access, accessibility, challenges with use, exclusions from digitalised social protection, and forms of social engineering and digital financial fraud?
- How accessible were digital financial service providers' and governments' reporting and grievance redressal systems?
- What role should fintech platforms, social media platforms, banking and financial institutions, government, and regulatory bodies play in reducing digital financial risks across the ecosystem?

This was a mixed methods study, consisting of a review of available literature in the field, followed by quantitative and qualitative data collection through surveys and in-depth interviews. The report highlights the experiences of persons with disabilities, gender minorities, the elderly, low income users, and regional language first users; to better understand how discrimination, exclusion or slow redressal processes may increase their risk or cause disproportionate harm when using digital financial services. It discusses users' experiences of fraud in the context of an evolving regulatory ecosystem, as well as practical challenges users face with redressal systems.

Key findings include:

1. Access to digital financial services, still requires improving access and accessibility of physical and phygital banking services, and good internet connectivity.
2. Even among mobile phone owners, many users still rely on shared devices, particularly among women and persons with disabilities.
3. There is a high need for support in utilising net banking services, with 60% of surveyed netbanking users mentioning that they sought help to conduct online banking transactions. Migrating to digital financial services is not a purely digital journey for users who are still building comfort with digital interfaces, or those whose languages are deprioritised in the development of digital financial platforms.
4. Age, gender, and income were significant factors in the access to the internet, and adoption of digital financial services. For instance, women and transgender persons over 45 years were less likely to have a Unified Payments Interface (UPI) account. Women, transgender persons, and disabled users of UPI were also more likely to be infrequent users compared to the rest of the sample.
5. Over reliance on digital platforms for the administration of direct benefit transfer programmes results in challenges and risks of exclusions for beneficiaries.

6. While awareness of common forms of fraud is high, awareness of security protocols, Know Your Customer (KYC) requirements and markers of trustworthy banking and non-banking institutions is low.
7. Irrespective of the amount of money lost during frauds, it caused significant financial and emotional burden, especially for low-income persons.
8. In the absence of monitoring frameworks, bad actors within the financial system are able to exploit vulnerabilities like the dependence of account holders on banking correspondents.
9. Gender and sexual minorities, and women face disproportionate impacts of harm in the event of financial loss, including the consequences of image-based sexual abuse, victim blaming, domestic violence and limits on financial independence.
10. Ineffective grievance redressal for cybercrimes is a major deterrent to reporting.
11. Digitalisation and the use of assistive technology have allowed some persons with visual impairments to gain relative levels of independence in managing their own finances and conducting transactions. However, implementation of accessibility policies and features remains uneven, and is marred by the continued exclusion and discrimination within traditional banking services.

Based on these findings, this report offers a set of recommendations addressed to stakeholders within the financial ecosystem such as banking and other financial institutions, regulatory bodies, fintech companies, cybersecurity professionals, as well as social media platforms and civil society organisations working on digital inclusion, safety and literacy. The recommendations offer nuanced perspectives on how digital financial harms can be prevented and mitigated based on our interactions with various stakeholders during the research process.

Key recommendations emerging from the study are:

1. Create meaningful connectivity and access to digital platforms by improving public infrastructure and addressing the challenges associated with shared devices and mediated use.
2. Improve platform design to engender trust; increase accessibility and usability through assessment and better implementation of available technologies, regular design audits and facilitate availability in Indian languages.
3. Building awareness and capacity across user and stakeholder groups through customised and inclusive programming, working in partnership with communities.
4. Centre consumer protection in regulatory interventions and approaches to law enforcement, by implementing robust time-sensitive reporting and redressal mechanisms, placing accountability on financial institutions, and monitoring and curbing fraudulent activity.
5. Encourage transparent governance and public oversight by measuring and evaluating digital public infrastructures to maximise their public value.

How to read this report

This section of the report offers a brief overview of its structure, and the areas of research covered within each chapter. The report begins with a **brief introduction** sharing the research questions and objectives that guided the study.

Chapter 2 (Methods) that follows provides an in-depth introduction to the study design, data collection and analysis methods.

Chapter 3 (Background) provides a brief refresher on the developments in the digital financial ecosystem in India, with a focus on UPI systems, direct benefit transfers, and the growth of frauds and scams in India, followed by a discussion on the current regulatory approaches in India.

Report findings are presented in the following three chapters (Chapters 4-6). Beginning with **Chapter 4 (Access to digital devices and financial services)**, the report presents data to look at how questions of access to digital devices and internet, accessibility of services and exclusion impact the usage of physical, phygital and digital banking services. It summarises the drivers and challenges in the adoption of the Aadhaar enabled Payments System (AePS), netbanking, and UPI, with a specific focus on certain user groups.

Chapter 5 (Beneficiary experiences with digitalisation and social protection) discusses the question of how the introduction of digitisation within the benefits delivery system is experienced by beneficiaries of social security programmes, and what measures people utilise to adapt to these changes and challenges they experience within the system.

Chapter 6 (Digital financial frauds: Risk and vulnerabilities) examines the level of fraud awareness, quantum of financial loss, and harms that victims of digital fraud experienced, with specific gendered experiences. It also provides a breakdown of the modus operandi, and issues with grievance redressal mechanisms.

Chapter 7 (Discussion and recommendations) distils these findings into actionable suggestions for various actors including, banking and financial institutions, regulatory bodies, policymakers, fintech and social media platforms, civil society organisations, and

cybersecurity and product design professionals working across the landscape of digital financial services.

This is finally followed by **Chapter 8 (Conclusion)**, which summarises the study's key takeaways for stakeholders in the financial ecosystem.

Note on figures and quotes:

- The data for charts and tables are drawn from our study and have as source: **CIS digital financial harms survey, April – September 2024, N = 3,784, unless specified otherwise**.
- In the findings chapters (4-6), quotes in **navy blue (hex #1f3750)** indicate insights from **key informant interviews (KIIs)** and quotes in **dark magenta (hex #76425a)** indicate insights from participants from **focus group discussions (FGDs).**

The figures presented in chapters four, five, and six have the following notes to keep in mind:

- The charts used throughout this report include simple horizontal bar charts, vertical bar charts, 100% horizontal stacked charts, and grouped bar charts.
- The main socio-demographic variables against which the themes were analysed include states and UTs, age and gender, and monthly personal income.
- The primary colours for stacked charts are blue-green [hex #63A895], navy blue [hex #1F3750], magenta [hex #905171]. All horizontal bar charts are blue-green [hex #63A895] and all vertical bar charts are magenta [hex #905171].
- The questionnaire primarily consisted of single-select and multi-select questions. The data, presented as percentages, for single-select questions, adds up to 100%, excluding rounding off errors,. Whereas, with data reflecting multi-select questions the total percentage exceeds 100%.

1. Introduction

Over the past decade in India, narratives of financial inclusion and digital inclusion have increasingly converged. Digital and digitally-enabled technologies have been seen as gateways for access to financial services, particularly for those users who were previously outside formal financial and banking infrastructures. To this end, the past decade has witnessed concerted efforts towards leveraging digital technologies to achieve financial inclusion goals.

These digital financial inclusion efforts have borne fruit in terms of scale. A coalition of state actors, industry stakeholders, and funders have enabled the consolidation of digital public infrastructures for financial services, based on a foundation of digital identity, payments, and data exchanges.[1] Digital payments through the Unified Payments Interface (UPI) have seen an exponential rise since UPI's introduction in 2016, in terms of both transaction value and volume. In early 2025, nearly INR 23.48 lakh crores was processed through UPI across 1,699 crore transactions.[2, 3] Digitalised welfare delivery through the infrastructure of Direct Benefit Transfers (DBT) was being facilitated for over 1,000 social protection schemes at the national and state levels, by the end of 2023.[4] Alongside these digital public infrastructure (DPI) initiatives, an enabling regulatory environment and developments in digital technologies have been credited as driving the

[1] Mila Samdub. '"Digital Public Infrastructure" at a Turning Point from Definitions to Motivations', 26 February 2025. https://cyberbrics.info/digital-public-infrastructure-at-a-turning-point-from-definitions-to-motivations/.

[2] Seena Mary Mathew, Dr Shanimon.S, Sarvy Joseph, and Dr Minija Abraham. 'Exploring the Exponential Growth of UPI in India: A Study on Digital Payment Transformation (2016–2024)'. *Library Progress International* 44, no. 3 (11 October 2024): 10796–805. https://doi.org/10.48165/bapas.2024.44.2.1.

[3] Press Information Bureau. 'Unified Payments Interface (UPI) Provides an Opportunity to Other Countries to Learn from the Indian Experience - Professor Carlos Montes, Cambridge Business School', 27 February 2025. https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=2106794.

[4] Press Information Bureau. 'Ministry of Finance Year Ender 2023: Department of Expenditure', December 27, 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1990746

rise of the financial technology sector, which had a market share of over USD 110 billion (~ INR 9,40,844.85 crores) as of 2024, with over 9,000 financial technology entities.[5]

While several benefits have been realised through these developments, the increasing presence and adoption of digital financial services has not escaped its share of contradictions and challenges, especially for those at intersecting axes of marginalisation.

Recent years have seen a proliferation of increasingly complex financial frauds mediated and enabled through digital means. According to data from the nation-wide cyber fraud reporting system, 12 lakh cyber fraud complaints were received in 2024, which was over a third of frauds recorded since 2021.[6] Online financial frauds accounted for 60% of cybercrime reported on the National Cybercrime Reporting Portal in 2023.[7]

In addition, when it comes to social protections and the deployment of digitised interventions to that end, various on-ground reports and field research have raised concerns regarding exclusion errors (exclusion of eligible beneficiaries at stages of enrolment in schemes, payments and settlements of benefits, and withdrawals), among other issues.[8, 9]

Further, digital and financial divides around access and literacy continue to be a reality especially for marginalised user groups, creating barriers to adoption, as well as risks of exclusion.[10, 11, 12]

---

[5] ASSOCHAM. 'Press Release: Indian FinTech Industry Projected to Reach $420 Billion by 2029 - Ajay Kumar Choudhary, Non-Executive Chairman and Independent Director, NPCI'. Accessed 5 April 2025. https://www.assocham.org/press-release-page.php?release-name=indian-fintech-industry-projected-to-reach-420-billion-by-2029-ajay-kumar-choudhary-non-executive-chairman-and-independent-director-npci.

[6] "Digital Payment and Online Security Measures for Data Protection", Standing Committee on Information Technology, Seventeenth Lok Sabha, Forty Fourth Report, February 8, 2024, https://sansad.in/getFile/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_54.pdf?source=loksabhadocs

[7] "Digital Payment and Online Security Measures for Data Protection", Standing Committee on Information Technology, Seventeenth Lok Sabha, Forty Fourth Report, February 8, 2024, https://sansad.in/getFile/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_54.pdf?source=loksabhadocs

[8] LibTech India. 'Length of the Last Mile: Delays and Hurdles in NREGA Wage Payments'. LibTech India, November 2020. https://libtech.in/wp-content/uploads/2020/11/LastMile_ReportLayout_vfinal.pdf.

[9] Sameet Panda. 'Data Systems in Welfare: Impact of the JAM Trinity on Pension & PDS in Odisha during COVID-19'. Centre for Internet and Society, 21 February 2021. https://cis-india.org/raw/sameet-panda-jam-trinity-pension-pds-odisha-covid-19.

[10] Indian Express. '"Some 120 cr mobile phones in use in country, main priority to increase 4G network's scope:" Scindia', Indian Express, July 11, 2024, available at https://indianexpress.com/article/india/mobile-phones-country-main-priority-increase-networks-scope-scindia-9447732/

[11] Abhishek Waghmare. 'Access to Phones and the Internet'. Data For India, 29 February 2024. https://www.dataforindia.com/comm-tech/.

[12] R. Umesh and Y. Nagaraju, "Direct Benefit Transfer in India: Progress, Challenges, and the Path Forward", International Journal for Multidisciplinary Research, Volume 7, Issue 1, January-February 2025, available at https://ijfmr.com/papers/2025/1/34574.pdf

It is in this context that we situate our research. Our study is an attempt to centre the experiences of marginalised users navigating the digitalisation[13] of finance. We foreground how vulnerabilities specifically around age, income, gender, sexuality, disability, and language shape risks and harms from digital financial services. Our study builds on emerging research that has explored vulnerabilities and harms for certain marginalised users such as women and elderly persons through their experiences with particular digital financial services.[14, 15] However, a gap remains in terms of understanding user experiences across vulnerable groups and across a range of interrelated digital financial infrastructures. Further, very little disaggregated and intersectional quantitative and qualitative data is available on experiences of marginalised groups. Our study aims to address some of these evidence gaps through a methodological approach guided by feminist and sociotechnical analyses of digitalised systems.[16, 17, 18]

Our approach unpacks power relations that shape users' everyday experiences with digital financial services in India. These power relations play out at multiple levels where they determine user experiences within households, within communities, with financial and digital infrastructures, and with powerful actors like governments and digital financial service providers. For instance, within households, patriarchal norms decide whether some users gain access to financial accounts and digital devices, while some do not. Within communities, networks of trust (and distrust) are crucial in determining access, particularly for users who are more likely to rely on support for registration and use of digital financial services.

---

[13] We use the term 'digitalisation' here to refer to the sociotechnical aspects of the digital turn and its impact, but in this report and more generally, the term is often used interchangeably with digitisation which refers to technical facets of this shift. As Legner et. al (2017) elaborate, "digitization is the conversion of analog into digital signals, adopting a more technical perspective that is characterized by a dematerialization of information or, in other words: the redundancy of physical assets in terms of information storage, transmission, and processing. In contrast, digitalization describes socio-technical conditions of the adoption and use of digital technologies – also with a focus on their societal, organizational, and individual impact." As paraphrased in Adeline Frenzel et. al, "Digitization or digitalization? –Toward an understanding of definitions, use and application in IS research" (2021).AMCIS 2021. Proceedings. 18 https://aisel.aisnet.org/amcis2021/adv_info_systems_general_track/adv_info_systems_general_track/18

[14] MicroSave Consulting. 'DBT Diagnostic Study: Female Beneficiaries' Experience of Receiving DBT'. MicroSave Consulting, September 2022. https://www.microsave.net/wp-content/uploads/2022/11/221110_DBT-diagnostic-study-Female-beneficiaries-experience-of-receiving-DBT.pdf.

[15] SII Secretariat. 'Understanding Senior Citizens' Experience with Online Fraud'. Safer Internet India, 25 February 2025. https://www.saferinternetindia.com/post/understanding-senior-citizens-experience-with-online-fraud.

[16] Suprateek Sarker, Sutirtha Chatterjee, and Xiao Xiao. 'How "Sociotechnical" Is Our IS Research?: An Assessment and Possible Ways Forward'. In Proceedings of the 34th International Conference on Information Systems. ICIS 2013, 1185. Association for Information Systems. AIS Electronic Library (AISeL), 2013. https://aisel.aisnet.org/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1185&context=icis2013.

[17]Yingqin Zheng and Geoff Walsham. 'Inequality of What? An Intersectional Approach to Digital Inequality under Covid-19'. Information and Organization 31, no. 1 (1 March 2021): 100341. https://doi.org/10.1016/j.infoandorg.2021.100341.

[18] L. Robinson, J. Schulz, G. Blank, M. Ragnedda, H. Ono, B. Hogan, G. S. Mesch, et al. 'Digital Inequalities 2.0: Legacy Inequalities in the Information Age'. First Monday 25, no. 7 (2020). https://doi.org/10.5210/fm.v25i7.10842.

Developments in digital financial services in recent years also mean that users interact with a range of public and private infrastructures and actors. These relate to banking, internet, and digital public infrastructures; financial and digital platforms; and government bureaucracies. As digital financial services become progressively important in users' everyday financial lives, some questions become critical: those around understanding the design and governance of digital financial services, the relative power that digital financial infrastructures and actors hold over users, and the risks for users that may compound across these varied infrastructures and actors.

Guided by this feminist and sociotechnical approach, we undertook a mixed methods study spanning nine states and union territories in India. For our study, we surveyed 3,784 users, with differing levels of access to digital devices, digital services and the internet; and undertook 18 semi-structured interviews and seven focus group discussions with specific user groups and stakeholders. Through our study's findings, we highlight experiences of persons with disabilities, transgender persons, gender and sexual minorities, elderly persons, women, regional language-first users, and persons facing digital and economic vulnerabilities.

Digital financial harms, in our framework, include being negatively impacted by financial misinformation, the loss of an asset, loss of control over assets, loss of potential income, financial abuse, overindebtedness, financial mis/disinformation, difficulty accessing social protection and exclusion from financial services and welfare delivery. While greater attention has been paid to digital financial fraud in other research, through this study, we aim to situate experiences of fraud alongside experiences of harms that are understudied and sometimes overlooked.

Through this mixed methods research study, we aimed to:

- Assess the financial risks and harms users are exposed to when using a wide range of digital financial services, including social media, digital banking, digital payments (UPI), fintech platforms, and digitalised social protection (DBT). Apart from looking at general users, we specifically centred the experiences of elderly persons, persons with disabilities, persons identifying as gender and sexual minorities, women, regional language-first users, and persons facing digital and economic vulnerabilities.
- Understand the experiences of users across three key areas: access to digital and digital financial services and associated challenges, experience of accessing direct benefit transfers and experience of digital financial frauds.
- Produce an evidence base of qualitative and quantitative insights for key stakeholders with regard to experiences of digital financial risks and harm.
- Provide recommendations for improved policy and platform design to address interconnected risks and harms.

2. Methods

2.1. Study design and scope

Digital financial harms comprise an expansive area of study, with developments across various related sectors, including but not limited to payments, personal finance and investments, insurance, banking, credit, pension and insolvency among others. Based on the learnings from a scoping literature review, and public awareness about the various kinds of digital harms, we decided to limit the scope of the study to digital financial harms in specific areas, and their impact on certain user groups. This study is therefore exploratory in nature, and the topic would require further research in order to generalise results to a larger population. Given some of these limitations, the study also adopted a mixed methods approach (which combines the use of qualitative and quantitative data) in order to arrive at a better understanding of the current financial landscape, and the prevalence of these harms.

The second phase of this research adopted a concurrent nested design, wherein both quantitative and qualitative data collection was undertaken simultaneously. This included:

- a quantitative survey of 3,784 participants
- key informant interviews (KIIs) with 18 participants, and
- seven focus group discussions (FGDs) covering 63 people across specific user groups - the elderly, women, gender and sexual minorities, and persons with disabilities.

The setting for this study was India, and the study population comprised the constituencies mentioned above.

2.2. Literature review: Secondary/desk-based research sources

The study commenced with a desk-based scoping review of literature to map the prevalence and nature of financial harms mediated through digital platforms in India. Given the limited amount of research publicly available on the topic in India, this involved parsing through several secondary research sources, including but not limited to academic literature, media reportage, official documentation and statistics shared by regulatory bodies, and research undertaken by civil society and fintech organisations on types of digital financial harms.

Our understanding of 'digital financial harms,' while informed by conceptual and theoretical frameworks drawing from cybersecurity risks and harm, also moves away from the "threat-centric approach"[19] common in mainstream discourse, to focus on financial harms itself as a socio-economic experience. This approach emphasises the prevalence of such harms and its impact on stakeholders, especially among specific user groups. This also includes unpacking and navigating the continuum of offline and online harms,[20] where access, digital and financial literacy play a crucial role. Lastly, there is also a need to map the risks of harm against affordances of the internet and digital media technologies, and socio-technological environments of users which may create conditions of vulnerability to harms.[21]

Our learnings from the literature review further informed the development of the research questions, study sample and recruitment. We also conducted six scoping interviews with subject experts working in the areas of digital financial inclusion, access, safety and accessibility of digital financial platforms, social welfare and digitisation. Based on these learnings, the study sample was determined, with a focus on specific user groups—persons with disabilities, elderly, women, gender and sexual minorities and regional language speakers in addition to the general population.

2.3. Sampling, recruitment and data collection

2.3.1. Survey

Research tools overview: The insights from the literature review and scoping interviews with subject area experts were utilised to develop the instruments for the survey. The survey guide was divided into three distinct sections:

[19] Agrafiotis, Ioannis and Bada, Maria and Cornish, Paul and Creese, Sadie and Goldsmith, Michael and Ignatuschtschenko, Eva and Roberts, Taylor and Upton, David M., Cyber Harm: Concepts, Taxonomy and Measurement. Saïd Business School WP 2016-23, Available at SSRN: http://dx.doi.org/10.2139/ssrn.2828646

[20] Munk, T., & Kennedy, M. Eds.*Victimisation in the Digital Age: An Online/Offline Continuum Approach* (1st ed.). London: Routledge, 2024. https://doi.org/10.4324/9781032714202

[21] Livingstone, Sonia."Online risk, harm and vulnerability: reflections on the evidence base for child Internet safety policy.". ZER: Journal of Communication Studies, 18 (35).2013. pp. 13-28. ISSN 1137-1102

- Socio-demographic information including device access.
- Mapping the level of access based on their use of digital banking services, AEPS, UPI, and access to financial services.
- Assessing the experience of financial harms, specifically with reference to fraud, and exclusion from welfare and benefits.

The draft survey was reviewed by subject experts working in some of the areas mentioned above, and the finalised instrument was translated into six languages—Assamese, Bangla, Hindi, Kannada, Marathi and Tamil.

Sampling and recruitment strategy: The final sample size for the survey was 3,784 persons across nine Indian states, with participants from urban and rural geographies. The states were chosen based on research across various databases and reports such as the report by the National Commission on Population[22] for population projections for 2023-24; Internet and Mobile Association of India (IAMAI)[23] and the National Family and Health Survey (NFHS-5)[24] for internet access and use, and State Bank of India (SBI) analysis[25] on levels of UPI usage across the country. This was further disaggregated across urban and rural regions in states across six geographic zones, North, North East, South, East, West and Central. We employed quota sampling to arrive at specific quotas within each state/zone for each of the focus user groups mentioned above. The sample was further disaggregated along gender, income, and age which can be found in **Annexure A**. As this was quota-based sampling, the findings are therefore not representative or generalisable to the larger population.

Bank account ownership was a precondition of the study to ensure respondents could meaningfully discuss their adoption, and other experiences with digital financial services and as a result, almost all survey respondents had access to an individual bank account. This also meant that we were unable to engage with a significant portion of the population that continues to have no/limited access to banking services, and thereby has little experience of handling their finances via bank accounts and/or digital platforms. Given the scope of the current study, we acknowledge this limitation and hope to

[22] National Commission on Population, Ministry of Health & Family Welfare. 'Population Projections for India and States 2011-2036; Report of the Technical Group on Population Projections'. National Commission on Population, Ministry of Health & Family Welfare, July 2020. https://mohfw.gov.in/sites/default/files/Population%20Projection%20Report%202011-2036%20-%20upload_compressed_0.pdf.

[23] "Internet in India: 2022", IAMAI, April 2023, https://www.iamai.in/sites/default/files/research/Internet%20in%20India%202022_Print%20version.pdf.

[24] "National Family Health Survey - 4 & 5: State", *The National Data and Analytics Platforms*, accessed June 2023, https://ndap.niti.gov.in/dataset/6821.

[25] SBI Research. "Withdrawal of Rs 2000 Note: How it could result in a bank deposit boost, repayment of loans boost, consumption boost, RBI retail CBDC boost and a possible GDP boost", SBI Research, 19 June 2023, https://sbi.co.in/documents/13958/36530824/19062023-SBI+Analysis+on+Withdrawal+of+Rs+2000+Note.pdf/01c08bbe-0012-5f42-d60a-ced27f82e857?t=1687153549181.

address the same in subsequent research. The figures below (figures 2.1. to 2.5.) detail the distribution of survey respondents across different demographic vectors.

Figure 2.1. Distribution of survey respondents across states and union territories (UTs)

States and UTs	N	Percentage
Maharashtra	728	19
Uttar Pradesh	648	17
Rajasthan	436	12
Bihar	394	10
West Bengal	373	10
Tamil Nadu	372	10
Karnataka	294	8
Delhi	280	7
Assam	259	7
Total	**3,784**	**100**

Figure 2.2. Distribution of survey respondents across age groups

Age range	N	Percentage
18 to 30 years	1,619	43
31 to 45 years	1,371	36
46 to 59 years	348	9
> = 60 years	446	12
Total	**3,784**	**100**

Figure 2.3. Distribution of survey respondents by gender and sexual identity

Gender and sexual minorities	N	Percentage
Transgender persons	252	6
Sexual minorities	201	5

Women over 59	206	5
Women with disability	110	3

Note: These categories have overlap especially with women over 59

Figure 2.4. Distribution of survey respondents by disability

Persons with disabilities	N	Percentage
Yes	230	6
No	3,554	94
Total	**3,784**	**100**

Figure 2.5. Distribution of survey respondents by monthly personal income

Monthly personal income (INR)	N	Percentage
No income	1,073	28
1 to 5,000	322	9
5,001 to 10,000	598	16
10,001 to 18,000	955	25
18,001 to 30,000	648	17
> 30,000	188	5
Total	**3,784**	**100**

For further demographic breakdown of survey respondents, see **Annexure A**.

Data collection: The final recruitment of survey respondents, and data collection was undertaken by an external data collection agency over a period of six months from April - September 2024. After a series of initial training sessions and testing of the survey tools to address any technical, conceptual and programming difficulties, in-person data collection was conducted in two phases across the nine states by the survey collection agency.

The raw data was shared with the research team at the Centre for Internet and Society (CIS) at regular intervals, including updates on the number and frequency of data checks being conducted by the data collection team.

2.3.2. Key informant interviews

Research tools overview: Preparation for qualitative data collection began alongside the survey, and was anchored by the research team through six scoping interviews undertaken early in the research process. The guide for the in-depth questionnaire was developed by the team so as to complement the data to be collected through the survey, and keeping in mind a set of key constituencies/stakeholders to tap into for the research. The interview guide was also reviewed internally by researchers working in areas relevant to the main research topic, before being tested for any logical or programming difficulties.

Sampling and recruitment strategy: A total of 18 interviews were conducted with subject experts from key stakeholder groups (see figure 2.6.). These included fintech platforms, social media platforms, cybersecurity experts, researchers/academics, journalists, and civil society organisations working on digital inclusion and finance. Given considerable challenges in locating subject experts in the relevant fields, we relied on a purposive and referential sampling approach to identify and recruit participants for the study.

Figure 2.6. Distribution of interview participants across stakeholder groups

Stakeholder Groups	No. of Interviews
Cybersecurity experts	2
Researchers/academics working on digital and financial inclusion	2
Civil society organisations working with the elderly, women, LGBTQIA+ persons, persons with disabilities,	6
Civil society organisations working on digital financial inclusion and access	2
Journalists working on technology, digital media, and digital finance beats	3
Fintech platforms and social media platforms	3
Total	**18**

Data collection: The interviews were conducted by members of the CIS research team over a period of eight months. All interviews were conducted online, with data being collected in the form of notes and audio recording with the informed consent of participants. The interviews were conducted in English and a mix of regional languages where required.

2.3.3. Focus group discussions

Research tools overview: The FGDs were specific to the five user groups identified at the beginning of the research study—elderly, women, regional language users, gender and sexual minorities, and persons with disabilities. The questionnaires were developed accordingly, with a focus on specific thematic areas/questions/challenges most relevant to these groups. The FGD questionnaires were also reviewed internally and then shared with the data collection agency for collaborative implementation.

Sampling and recruitment strategy: A total of 7 FGDs were conducted with specific user groups (see figure 2.7.). The sample for the FGDs was drawn based on a cross-section of the zones/states in which the survey was being undertaken, and the focus groups for the study. The specific cities were selected based on convenience sampling, from the overall set of nine states, and the availability of civil society organisations (CSOs)/community-based organisations(CBOs) working closely with these user groups. Hence a set of seven FGDs were designed, and conducted in these selected cities by the survey team and researchers at CIS, alongside the quantitative data collection. All the FGDs were conducted in collaboration with CSOs/CBOs working with the relevant focus group in order to better facilitate conversations and address linguistic and context-specific challenges, if any.

Data collection: The FGDs were conducted by CIS and the data collection agency over a period of three months, in parallel with the survey. The data was recorded in the form of notes and recording where possible, with the informed consent of participants.

Figure 2.7. Distribution of FGD participants across location and language

Group	No. of participants	Location	Language/s
Elderly persons	10	Lucknow, Uttar Pradesh	Hindi
Women (<60 years)	11	Kota, Rajasthan	Hindi
Transgender persons	10	Patna, Bihar	Hindi
Women (rural- 25-45 years)	9	Velhe, Pune	Marathi
Women (rural >45 years)	8	Khed Shivapur, Pune	Marathi
Persons identifying as gender and sexual minorities	8	Chennai, Tamil Nadu	Tamil
Persons with disabilities	7	Bengaluru, Karnataka	Kannada, Tamil, Telugu
Total	**63**		

2.4. Data analysis

2.4.1. Quantitative data analysis

Data verification was carried out in tandem with the data collection, and continuous feedback was provided to the agency to improve data quality of subsequent phases. For details on the data verification and cleaning process, see **Annexure B**.

Following the data verification and cleaning process, data analysis methods included parsing tabulations of categorical variables and generating cross-tabulations of important variables with socio-demographic variables to understand distribution across geographic regions, age, income, specified user groups per our study, migrant status, caste category, and religious identity. The cross tabulations were organised by digital access and digital infrastructure, financial access and financial infrastructure, accessibility and usage, platform/provider design, service outcomes including challenges, and mediated use.

2.4.2. Qualitative data analysis

Focus group discussions: The qualitative analysis for the focus group discussions data began with an in-depth coding exercise to identity and organise key themes. A blended approach of deductive/ a priori coding and inductive/ emergent coding was adopted for analysing FGD data. We undertook a two-level scheme for coding—the first level involved general a priori themes drawing from the literature review; and the second level involved more specific emergent codes drawing from participants' narratives in the data, which were nested within a priori themes.[26]

On completion of the FGD coding, 192 codes emerged, with 16 first-level a priori themes including those around digital and financial access, digital and financial literacy, usage patterns of digital financial services, accessibility and usability of digital financial services, user experiences with informational and design practices of financial and relevant digital institutions, intermediaries and interpersonal dynamics relating to use of digital financial services, and so on. Further analysis was conducted through the preparation of analytical summaries and memos for each of these themes. An indicative list of a priori themes for the FGDs is as follows:

Figure 2.8. A priori themes from the focus group discussions

Digital and financial access
Digital and financial literacy
Digital financial access and digital financial literacy
Accessibility / usability

[26] Matthew B. Miles and A. Michael Huberman. *Qualitative data analysis: An expanded sourcebook* (2nd ed.).(Sage Publications, Inc., 1994)

Usage patterns
Platform/provider information, policies, practices, and/or design
Use/service risks and outcomes
Intermediary, third party, and/or interpersonal risks
Financial institution/platform/provider requirements
Policy requirements

Key informant interviews: The analysis for key informant interviews involved analysing perspectives from four main informant groups—researchers, journalists, community-based organisations, and representatives of fintech and social media platforms. An additional dimension of analysis was around the user/community groups that the key informants were primarily working with. These groups coincided with our specified user groups and included additional groups such as low income users, DBT and welfare beneficiaries, and victims of digital financial fraud.

A similar blended approach was adopted for analysis of the KIIs (as with the FGDs) with ten general a priori categories drawing from the literature review, and 74 further sub-themes identified and analysed for each of the four key informant groups. On completion of analysis of the KIIs, key themes included themes around digital and financial inclusion, digital literacy and capacity building, usage patterns of digital financial services, accessibility and usability of digital financial services, information asymmetry and transparency, and the regulatory ecosystem. Further analysis was conducted through the preparation of analytical summaries and memos for each of these themes. A list of key themes is as follows:

Figure 2.9. Main themes from the key informant interviews

Demographic vectors of vulnerability
Access barriers and exclusion (indirect risks and harms)
Usage preferences and patterns
Harms from information asymmetry and misinformation/ transparency
Mediated use/access to services
Digital divide, forced digitisation and digitalisation
Trust in digital financial services
Addressing harm through risk reduction

Addressing harm through impact reduction
Balancing consumer protection and innovation
Platform accountability and responsibility

2.5. Study ethics and participant safety practices

2.5.1. Informed consent

Protocols to ensure informed consent to participate in this study were followed for all modes of data collection. These were developed following conversations on asymmetries of power between researchers and participants, and with an understanding of self-reflexivity and positionality while undertaking primary data collection. This was also pertinent given the specific focus groups in this research, and the intersectional nature of social and economic harms being studied. Consent forms outlining objectives, methods and outputs of the study, risks and benefits of participation, data management and compensation were shared with all participants before proceeding with the data collection. Participants were free to withdraw from the study at any given point. Consent was recorded in writing as well as on audio, and only the latter where participants were unable to share written consent.

2.5.2. Compensation

All participants were compensated for their time, in the form of gifts/gift vouchers (surveys), and honoraria (KIIs and FGDs). Reviewers, facilitators, translators were also compensated for their time during instrument building and data collection.

2.5.3. Privacy and attribution

The consent forms shared with participants clearly outlined terms of privacy and attribution, where in the case of the surveys and FGDs, all data was anonymised, and for KIIs the research participants were able to choose whether to stay anonymous, or the manner of attribution for their inputs. For the surveys we also established specific protocols for separating PII from non-PII primary research data.

2.5.4. Data management, processing, storage and deletion

A data management plan was developed to establish protocols for storage, retention, use and deletion of primary data sets by the agency and CIS after a stipulated duration. Access to the non-PII primary research data was also restricted to only members of the research team at CIS.

2.6. Study limitations

2.6.1. Secondary sources

A significant challenge with this study was the lack of adequate secondary sources, including but not limited to official documentation of digital financial harms, journalistic and industry reportage, and academic research. While there are studies on specific platforms, such as UPI, or schemes such as the DBT, and large-scale studies on digital financial inclusion, there is limited research available in the Indian context on financial harms, and the impact of these on specific, marginalised user groups. As a result, the literature review for this study took longer than planned, and therefore the finalisation of the research questions and study instruments required a more considered and careful process.

2.6.2. Primary data collection

There were several limitations with the primary data collection phase, due to the challenging topic and the difficulties with a quota sampling approach. Given the limited capacity of the survey agency in identifying respondents across all the user groups with the help of the relevant CSOs/CBOs it took us some time in commencing fieldwork. With the KIIs and FGDs again, identifying respondents, and organisations working in these areas with the specific user groups proved to be a difficult task. Even with a snowball sampling approach, we were only able to identify a limited set of research participants for the KIIs. There were also certain external variables, such as the general elections in India in April–May 2024, and vagaries such as a heatwave and floods in some states which delayed primary data collection.

The following chapters in this report delve deeper into some of the findings from this research study, with a focus on access to digital financial services, digitisation of welfare services and the prevalence and experience of frauds and harms.

3. Background

Over the last decade, India has been actively promoting the use of digital technologies in various sectors such as healthcare,[27] education,[28] agriculture,[29] land records,[30], and so on, especially under the aegis of the Digital India programme. Digital India is a campaign through which the Government of India seeks to "transform India into a digitally empowered society and knowledge economy" through "digital delivery of services," and "expanding the digital economy".[31] Digital payments are one of the major pillars of this shift to digital technology and the motivations behind adopting digital means for financial transactions include increased financial inclusion, convenience, transparency, and economic growth.[32] Some of the key factors contributing to the growth of the digital financial ecosystem over the last few years include the growth in internet and mobile banking, digital wallets, development of the Aadhaar enabled Payment System (AePS), advent of the Unified Payments Interface (UPI) and the push towards Direct Benefit Transfer (DBT).

The drive for innovation in payments and settlements has not been limited just to UPI but also encompasses systems such as Immediate Payment Service (IMPS) for instant payments, UPI Lite X for offline payments, Real Time Gross Settlement (RTGS) for large

[27] "Ayushman Bharat Digital Mission", Digital India, accessed February 25, 2025, https://www.digitalindia.gov.in/initiative/ayushman-bharat-digital-mission/
[28] "Learning Management System (LMS)", Digital India, accessed February 25, 2025, https://www.digitalindia.gov.in/initiative/lms/
[29] "Sathi", Digital India, accessed February 25, 2025, https://www.digitalindia.gov.in/initiative/sathi/
[30] "eSampada", Digital India, accessed February 25, 2025, https://www.digitalindia.gov.in/initiative/esampada/
[31] "Digital India: Power to Empower", digitalindia, accessed February 25, 2025, https://www.digitalindia.gov.in/about-us/
[32] Sanjeev Chaddha and Sanket Jain, "Digital Transformation of Financial Sector in India- Evolution, Issues and Challenges", Samriddhi, Vol. 2, Iss. 1(2024),p. 100, available at https://mcrhrdi.gov.in/images/samriddhi/number2/10.Digital%20Transformation%20of%20Financial%20Sector%20in%20India.pdf

value payments, Bharat Bill Payment System (BBPS), clearing houses like the National Automated Clearing House (NACH), the Aadhaar Payment Bridge System (APBS) for welfare payments, the National Electronic Toll Collection (NETC), and many more.[33]

Consumers are using digital financial services for a wider range of applications than before. The Reserve Bank of India (RBI) estimates about 57 crore digital transactions are conducted daily, over two-thirds of which are facilitated via UPI. Since 2013, transaction volumes have increased 94 times, with transaction values increasing 3.5 times at INR 2758 lakh crore by 2024.[34] While a large number of transactions continue to remain cash dependent, there is a push to encourage and incentivise digitalisation. In addition to mandating zero merchant discount rate (MDR) on a vast majority of UPI transactions, the Indian government approved a 2,600 crore incentive scheme to promote the use of RuPay credit cards and peer to merchant BHIM-UPI payments in 2023.[35]

As shared in the introduction, our report focuses on three main issues: access to digital financial services, direct benefit transfers, and frauds. In the subsequent sections of this chapter we aim to provide some background to these issues. This is not meant to be exhaustive but aims to highlight some key moments and points of inflection in the digital financial journey of India.

3.1. Unified Payments Interface (UPI)

The journey of UPI started in the late 2000s when the Reserve Bank of India (RBI) first conceptualised the idea of a separate entity to manage payment systems in India. This led to the establishment of the National Payments Corporation of India (NPCI) in 2008, an umbrella organisation for operating retail payment and settlement systems in India. The formation of the NPCI was a joint initiative of the RBI and the Indian Banks Association (IBA) with the aim to modernise India's payment systems.[36] It was formed as a not-for-profit company under the Companies Act, 1956 by ten banks[37] each of whom contributed for a 10% stake in the company. The participating banks could not make any profit from NPCI and any revenues or profits had to be reinvested. Although the government of India does not have a direct stake in the NPCI, it controls a majority stake through the public sector banks (Government of India owns a majority stake in public sector banks). In fact, by law, the majority shareholding in NPCI is required to be held by

[33] "Payment System Report, December 2024", Reserve Bank of India, accessed February 25, 2025. https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=23127

[34] ibid.

[35] "Cabinet approves the incentive scheme for promotion of RuPay Debit Cards and low-value BHIM-UPI transactions (P2M)", Press Information Bureau, 11 January 2023, https://pib.gov.in/PressReleasePage.aspx?PRID=1890314

[36] "An Introduction to NPCI and its various products", NPCI, accessed February 25, 2025, https://www.npci.org.in/who-we-are/about-us

[37] State Bank of India, Bank of Baroda, Punjab National Bank, Canara Bank, Bank of India, and Union Bank of India; private banks ICICI Bank, HDFC Bank; and foreign banks Citibank and HSBC.

public sector banks.[38] In 2016, the shareholding was increased to 56 member banks and in 2020, new entities regulated by RBI were introduced, consisting of payment service operators, payment banks, small finance banks, and so on.[39]

In its initial years the NPCI launched a number of payment systems, some of which later contributed to the development of the UPI. In 2010, it launched the Aadhaar enabled Payment System (AePS), which allowed online interoperable transactions at ePoS[40] through the Business correspondent of any bank using Aadhaar authentication that uses their Aadhaar number, bank name and biometrics to conduct transactions. This system was aimed at providing basic banking services without regular brick and mortar banks. It provides a phygital mode of banking without the use of documents like passbooks, ATM cards, or cheque books. By 2013, the NPCI launched the Aadhaar Payment Bridge System (APBS) which "used Aadhaar number as a central key for electronically channelising government benefits and subsidies in the Aadhaar Enabled Bank Accounts (AEBA) of the intended beneficiaries," which offered the government an opportunity to reengineer the process for delivery of its welfare schemes.[41]

3.1.1. Launch and adoption of UPI

The concept of a more efficient payment system gained further traction in 2015 because the RBI sought to adopt new payment systems as was being done in other countries, and the NPCI was looking to make better products.[42] As a result, in April 2016, NPCI officially launched UPI, a payments system that brought multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, fund routing and merchant payments onto a single platform.

> The aspect of UPI that made it unique and appealing was that it was a multi application system, which means that users registered on any UPI platform could make transactions to any other account registered with UPI, irrespective of the app or bank of the counterparty. Thus users were not restricted to using a particular bank's mobile app or payment platform but could use the UPI app or any UPI-enabled app to make transactions to any other UPI-enabled app.

This made UPI a convenient single platform for transactions, eliminating the need for users to maintain multiple accounts or download multiple apps to make payments. Further, payments over UPI did not require people to share multiple pieces of

[38] Section 4(2), Payment and Settlement Systems Act, 2007.
[39] "An Introduction to NPCI and its various products", NPCI, accessed February 25, 2025, https://www.npci.org.in/who-we-are/about-us
[40] An Electronic Point of Sale, a digital checkout and till system offering different functions to retail businesses including but not limited to taking payments, creating bills, among others.
[41] "ABPS Banks FAQs", NPCI, accessed February 25, 2025, https://www.npci.org.in/what-we-do/nach/faqs/banks
[42] William Cook and Anand Raman, "National Payments Corporation of India and the Remaking of Payments in India." Working Paper, 2019, Washington, D.C.: CGAP, available at https://www.cgap.org/sites/default/files/publications/2019_05_07_NPCI_Working_Paper.pdf.

information like account numbers or IFSC codes of the recipients, but could be done using a mobile phone number or a quick response (QR) code which could be sent and scanned using a smartphone.[43]

To ensure a uniform customer experience for UPI and to cater to those banks which were unable to develop a UPI app for their customers, the NPCI launched its own UPI based payments app in December, 2016 named as the BHIM app (Bharat Interface for Money).[44]

The COVID pandemic further spurred the growth of UPI in 2020. UPI transactions recorded a 50% growth, from 999.57 million in April 2020 to 1,497.36 million in June 2020.[45] However, the sudden increase in transactions caused other problems such as increased transaction failures, with State Bank of India (which processed the highest number of UPI transactions) reporting a failure rate as high as 5% in September 2020.[46] These statistics have now been brought to less than 1%.[47]

3.1.2. Successes

Although demonetisation (along with the quick roll-out of the BHIM app) and the pandemic contributed to the growth of UPI, there were other efficiencies and advantages inherent in the UPI system that also contributed to its success. Some of the major ones are mentioned below:

- **Catering to small merchants and government impetus**: There has been a concerted effort by the UPI member banks to onboard small vendors and merchants by charging the same fees for such transactions as regular P2P transactions. The government has also taken various steps by exempting homegrown UPI and RuPay cards from MDR (Merchant Discount Rate) fees from January 1, 2020.[48]
- **Ease of development of third party applications**: UPI's open architecture allowed third parties to easily develop their own apps giving consumers greater

[43] Giulio Cornelli, Jon Frost, Leonardo Gambacorta, Sonalika Sinha & Robert M Townsend, "The organisation of digital payments in India - lessons from the Unified Payments Interface (UPI)," In BIS Papers chapters: Bank for International Settlements (ed.), Faster digital payments: global and regional perspectives, volume 127, 2024.pp. 61-73. https://ideas.repec.org/h/bis/bisbpc/152-05.html.

[44] "Bharat Interface for Money (BHIM)", Cashlessindia, accessed February 25, 2025, http://cashlessindia.gov.in/bhim.html

[45] "UPI Product Statistics", NPCI, accessed February 25, 2025, https://www.npci.org.in/what-we-do/upi/product-statistics

[46] A. Kumar, Choudhary, R. K., Mishra, S. K., Kar, S. K., & Bansal, R. "The Growth Trajectory of UPI-Based Mobile Payments in India: Enablers and Inhibitors", Indian Journal of Finance and Banking, 11(1), 2022. 45-59. https://doi.org/10.46281/ijfb.v11i1.1855

[47] "UPI Ecosystem Statistics", NPCI, accessed February 25, 2025, https://www.npci.org.in/what-we-do/upi/upi-ecosystem-statistics

[48] "Payment System Report, December 2024", Reserve Bank of India, accessed February 25, 2025. https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=23127

choice. However, the 80% monopoly of GooglePay and PhonePe in the UPI ecosystem has made many question whether mere open architecture is enough.[49]

- **Easy use**: The fact that a person can access the UPI ecosystem using only the bank account and an app, has made onboarding individuals much easier.

3.1.3. Drawbacks

The UPI system has been considered by many as an extremely successful project and its success is also being shared with other countries, such as the UAE, Singapore, Bhutan, Nepal, Sri Lanka, France and Mauritius.[50] However, the success of UPI does not mean that it is without any drawbacks or future challenges, some of which are discussed below:

- **Complex structure and multiple failure points**: UPI transactions are carried out using the core banking systems of both sender and receiver banks. The payment architecture has a complex structure and multiple failure points. Each transaction has four participants (the PSP, sender bank, NPCI and receiver bank) and a typical UPI transaction flow involves 18 steps, which increases the risk of potential failures.[51] However, it must be noted that the failure rate of UPI transactions has been brought down from a high of 10% in 2016 when it was launched to 0.8% in 2024.[52]
- **No incentives for investment**: UPI by itself does not add to the revenues of banks and PSPs. Its zero customer charges and zero MDR policies offer no incentive for banks to invest in infrastructure or improved customer experience.[53] While the abolition of these fees has increased the adoption of UPI by merchants, they have resulted in loss of a major revenue stream for banks and payment service providers (PSPs). However payment mandates, EMIs, overdraft accounts, B2B collection and payments continue to generate revenue for industry players. Further, PSPs are also trying to innovate and discover other sources of revenue generation apart from transaction-based revenue such as revenues from partner banks or aggregating and leveraging payment data for revenue generation, which could lead to unwanted consequences for the users such as data proliferation.[54]

---

[49] In order to address this situation UPI introduced a new rule that no single UPI application should account for more than 30% of the market, however the enforcement of this Rule has now been extended to December 31, 2026.

[50] "UPI: Revolutionizing Digital Payments in India", Ministry of Finance, December 1, 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2079544

[51] "The remarkable rise of UPI in 2020", PriceWaterhouseCooper, December 2020. https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/point-of-view/pov-downloads/the-remarkable-rise-of-upi-in-2020.pdf

[52] "UPI Achieves 99.2% Success Rate: NPCI Highlights the Success", Paytm, accessed February 25, 2025, https://paytm.com/blog/payments/upi/upi-decline-rate-drops-to-0-8-global-expansion/

[53] Jayaram Narayanan, "A Study on Growth of UPI Apps in India After COVID Outbreak", International Journal of Emerging Technologies and Innovative Research, Vol.8, Issue 9, at pg. .c333-c338, September-2021, available at http://www.jetir.org/papers/JETIR2109243.pdf.

[54] "The remarkable rise of UPI in 2020", PriceWaterhouseCooper, December 2020. https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/point-of-view/pov-downloads/the-remarkable-rise-of-upi-in-2020.pdf

- **Digital divide**: By its very nature UPI requires users to have access to digital devices and also possess a basic level of digital literacy. While mobile phone usage in India is increasing, mobile penetration still stands at only about 70%-80%,[55] further a large percentage of mobile users, specially women, do not have an exclusive device of their own.[56] Bridging the digital divide is a major concern for the growth of UPI.
- **Lack of transparency**: There are some concerns about transparency in the process of development of UPI, specially regarding participation of volunteers from certain advocacy groups[57, 58] and their mandates which were decided behind closed doors. UPI, promoted as a part of IndiaStack,[59] is neither bound by procurement prohibitions nor are their actions auditable. However, NPCI being the only retail payments organisation approved by the RBI brings up issues of lack of competition, governance and accountability in the functioning of NPCI.[60]

3.3. Direct Benefit Transfers[61]

Direct benefit transfer or DBT refers to the programme of the government of India to transfer various government benefits (fuel subsidies, etc.) directly to the bank accounts of intended beneficiaries. It was launched in 2013 with an intent to streamline the delivery of government benefits by leveraging digital technology.[62] The Indian government has from time to time announced various welfare schemes for different segments of the society. These schemes could be either Central (federal), State specific

[55] "Some 120 cr mobile phones in use in country, main priority to increase 4G network's scope: Scindia", Indian Express, July 11, 2024, available at https://indianexpress.com/article/india/mobile-phones-country-main-priority-increase-networks-scope-scindia-9447732/

[56] "Access to phones and the internet", Data for India, accessed February 25, 2025, https://www.dataforindia.com/comm-tech/

[57] The involvement of the Indian Software Product Industry Roundtable (iSPIRT) has been criticised by many for the lack of transparency around their relationship as well as potential conflicts of interest. See Trisha Jalan, "iSPIRT participation in RBI meeting on data localisation may have been 'conflict of interest': USISPF 2018 letter to Finance Ministry", August 5, 2019. https://www.medianama.com/2019/08/223-usispf-letter-to-finance-ministry-ispirt-conflict-of-interest-2/;

[58] Nileena MS, Is India privatising governance through partnerships in public digital infrastructure? October 20, 2020. https://caravanmagazine.in/policy/is-india-privatising-governance-through-partnerships-public-digital-infrastructure.

[59] India Stack is a moniker for a set of open APIs on top of which various technology applications may be built. Available at https://indiastack.org, Accessed March 28, 2025.

[60] Jyoti Panday, 'India Stack: Public-Private Roads to Data Sovereignty', Internet Governance Project, Georgia Tech, 2023. https://www.internetgovernance.org/wp-content/uploads/India_stack_9_1_2023.pdf.

[61] In addition to digitalised cash transfers, the DBT infrastructure covers broader social protection schemes. DBT 'in kind' is in use in schemes such as the Public Distribution System (PDS) through Aadhaar-enabled biometrics authentication. In addition, wage payments of workers delivering schemes (such as 'honoraria' for Accredited Social Health Activist, or ASHA workers) are transferred through DBT. In this report, we focus solely on DBT for digitalised cash transfers, pensions, scholarships, and wage payments under employment guarantee schemes.

[62] "The Direct Benefit Transfer", DBT Mission, Cabinet Secretariat, https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf. Accessed February 25, 2025.

or a joint collaboration between the Centre and the States (centrally-sponsored schemes).[63]

3.3.1. Rationale for DBT

In a number of economic analyses carried out by the government, it was found that rich households were benefiting from government subsidies more than was originally intended. Market distortions and leakages were not only causing wastage but also an opportunity cost on the use of government resources.[64] DBT was suggested as the solution to bring in "efficiency, effectiveness, transparency and accountability" in the system to ensure time bound transfer of welfare benefits into the bank account of the beneficiaries. An additional stated benefit was that the beneficiary could withdraw the benefits from anywhere in the country, which can be especially helpful for those who migrate frequently.[65]

Aadhaar is used as a means of authentication of identity of the intended beneficiary of a DBT scheme, with the added aim of reducing duplication (ensuring that a single individual is not listed as a beneficiary multiple times). DBT payments are made into the Aadhaar linked bank accounts of the beneficiaries, using Aadhaar as a financial address.

The introduction of DBT has marked a substantial shift from bank account-based benefit transfers to Aadhaar-based benefit transfers. A beneficiary's 12-digit Aadhaar has now become their primary financial address and documentation for:

i. enrolling them in schemes (through Aadhaar-linked personal data and biometrics)
ii. transferring benefits through an Aadhaar-linked payments and settlements mechanism (the Aadhaar Payment Bridge System)
iii. disbursing benefits through an Aadhaar-and biometrics-enabled cash withdrawal system (the Aadhaar enabled Payment System)

In order to ensure that intended beneficiaries could receive payments under DBT, the government had to ensure that they were part of the financial system. For this purpose, the government used the Pradhan Mantri Jan Dhan Yojana (PMJDY), launched in 2014, to open over 52.3 crore bank accounts. In order to increase financial inclusion even further, the Reserve Bank of India introduced the system of Business Correspondents / Banking Correspondents / Bank Mitras (BC) as an alternative to brick and mortar banks. A BC is a representative authorised to offer services such as cash transactions where banks do not

[63] "Schemes", India.gov.in, accessed February 25, 2025.https://www.india.gov.in/my-government/schemes-0
[64] Saurabh K. Tiwari and Anshuman Kamila, "Direct Benefit Transfer - Paradigm and Evolution", Compendium of eGovernance Initiatives, Chapter 3, Department of Administrative Reforms and Public Grievances, accessed on March 15, 2025 https://nceg.gov.in/assets/pdf/Compendium-Booklet-25th-NCeG.pdf.
[65] "The Direct Benefit Transfer", DBT Mission, Cabinet Secretariat, accessed March 17, 2025 https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf

have a branch. Business Correspondents were intended to play a vital role in operationalising the DBT programme and ensuring last mile connectivity.[66]

More than a decade since the government's efforts to scale DBT, with the Jan-Dhan, Aadhaar and Mobile (JAM) Trinity as a catalyst, digitalised welfare delivery through DBT now forms a crucial aspect of India's social protection infrastructure, spanning 1,016 central, centrally-sponsored, and state schemes as of December 2023, and having registered more than 104 crore DBT beneficiaries as of September 2023.[67]

Key schemes implemented through DBT include centrally-sponsored schemes such as the National Social Assistance Programme (NSAP), Pradhan Mantri Kisan Samman Nidhi (PM KISAN), Mahatma Gandhi National Rural Employment Guarantee Act (MGNREGA), and LPG subsidy schemes such as PM Ujjwala Yojana (PMUY).

National Social Assistance Programme (NSAP)—Set of social assistance schemes including monthly pensions for persons in households below the poverty line—elderly persons, widowed women below 60 years, and persons with disabilities below 60 years. The programme also covers the National Family Benefit Scheme, where a lump sum of INR 10,000 is transferred to a BPL household in case of the death of the primary earner.[68]

PM KISAN—Income support for landholder farmers. DBT of INR 6,000 per year transferred in three installments.[69]

MGNREGA—Rural employment guarantee programme with a legal guarantee of wage employment for adults in rural households, wherein wage payments are transferred through DBT.[70]

PM Ujjwala Yojana 2.0—DBT subsidy scheme transferred to adult women beneficiaries of poor households with a LPG connection, where a subsidy of INR 200 is transferred for each 14.2 kg LPG cylinder for up to 12 refills per year.[71]

[66] Ibid.

[67] "Ministry of Finance Year Ender 2023: Department of Expenditure", Press Information Bureau, December 27, 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1990746

[68] "About Us", National Social Assistance Program, accessed February 25, 2025, https://nsap.nic.in/circular.do?method=aboutus

[69] "Pradhan Mantri Kisan Samman Nidhi Scheme", Operational Guidelines, Ministry of Agriculture and Farmers' Welfare, March 29, 2020, https://pmkisan.gov.in/Documents/RevisedPM-KISANOperationalGuidelines(English).pdf

[70] Mahatma Gandhi National Rural Guarantee Act, 2005: Annual Master Circular 2024-25", Ministry of Rural Development, accessed February 25, 2025, https://nregaplus.nic.in/netnrega/WriteReaddata/Circulars/AMC_2024-25-English.pdf

[71] "Cabinet approves expansion of Ujjwala Yojana", Press Information Bureau, September 13, 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1957091

3.3.2. Successes

As per official records, this approach has led to significant savings for the public exchequer by cleansing scheme databases, removing millions of fake, non-existent, and ineligible beneficiaries across multiple government ministries and departments. Government figures claim that Aadhaar-driven DBT has led to the elimination of over 4.15 crore "fake" LPG connections and 5.03 crore duplicate ration cards, streamlining the distribution of essential services like cooking gas and food subsidies.[72]

However, there are some reports which suggest that not all exclusions of beneficiaries from government schemes are necessarily due to de-duplication and removal of fake beneficiaries. Some beneficiaries may have been excluded due to documentation requirements,[73] and administrative pressure to shift to APBS for payments.[74]

The DBT system has been acknowledged by the World Bank as an efficient and successful system for implementing welfare schemes especially during the COVID-19 pandemic. As per the World Bank's data more than 87% of the poorest households reported receiving at least one benefit – food or cash – under the PMGKY between May and August 2020.[75]

3.3.3. Challenges and drawbacks

Despite being considered as a significant improvement on the existing system of subsidies, DBT still has many challenges that need to be addressed. Some key challenges are highlighted below:

- **Issues with documentation**: Some individuals may not possess the required identification or access to digital platforms, leading to their exclusion from benefits.[76] Difficulties during the process of seeding details of the beneficiaries may arise due to many factors including lack of documentation, delays in document verification, or due to spelling mismatch across databases and documents. Lack of bank accounts and delays by the banks in uploading the

[72] "Aadhaar: A Unique Identity For The People", Press Information Bureau, October 24, 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2067940

[73] Sameet Panda and Vipul Kumar, "Failures in the digitisation of India's food security programme: the exclusion of married women of Odisha", Privacy International, March 23, 2021, available at https://privacyinternational.org/long-read/4468/failures-digitisation-indias-food-security-programme-exclusion-married-women-odisha

[74] The Wire Staff, "MGNREGA Sees Record Job Card Deletions in 2022-23 Due to 'Violation in Procedure', Finds Report", *The Wire*, October 20, 2023, https://thewire.in/government/mgnrega-sees-record-job-card-deletions-in-2022-23-due-to-violation-in-procedure-finds-report

[75] Shrayana Bhattacharya and Sutirtha Sinha Roy, "Intent to Implementation: Summary of Lessons from Tracking India's Social Protection Response to COVID-19", June 29, 2021, World Bank Group, available at https://documents1.worldbank.org/curated/en/404061625000764344/pdf/Intent-to-Implementation-Summary-of-Lessons-from-Tracking-India-s-Social-Protection-Response-to-COVID-19.pdf

[76] Sameet Panda, "Data Systems in Welfare: Impact of the JAM Trinity on Pension & PDS in Odisha during COVID-19", Centre for Internet and Society, February 25, 2021, available at sameet-panda-impact-of-the-jam-trinity-on-pension-pds-in-odisha-during-covid-19

seeding details on the central database (NPCI mapper) have also been highlighted as potential challenges.[77]

- **Lack of transparency and grievance redressal**: Although digitalisation was supposed to bring about transparency, challenges persist. [78] Even though the issues leading to delays in DBT may be rectifiable in most instances, the problem occurs due to the fact that beneficiaries are often unaware of the reasons behind delays and suspensions of payments.[79] Inadequate grievance redressal mechanisms for disputes related to DBT result in further challenges for beneficiaries.[80]

- **Technological glitches and procedural barriers**: Due to the heavy dependence of DBT on technology, its effectiveness may be hampered in areas with limited technological infrastructure,[81] as well as due to technological glitches.[82] There are also issues related to connectivity and slow internet speed which lead to further problems for the intended beneficiaries.[83] Apart from purely technological issues there may also be procedural problems such as freezing of the bank accounts of beneficiaries for want of complete KYC details, a problem highlighted by the RBI itself.[84]

---

[77] Abhishek Jain, Shalu Agrawal and Karthik Ganesan, "DBTL Performance Evaluation: Insights from the world's largest subsidy benefit transfer scheme", International Institute for Sustainable Development and Council on Energy, Environment and Water, April 2016, available at https://www.iisd.org/system/files/publications/dbtl-performance-evaluation.pdf

[78] Sameet Panda, "Data Systems in Welfare: Impact of the JAM Trinity on Pension & PDS in Odisha during COVID-19", February 25, 2021, Centre for Internet and Society, available at https://cis-india.org/raw/sameet-panda-impact-of-the-jam-trinity-on-pension-pds-in-odisha-during-covid-19

[79] Aarushi Gupta, Aishwarya Narayan, Pramiti Lonkar, Aarti Malik, and Nishanth Kumar, "STATE OF EXCLUSION Delivery of Government-to-Citizen Cash Transfers in India", The Social Protection Initiative, Dvara Research, June, 3, 2022, https://dvararesearch.com/wp-content/uploads/2024/01/State-of-Exclusion-Delivery-of-Government-to-Citizen-Cash-Transfers-in-India.pdf

[80] V.C. Saravanan and R. Karuppaiah, "A Critical Analysis Of Direct Benefit Transfer In India", International Journal of Novel Research and Development, Volume 10, Issue 1, January 2025, https://ijnrd.org/papers/IJNRD2501065.pdf

[81] Ibid.

[82] Rishika Kriti. "Ludhiana: PDS beneficiaries hassled as tech glitches hamper KYC", Hindustan Times, March 4, 2025, available at https://www.hindustantimes.com/cities/chandigarh-news/ludhiana-pds-beneficiaries-hassled-as-tech-glitches-hamper-kyc-101741025166100.html

[83] V.C. Saravanan and R. Karuppaiah, "A Critical Analysis Of Direct Benefit Transfer In India", International Journal of Novel Research and Development, Volume 10, Issue 1, January 2025, https://ijnrd.org/papers/IJNRD2501065.pdf

[84] "DBT: RBI Pulls up Banks for Freezing Accounts over KYC", Times of India, November 20, 2024, available at https://timesofindia.indiatimes.com/business/india-business/dbt-rbi-pulls-up-banks-for-freezing-accounts-over-kyc/articleshow/115468122.cms

- **Dependence on Aadhaar**: Overdependence on Aadhaar has led to issues due to mismatch of details between the Aadhaar database and other documents provided by the beneficiaries.[85] The process for those who do not have Aadhaar is much more cumbersome, wherein they are allowed to enroll using alternate means upon providing proof of having applied for Aadhaar.[86] Dependence on Aadhaar may also lead to disruptions in withdrawing benefits through AePS due to Aadhaar-linked biometric authentication failures.[87] Beneficiaries have reported making multiple visits for withdrawals due to these failures.[88]

- **Weaknesses in the Banking Correspondent (BC) system**: Although a large part of the DBT process is digitised, the point of contact for cash withdrawal for many beneficiaries, especially in the rural areas is the banking correspondent under the 'phygital' Aadhaar enabled Payment System (AePS). Low penetration of BCs in remote and tribal areas is still an issue that needs to be addressed.[89] Further, surveys reveal that more than a quarter of the agents are incurring losses and low revenues have a direct bearing on service quality.[90] Apart from that over 30 percent of users who rely on BCs for last mile banking services reported having to pay a certain amount of commission (bribe) that is deducted from the cash disbursed on withdrawals.[91]

[85] V.C. Saravanan and R. Karuppaiah, "A Critical Analysis Of Direct Benefit Transfer In India", International Journal of Novel Research and Development, Volume 10, Issue 1, January 2025, https://ijnrd.org/papers/IJNRD2501065.pdf

[86] Saurabh K. Tiwari and Anshuman Kamila, "Direct Benefit Transfer - Paradigm and Evolution", Compendium of eGovernance Initiatives, Chapter 3, Department of Administrative Reforms and Public Grievances, accessed on March 15, 2025, available at https://nceg.gov.in/assets/pdf/Compendium-Booklet-25th-NCeG.pdf.

[87] Nayana Kirasur, "Notes from the Field: How Does Aadhaar-Enabled Welfare Delivery Exclude Women?", IT For Change, February, 2022, available at https://itforchange.net/index.php/notes-from-field-how-does-aadhaar-enabled-welfare-delivery-exclude-women

[88] LibTech India, "Length of the Last Mile: Delays and Hurdles in NREGA Wage Payments", Foreword by Jean Dreze, LibTech India, November, 2020, https://libtech.in/wp-content/uploads/2020/11/LastMile_ReportLayout_vfinal.pdf

[89] LibTech India, "Length of Last Mile Delivery in Tribal Areas of Andhra Pradesh", LibTech, accessed on March 28, 2025, https://libtech.in/wp-content/uploads/2023/08/LOLM_Tribal_AP_English.pdf

[90] Sumita Kale, Laveesh Bhandari and V. Anantha Nageswaran, "Direct Benefit Transfers: Status and Challenges Ahead", White Paper July 2021, Indicus Foundation, available at https://www.indicus.org/admin/pdf_doc/Direct-Benefit-Transfer-Status-and-Challenges-Ahead.pdf

[91] LibTech India, "Length of the Last Mile: Delays and Hurdles in NREGA Wage Payments", Foreword by Jean Dreze, LibTech India, November, 2020, https://libtech.in/wp-content/uploads/2020/11/LastMile_ReportLayout_vfinal.pdf

3.4. Digital financial frauds and cybercrimes

The rapid growth of UPI in the last few years,[92] coupled with limited digital access and digital literacy, especially in vulnerable groups such as the elderly, women, low-literate, etc. has also seen a large number of frauds and scams being perpetrated using the UPI system.[93] It must be noted that a large number of scams are not specific to the UPI platform, but cybercriminals exploit the ease of carrying out transactions through UPI and exploit vulnerabilities in the system.[94] It is important to note that tactics are often combined by actors depending on the account and platforms targeted. In combination these tactics can be used to gain victims' trust, commit identity theft, takeover financial accounts, conduct unauthorised transactions, money laundering and extortion.

Looking at reported incidents of fraud compiled by the RBI, and the National Cybercrime Reporting Portal,[95, 96] and news reportage on emerging forms of online fraud, here is a broad compilation of financial frauds enacted online. Click on the hyperlinks, if you would like to learn more about the modus operandi or real-world cases described in the table Figure 3.1.

Figure 3.1. An illustrative list of digital financial fraud mechanisms

Modus Operandi	Brief definition	Can look like		
Social engineering	Psychological manipulation to trick individuals into disclosing financial and personal information, or providing direct access to accounts and financial assets.	Baiting: Offering something enticing to deceive individuals into revealing financial details, like lottery and online job scams, as well as fake advertisements with deep discounts	Pretexting: Creating a false scenario to extract sensitive information or payments, e.g. romance scams	Social intimidation: Threatening individuals with spreading misinformation or doctored images within known circles to extort ransom payments, e.g. sextortion and fraudulent loan scams

[92] "UPI transactions have increased from 1,246.84 million in March, 2020 to 16,730.01 million in December, 2024", NPCI, accessed on February 25, 2025, https://www.npci.org.in/what-we-do/upi/product-statistics.
[93] TOI Tech Desk. "RBI data suggests rise in online payment frauds in India: Reasons and what users should do", Times of India, June 2, 2024, https://timesofindia.indiatimes.com/technology/tech-news/rbi-data-suggests-rise-in-online-payment-frauds-in-india-reasons-and-what-users-should-do/articleshow/110627011.cms
[94] "UPI Frauds: Common Types of UPI Scams & Prevention Methods", Razorpay, February 26, 2025, https://razorpay.com/blog/upi-frauds-types-tactics/
[95] Reserve Bank of India. "Be(A)ware: A Booklet on the Modus Operandi of Financial Fraudsters", Office of the RBI Ombudsman (Mumbai-II), 7 March 2022, https://rbidocs.rbi.org.in/rdocs/content/PDFs/BEAWARE07032022.pdf
[96] Learn About Cybercrime", National Cyber Crime Reporting Portal, accessed 22 Feb 2025, https://cybercrime.gov.in/webform/crimecatdes.aspx

Phishing	Impersonating a trusted organisation through the circulation of fake websites and links via SMS, social media, email or instant messenger to spread malware or con individuals into divulging sensitive information	Smishing: Circulating fake links to websites that look legitimate, such as those of banks or e-commerce sites, via SMS or instant messenger. When customers click on the link and enter their credentials fraudsters capture them.	Vishing: Vishing or voice phishing is a phishing attack over a telephone call. Imposters pose as bank employees, company executives, insurance agents, or government officials, and share some of the customer's personal information to gain their confidence. They then trick or pressurise customers into sharing confidential information, such as passwords, PINs, OTPs or CVVs, using urgency or emergency as a pretext.	Email phishing: The scammer may send an email impersonating an employer, relative, or company to get individuals to respond with sensitive details or conduct financial transactions.
Use of public infrastructure	Installing devices to capture sensitive information without being detected as individuals use installed infrastructure	Juice jacking: Public charging ports to transfer malware to customers' phones, allowing them to access or steal sensitive data such as emails, SMS or saved passwords.	Card skimming: Fraudsters install skimming devices in ATM machines and point of sale devices to steal credit and debit card data to create a duplicate card. They may also install a dummy keypad or hidden camera to capture ATM pins.	AePS agent based fraud: Banking correspondents may conduct unauthorised transactions without the customer's awareness to withdraw additional cash or may pretend to deposit cash while pocketing it
Other forms of Impersonation	Scammers pose as authority figures, family members or customer service agents to draw from the trust and legitimacy associated with that position or brand	Tech support fraud: Fraudsters pose as tech support agents online to target individuals who are not tech savvy into sharing remote access to their devices via screen mirroring software	Social media impersonation: Scammers create fake social media accounts using users' details. They then send requests to the users' friends for money or blackmail or extort them for money using their private information.	AI voice scams: Using AI generated voice clones over calls to convince people a loved one is in a danger or a tight situation and needs money urgently

E-commerce frauds	Using e-commerce sites to deceive consumers into purchasing an item, then delivering a counterfeit or nothing at all	Non-delivery of goods	Counterfeit products: Selling imitation or counterfeit goods online while advertising something else on the listing	Phoney marketplaces: Creating websites that appear genuine but fail to deliver purchased products.
Fraudulent investment opportunities	Fraudulent investment schemes targeting investors through social media, unverified mobile applications, and other online platforms.	Ponzi schemes: Promising high returns to early investors with funds sourced from subsequent investors.	Rug pull scams: Developers of decentralised finance initiatives, like NFTs and cryptocurrencies, may mislead individuals to invest in a new project and then abandon it just to abscond with the funds invested, leaving investors with a worthless asset.	Pump and dump schemes: Influencers may spread misinformation through their influence on social media and other media channels, to drive share prices high. Once the share price is elevated, they dump a large chunk of shares booking a profit. Meanwhile, leaving gullible retail investors vulnerable to loss.

Sources: *Multiple: Analysis by CIS of reported incidents of fraud compiled by the RBI, and the National Cybercrime Reporting Portal; RBI informational booklet on modus operandi of digital financial frauds (see here); and news reporting and research reports compiled from desk research by CIS, hyperlinked above.*

3.4.1. Redressal mechanisms

One of the most common ways in which the authorities, both governmental as well as private, try to prevent digital financial frauds is by spreading awareness about these frauds through SMS-based, IVR, and online public interest campaigns informing users not to share their personal information with unverified individuals.[97] At an institutional level, the NPCI implements a Real-time Fraud Risk Monitoring and Management Solution (FRM), a system which processes transactions in real time and near real time mode using model scores based on artificial intelligence. Based on fraud reporting by member banks, NPCI analyses the data to identify fraud trends, takes corrective and mitigating action, and also initiates ecosystem level changes by engaging with relevant stakeholders. NPCI also carries out workshops and training sessions for its stakeholders on an ongoing basis.[98]

[97] "Fraud Awareness", NPCI, accessed on February 25, 2025, https://www.npci.org.in/npci-in-news/knowledge-centre/fraud-awareness
[98] "Fraud Risk Management", NPCI, accessed on February 25, 2025, https://www.npci.org.in/who-we-are/risk-management/fraud-risk-management

In terms of customer liability, the RBI Guidelines on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions,[99] dated July 6, 2017 state that customers have the obligation to report unauthorised or fraudulent transactions to their banks as soon as possible, the longer the time taken for reporting, higher would be the chance of loss. The Guidelines specify that the customer will be liable to zero loss under very limited circumstances specified in the Guidelines.[100] This zero loss protection is not valid if the loss has been caused by the "negligence"[101] of the customer (such as by revealing payment credentials).

In 2021, the RBI issued the Integrated Ombudsman Scheme, 2021,[102] which offers an alternative grievance redressal mechanism to users for any shortcoming or inadequacy in service (irrespective of financial loss) by banks, or fintech entities providing UPI, BBPS, AePS, or other similar fintech services. Users have the option to file a complaint using the RBI complaints management system platform or by sending a physical complaint via mail, if they do not receive appropriate redressal of their complaints by the fintech entities.[103]

Another option that users have in case they are victimised by cyber frauds is reporting the transaction to the National Cyber Crime Portal, which has a dedicated link for financial frauds;[104] however, there is no substantive data available to show how effective or ineffective this method is in redressing financial frauds.

3.5. Regulatory framework

The financial sector in India is primarily regulated by two regulators, the Reserve Bank of India (RBI), India's central bank which regulates banks and other finance companies, and the Securities and Exchange Board of India (SEBI), which regulates the securities markets in India.[105] The RBI and the SEBI are both independent regulatory bodies which derive their powers from legislation and perform the dual role of regulation as well as enforcement for their respective parts of the financial sector. Payment services are governed by the Payment and Settlement Systems Act, 2007 under which entities can ask for different licenses such as payment aggregators, payment gateways as well as

[99] "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions", RBI Circular, dated July 6, 2017, available at https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=11040

[100] Ibid.

[101] Ibid.

[102] Reserve Bank of India. "Reserve Bank – Integrated Ombudsman Scheme, 2021", available at https://rbidocs.rbi.org.in/rdocs/content/pdfs/RBIOS2021_amendments05082022.pdf

[103] Complaint Management System, Reserve Bank of India, accessed on March 30, 2025 https://cms.rbi.org.in/cms/indexpage.html#eng

[104] "National Cybercrime Reporting Portal", Indian Cyber Crime Coordination Centre, accessed on February 25, 2025, https://cybercrime.gov.in/Webform/Index.aspx

[105] There are also other institutions such as the Insurance Regulatory and Development Authority (IRDA), the Forward Markets Commission, etc. but the RBI and the SEBI are the two most important institutions.

prepaid payment instruments. The Act designates the RBI as the authority with the power and responsibility for regulating and supervising the payment systems in India.[106]

The NPCI is the only entity which has been authorised as a Retail Payments Organisation by the RBI under the Payment and Settlement Systems Act, 2007 and as of March 11, 2025 eight of its payment systems,[107] including UPI, had received approval from the RBI as authorised payment systems.[108] As part of its regulatory and supervisory function over payment systems, the RBI issued Guidelines on Regulation of Payment Aggregators and Payment Gateways in 2021,[109] which imposed a licensing requirement on payment aggregators, that is, entities that facilitate integration of various payment instruments for e-commerce sites and merchants.[110] Popular payment aggregators such as Razorpay, Mpay, Amazon Pay, and so on, fall into the category of payment aggregators that have been approved by the RBI.[111] The RBI also provides various conditions that the payment aggregators have to adhere to during operations including capital adequacy, governance, merchant onboarding, KYC, etc.[112] However, payment gateways, which provide technology infrastructure to route and facilitate processing of an online payment transaction without any involvement in handling of funds are essentially treated as technology providers or outsourcing partners[113] and are only required to adhere to certain information security and risk management requirements.

The RBI, in 2017, also issued a Master Direction on Issuance and Operation of Prepaid Payment Instruments.[114] These Master Directions define Prepaid Payment Instruments (PPIs) as instruments which facilitate purchase of goods and services, financial services, remittance facilities, and so on, against the value stored on the instruments. Typically e-wallet services would fall within this definition. PPIs are divided into different kinds

[106] Preamble, Payment and Settlement Systems Act, 2007.
[107] National Financial Switch (NFS), Immediate Payment Service (IMPS), Affiliation of RuPay Cards issued by banks and co-branded credit cards issued by NBFCs, National Automated Clearing House (NACH), Aadhaar enabled Payment System (AePS), Cheque Truncation System, Unified Payments Interface (UPI), National Electronic Toll Collection (NETC).
[108] "Approvals/ Certificates of Authorisation issued by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for Setting up and Operating Payment System in India", Reserve Bank of India, March 24, 2025, https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=12043
[109] "Guidelines on Regulation of Payment Aggregators and Payment Gateways", Reserve Bank of India, accessed on March 29, 2025, available at https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0
[110] Regulation 1.1.1, "Guidelines on Regulation of Payment Aggregators and Payment Gateways", Reserve Bank of India, https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0
[111] "Approvals/ Certificates of Authorisation issued by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for Setting up and Operating Payment System in India", Reserve Bank of India, March 24, 2025, https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=12043
[112] Regulations 4, 5, 6, 7, etc. "Guidelines on Regulation of Payment Aggregators and Payment Gateways", Reserve Bank of India, https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0
[113] Regulation 3.7, "Guidelines on Regulation of Payment Aggregators and Payment Gateways", Reserve Bank of India, https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0
[114] "Master Directions on Prepaid Payment Instruments (PPIs)", Reserve Bank of India, accessed on March 29, 2025, available at https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156

such as closed system PPIs such as small PPIs,[115] full-KYC PPIs,[116] PPIs for Mass Transit Systems,[117] etc. PPIs are classified as instruments which allow purchase of goods and services from the issuing entity only, do not permit cash withdrawal and cannot be used for payment or settlement for third party services, which do not require RBI approval[118]. The Master Direction prescribes different terms and conditions for regulating each of the above types of PPIs depending upon their unique characteristics such as KYC requirements, loading limits, withdrawal limits, transfer limits, etc.

Due to the fast paced growth of the digital credit market, in 2023, the RBI issued the Digital Lending Guidelines to regulate the digital lending activities of banks and non bank finance companies (NBFCs).[119] These Guidelines impose a number of conditions on the digital lending service providers including including those related to disbursal of funds, disclosures, fees and charges, borrower's creditworthiness and due diligence, cooling off/look-up period, data protection, privacy policies, grievance redressal as well as reporting requirements, etc.

While UPI and DBT have both found a significant amount of success in terms of their adoption by volume and their stated objective of transparency and financial inclusion, there are certain challenges that still need to be addressed, especially relating to the financial harms that may arise due to the adoption of these technologies by vulnerable groups. The current regulatory framework dealing with financial harms offers limited scope of redressal and needs to be made more robust and effective.

This issue of financial harms is explored in greater detail in the subsequent chapters, where we outline the findings from our research on the use of various digital financial services, with a focus on learnings related to UPI, social protection and digitalisation through DBT, and the growing prevalence of frauds and harms on online platforms, as it relates to certain vulnerable user groups.

[115] Regulation 2.8, "Master Directions on Prepaid Payment Instruments (PPIs)", Reserve Bank of India, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
[116] Ibid.
[117] Regulation 10.2, "Master Directions on Prepaid Payment Instruments (PPIs)", Reserve Bank of India, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
[118] Regulation 2.1, "Master Directions on Prepaid Payment Instruments (PPIs)", Reserve Bank of India, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
[119] "Guidelines on Digital Lending", Reserve Bank of India, accessed on March 29, 2025, available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12382&Mode=0

4.

Access to digital devices and financial services

4.1. Device access and ownership

Digital financial services assume a foundational level of access to financial services, the internet, and mobile messaging. While there are agent based services that aim to bridge the "digital divide," and provide phygital access[120] to digital financial services, having a mobile phone and number has become essential to verify identity and transactions over digital banking and fintech platforms.

Our survey looked at ownership of digital devices to understand respondents' device ownership and frequency and the nature of their internet usage. Understanding patterns of shared usage of household devices can also help understand whether certain groups face greater dependence or higher risk of exclusion from financial services. This is

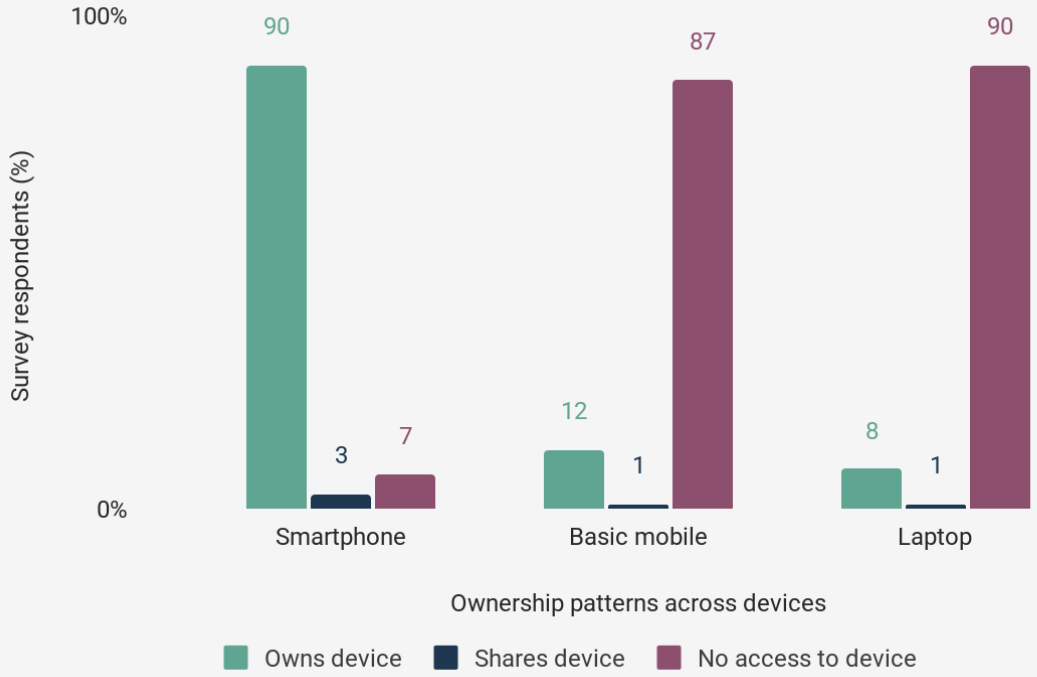
[120] Phygital experiences combine online and offline environments. This includes digital services mediated by agent based in-person support like banking services through the Aadhaar enabled Payments System (AePS) or in person services that are augmented using digital technology like ATMs.
For more, see Pasquale del Vecchio, Giustina Secundo, and Antonella Garzoni, "Phygital technologies and environments for breakthrough innovation in customers' and citizens' journey. A critical literature review and future agenda", *Technological Forecasting and Social Change* 189, (2023), https://www.sciencedirect.com/science/article/abs/pii/S0040162523000276

because financial services' verification procedures may necessitate limiting the number of accounts or wallets that can be created for applications on a single device.[121]

As seen in **figure 4.1.**, smartphones had the most usage among digital devices with 90% of respondents owning one followed distantly by basic or feature mobile phones at 12%. This is reflective of the vast majority of internet users whose access to the internet and online services begins with a mobile first pathway.

Figure 4.1. A majority of respondents owned a smartphone as compared to a basic mobile device or a laptop

Percentage of respondents, by device ownership (N = 3,784)



According to the 2023 GSMA Consumer Survey 28% of Indian users reported shared access being a barrier to mobile use.[122]

As **figure 4.2**. shows next, Rajasthan, Tamil Nadu and Karnataka had no users reporting shared access to smartphones. In Assam, West Bengal and Uttar Pradesh, over 65% of respondents who had no access to a smartphone were from rural areas.

[121] "Troubleshooting", *Paytm.com*, accessed November 2024, https://paytm.com/offer/kyc/troubleshooting
[122] GSMA. "The Mobile Gender Gap Report", GSMA, May 2024, https://www.gsma.com/r/wp-content/uploads/2024/05/The-Mobile-Gender-Gap-Report-2024.pdf?utm_source=website&utm_medium=button&utm_campaign=gender-gap-2024

Figure 4.2. A higher proportion of respondents did not own a smartphone in Rajasthan and Maharashtra

Smartphone ownership patterns, by states and UTs (percentage of respondents) [N = 3,784]

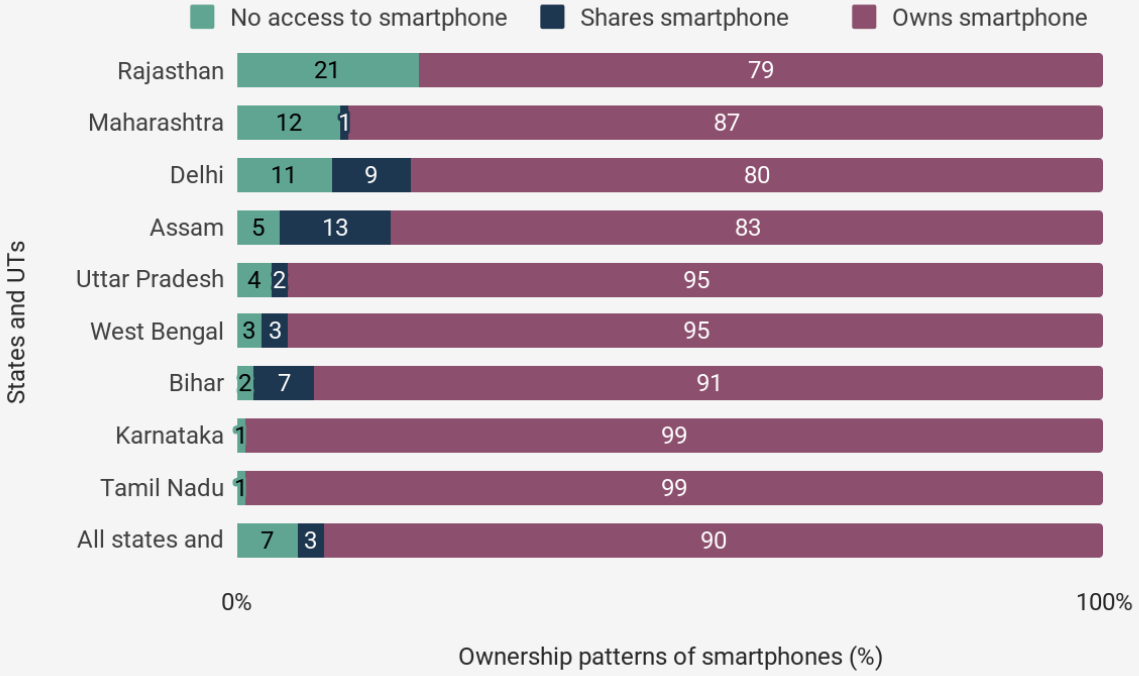
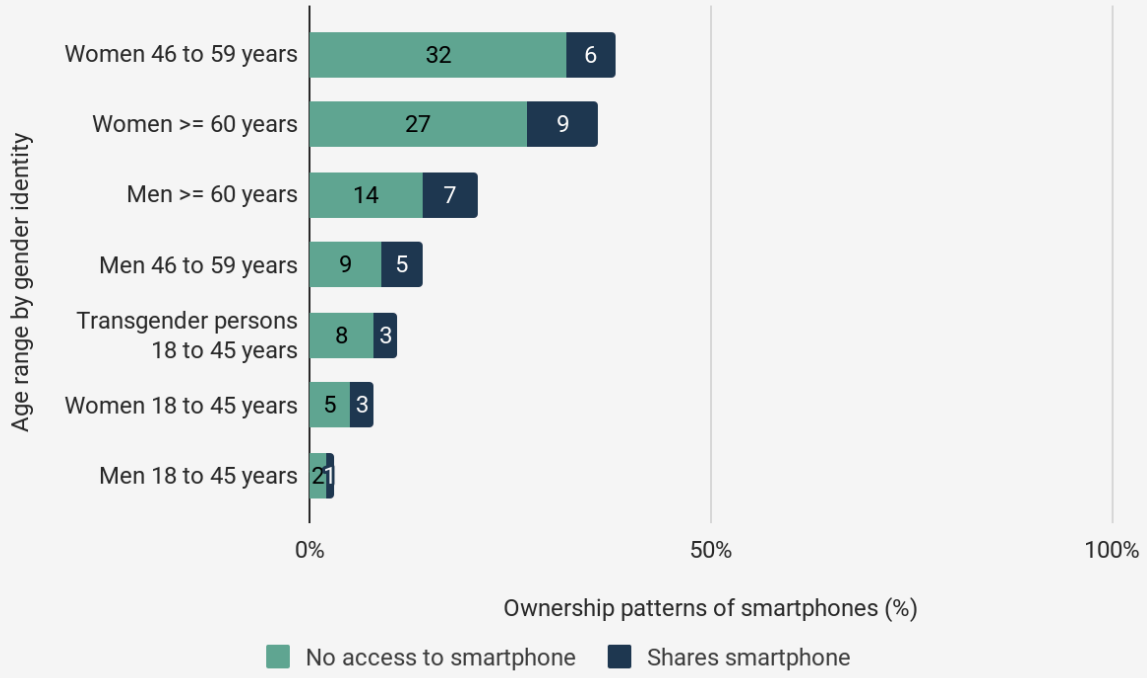


Figure 4.3. A higher proportion of women and men over 60 had shared access or did not own a smartphone at all

Percentage of respondents with shared or no access to smartphones, by age and gender identity [N = 381]



Note: Less than 1% of the respondents above 46 years were transgender persons and have therefore not been included as a category in this figure

In our study, reliance on shared usage was higher for certain groups, and age and gender were both factors for this. As seen in **figure 4.3**., the gap widens significantly for women over the age of 45 when compared with men in similar age brackets.

Among respondents who did not have any access to a smartphone (either owned or shared), almost two-thirds were women. Women's access to smartphones has been increasing however in recent years. Data from the National Family Health Survey shows that rates of mobile ownership among women grew in both rural and urban areas, from 37 percent in 2015–16 to 47 percent in 2019–21.[123] 9% of transgender respondents also did not own a smartphone, or have shared access to compensate.

Gendered aspects of reliance on shared smartphones

When it comes to smartphones, many households in India rely on shared devices that are primarily owned by male members of the household.[124] Women in rural areas, in particular, who did not own smartphones were the ones still using feature phones without mobile internet capabilities.

Women who attended a focus group discussion in rural Maharashtra mentioned that for most households in their district the household smartphone was reserved by the men of the household for personal use.

> When women don't even have smartphones, how do they access or utilise these [digital] services?
>
> **—CBO representative in a focus group discussion with SHG women in Velhe, Pune**

Marital status has also been observed to be an influencing factor for digital inclusion. Alongside lower rates of mobile ownership, married women have lower levels of digital literacy when compared to men and unmarried women.[125]

[123] "NFHS-5: Uptick in Health Indicators across India", Press Information Bureau, 20 December 2021, https://static.pib.gov.in/WriteReadData/specificdocs/documents/2021/dec/doc2021122061.pdf
[124] Abhishek Waghmare, "Access to phones and the internet", *Data for India*, 29 February 2024, https://www.dataforindia.com/comm-tech/
[125] M Vimalkumar, Jang Bahadur Singh, and Sujeet Kumar Sharma, "Exploring the multi-level digital divide in mobile phone adoption: A comparison of developing nations," Information Systems Frontiers, 23, (2021), 1057-1076. https://doi.org/10.1007/s10796-020-10032-5.

Persons with disabilities faced challenges with smartphone access

10%
(24 out of 230) did not own a smartphone

11%
(25 out of 230) only had shared access to a smartphone

Persons with disabilities often require assistive tech to ensure independent access to digital devices and services that may not centre their access needs.[126] Smartphone UI often includes some assistive technology features that can improve their utility for PwDs with vision, mobility, speech, cognitive and other impairments. This includes features like text to speech, dictation (speech to text), voice recognition, setting reminders, simplified gestures and ability to control text size and other screen parameters.[127] Some advocates consider smartphones an assistive technology in themself as well as an enabler of access to assistive technologies.[128]

Having a smartphone has increased accessibility of financial and communication services for persons with disabilities. For example, research participants with speech and hearing impairment used video calls for phone-based conversations in Indian Sign Language (ISL). During a focus group discussion, a participant with a visual impairment from Bengaluru, described their reliance on in-built device talkback features and assistive technologies to use digital financial services and other applications independently.

However, difficulties in accessing mobile based services persist since built-in assistive tech may not function smoothly across mobile applications and websites, and due to challenges with third party app integration.[129]

---

[126] Assistive technologies include a broad range of physical products and digital technologies that can support people by either helping maintain or improve an individual's functioning (related to cognition, communication, hearing, mobility, self-care and vision) or improving accessibility of a service or information that would otherwise be unavailable.
"Assistive technology", *World Health Organization*, accessed December 2024.
https://www.who.int/news-room/fact-sheets/detail/assistive-technology
"What is AT?", *Assistive Technology Industry Association*, accessed December 2024,
https://www.atia.org/home/at-resources/what-is-at/

[127] "Assistive technology in your pocket: the transformative potential of smartphones", *ATScale*, accessed December 2024,
https://atscalepartnership.org/news/2023/5/30/assistive-technology-in-your-pocket-the-transformative-potential-of-smartphones

[128] Ibid
"Mobile phones as assistive technologies: Gaps and opportunities", AT2030, 5 August 2019,
https://at2030.org/static/at2030_core/outputs/Mobile-phones-as-assistive-technologies.-Gaps-and_B2wSGDl.pdf

[129] Suraj Singh Senjam, Souvik Manna, and Covadonga Bascaran. "Smartphones-Based Assistive Technology: Accessibility Features and Apps for People with Visual Impairment, and its Usage, Challenges, and Usability Testing", *Clin Optom* volume no. 13 (2021): 311-322,
https://pmc.ncbi.nlm.nih.gov/articles/PMC8636846/

4.2. Age and gender are significant determinants of internet access and use

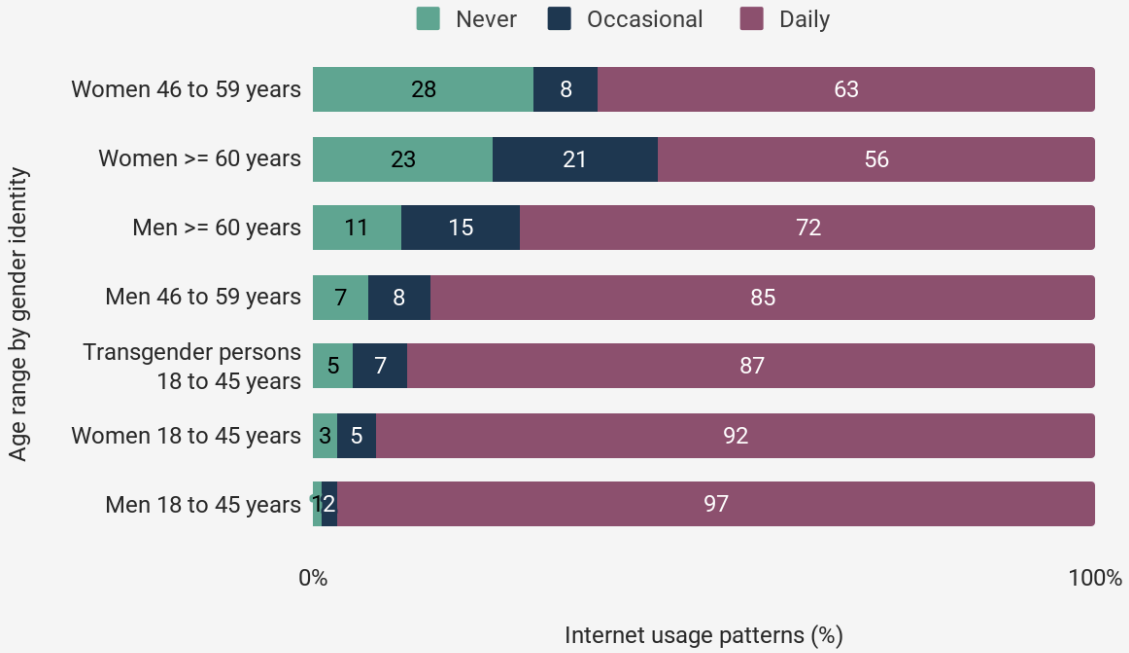
88% of the respondents in our survey used the internet everyday.

5% of the respondents reported never using the internet.

Consistent with recent consumer surveys,[130] age and gender were significant factors in determining internet usage. Around a fourth of women over 45, and around one in ten men over 60, reported never using the internet (see figure 4.4).

Figure 4.4. A higher proportion of women and men over 60 had never used the internet

Internet usage patterns by age and gender identity (percentage of respondents) [N = 3,784]



Note: Less than 1% of the respondents above 46 years were transgender persons and have therefore not been included as a category in this figure

Role of language: 14% of survey respondents did not use the English language at all, with another 25% only being familiar with some popular words and phrases. Language accessibility is a basic requirement for users to be able to use mobile applications independently, and reducing reliance on mediators and phygital services. Users who

[130] KANTAR/IAMAI. "Internet in India 2023", KANTAR/IAMAI, April 2024, https://www.iamai.in/sites/default/files/research/INTERNET%20IN%20INDIA%202023.pdf
Abhishek Waghmare, "Access to phones and the internet", *Data for India*, 29 February 2024, https://www.dataforindia.com/comm-tech/#lf-ftntref11

prefer to access internet and digital services in regional-languages comprise a large section of the active internet user base in India, with a study conducted by Google and KPMG stating that nine out of ten new internet users are likely to be native language speakers.[131]

4.3. Adoption of digital financial services

The digitalisation of financial services within this context has had to take place alongside programmes to improve financial inclusion and digital literacy. While digital financial services offer convenience, possibilities for independence and decreased transaction costs, we also see challenges in the same areas for vulnerable users.

In this chapter, we will explore access and adoption of various financial services, physical, phygital and digital. This section, Section 4.3, starts with a look at access to basic banking infrastructure and utilisation of bank accounts which is the foundational layer for financial inclusion, and necessary to enable access to digital financial services. We then examine infrastructure like the Aadhaar enabled Payments System (AePS) and the network of Automated Teller Machines (ATMs) that act as phygital interventions to improve convenience and access to selected banking services, and are the main avenues available to customers for cash withdrawals. Section 4.4.looks at the adoption of net banking and UPI services across different demographics. The final section, Section 4.5., discusses challenges with infrastructure, digital literacy and consumer support services that impact the adoption of digital financial services.

4.3.1. Access to banking infrastructure: The physical layer

A bank account is a key node in a consumer's journey of accessing and utilising digital financial services provided by banks, non-banking financial companies (NBFCs), and fintech platforms. It acts as a financial address, and key component of financial history and identity.

As bank account ownership was a precondition of the study, 99% of survey respondents had a personal bank account, and 3% also had joint accounts.

While there are many factors that have led to rapid adoption of digital financial services, there is some agreement that pandemic era measures and wide level bank account ownership, achieved with support from the Jan Dhan Yojana, were the foundation

[131] KPMG. "Indian Languages Defining India's Internet", KPMG, April 2017, https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Indian-languages-Defining-Indias-Internet.pdf

necessary to develop these services.[132] [133] An interview with a digital payments researcher, highlights how regulatory push as well as consumer demand created a fertile ground for growth in the digital payments ecosystem:

> This rapid adoption of UPI and other financial services has been partly driven by a regulatory push, and partly by consumer demand. It was growing at a constant pace, but there have been spikes like the Covid-19 lockdowns. This exponential growth, and its impacts have been understudied.
>
> Lot of new product categories and payment systems have been launched. Regulatory interventions are creating new marketplaces and closing doors on others. The larger theme here, since 2007 [Payment and Settlement Systems Act, 2007, RBI], is a long-term regulatory vision of having a centralised financial infrastructure. There are costs and benefits to this.
>
> **—A digital payments researcher from a consumer collective, in an interview**

Risks of exclusion of persons with disabilities and transgender users in banking and digital financial services

While bank account ownership is near universal, this is not the case for some groups. Persons with disabilities often face discrimination and infantilisation in the banking system.[134] Persons with disabilities often have to perform additional self-advocacy work to counter discriminatory attitudes or find accommodations for missing accessibility features when getting access to traditional and digital banking services.[135] This can even begin at the level of opening a bank account. A woman with a visual impairment from Bengaluru shared that she had been denied a bank account in her village because of ableist assumptions of the local bank employees. The bank felt opening a bank account for her would pose a higher risk of theft and manipulation, creating more liability for them:

---

[132] Ajit Ranade, "Role of 'Fintech' in Financial Inclusion and New Business Models", *Economic and Political Weekly* Volume 52., Issue 12. (2017): 125-128, https://www.jstor.org/stable/44166832.

[133] The wide reach of the Jan Dhan Yojana, launched in 2014, has also made banking services more affordable and increased enrollment. According to the Global Findex, individual bank account ownership in India grew from 35% in 2011 to 80% in 2017, dipping slightly in 2021 to 77.5%. However, accounting for a large number of inactive accounts, the account penetration for active bank account users in India is only 50% "The Global Findex Database 2021", *World Bank Group*, accessed November 2023, https://www.worldbank.org/en/publication/globalfindex/Data

[134] M Karpagam, "Indian banks can't ignore persons with disabilities. RBI guidelines exist for a reason", *The Print*, 30 March 2022, https://theprint.in/opinion/indian-banks-cant-ignore-persons-with-disabilities-rbi-guidelines-exist-for-a-reason/894115/

[135] Kameswaran et. al, "Advocacy as Access Work: How People with Visual Impairments Gain Access to Digital Banking in India", Proceedings of the ACM on Human-Computer Interaction, Volume 7, Issue CSCW1 (2023): 1-23, https://dl.acm.org/doi/abs/10.1145/3579596

It's not like I am afraid of using GooglePay or Phonepe. In fact, I had gone to my hometown to try and open an individual bank account. But, I was told that, "You are blind and you will not be able to handle it" and sent back.
I think it is because the bank is concerned that if something happens, like if cash gets stolen from visually impaired customers, then the bank will have to repay.

—Participant in a focus group discussion with persons with disabilities in Bengaluru, Karnataka

Transgender people may at times face enrollment barriers when opening bank accounts due to documentation inconsistencies or lack of identity documents like PAN and Aadhaar.[136] This is despite the 2015 RBI directions for banks to include a 'third gender' column in their forms to facilitate opening bank accounts.[137] Opening a bank account can still become a challenge because of discrepancies across documents[138] where gender and names may not match. For people who have left home, they may not have documentation like rental agreements or electricity bills in their name to show they live near a particular bank branch. A study from Odisha found other factors including low financial literacy, awareness, lack of formal employment, and discriminatory behaviour of bank staff were responsible for low levels of bank account ownership among the transgender community.[139] As we heard from an interviewee working with gender and sexual minorities

Individuals may not have a formal proof of address. I have seen a case where registration for new bank accounts became an issue for residents of one community. If it's one person you can show an address, but if it's 25 people with the same address then that brings up issues. Registration processes have been stalled for many because of similar issues.

For those who have older bank accounts, this can create an issue at the KYC stage when linking with payment platforms. This also happens because some hesitate from updating their documents like Aadhaar and PAN or going through with a KYC process, even after receiving a transgender ID, from fear of their gender identity being revealed to their families.

— Project staff at a CSO working with gender and sexual minorities

[136] Vinita Bhatia, "The Trans Community's Never-Ending Fight For Financial Inclusion", *Outlook Business*, 15 June 2022, https://www.outlookbusiness.com/news/the-trans-community-s-never-ending-fight-for-financial-inclusion--news-202307

[137] "RBI directs banks to include 'third gender' in forms", *India Today*, 5 March 2015, https://www.indiatoday.in/business/story/rbi-third-gender-transgender-in-forms-directs-banks-249996-2015-03-05

[138] Arushi Raj and Fatima Juned, "Gendered identities and digital inequalities: an exploration of the lived realities of the transgender community in the Indian digital welfare state", *Gender & Development*, volume no. 30, issue no. 3 (2022): 531-549, https://www.tandfonline.com/doi/full/10.1080/13552074.2022.2131250;

[139] Rajesh Barik and Pritee Sharma, "What Constraints Financial Inclusion for the Transgender Community? Field-based Evidences from Odisha (India)", *Contemporary Voice of Dalit*, volume no. 13, issue no. 1 (2021): 66-80, https://journals.sagepub.com/doi/abs/10.1177/2455328X20922434?journalCode=voda

4.3.2. Adoption of Aadhaar enabled Payments System: A phygital intervention

AePS allows users to bypass the need for physical visits to the bank and an ATM for cash withdrawals or deposits. Instead, a customer can access these services by visiting a Customer Service Point (CSP) or engaging a business correspondent. They serve as a retail agent duly authorised by financial institutions to provide a restricted spectrum of banking services.[140]

Biometric banking

In our study, 66% of the respondents had enabled their bank accounts for biometric transactions.

Biometrics are used across physical, phygital and digital mediums of banking to verify identity, authenticate transactions and prevent fraud. This can be done using iris scans, fingerprint, voice and facial recognition, as well as analysis of behavioral biometrics.[141] AePS discussed earlier is a good example of biometric banking where iris scans or fingerprints are used to verify customer identity and initiate transactions.

Among those who had biometric enabled bank accounts, we observed higher percentages in certain regions, states and among specific user groups. More respondents in rural areas (78%) had bank accounts enabled for biometric banking while it was less than 60% in urban areas. Across states, less than 50% of the respondents in Tamil Nadu and Maharashtra were using biometric verification for banking. Whereas in Karnataka and Uttar Pradesh, over 90% of the respondents had enabled their bank accounts for biometric banking, as seen in **figure 4.5.**

Compared to the general population, where only 62% report having enabled their bank account for biometric banking, 72% of the respondents with disabilities and 81% of transgender respondents had a biometric enabled bank account.

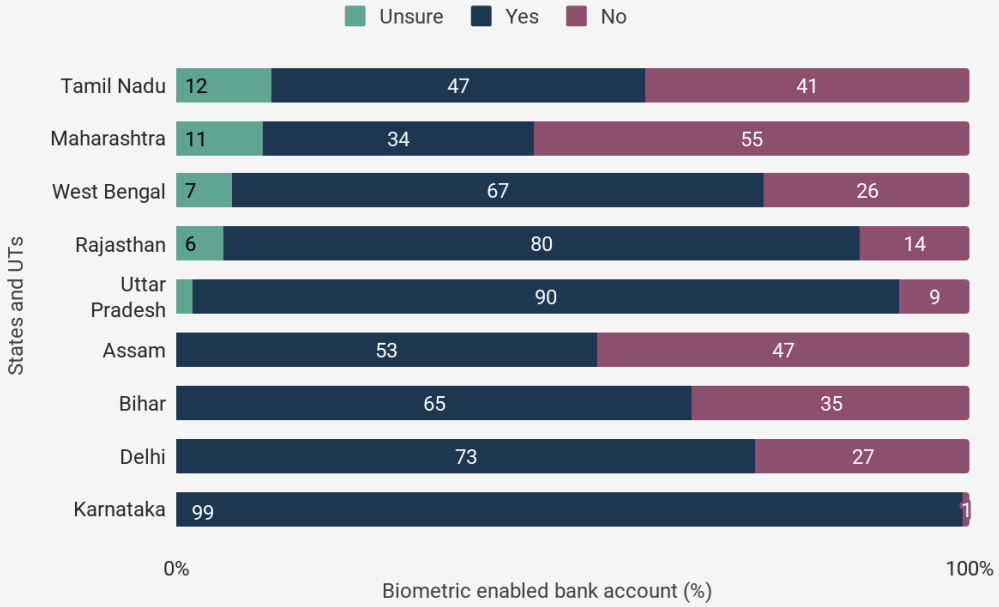
Where across age groups under 60, around 65% of the respondents in each age group had such an account, a much higher 74% of the elderly respondents had enabled their bank account for biometric enabled banking.

[140] Ibid

[141] Bahadori, Mina & Soltani, Morteza & Soleimani, Masoumeh & Moshayedi, Ata Jahangir & Marani, Mehdi, "The Role of Biometric in Banking: A Review.", *EAI Endorsed Transactions on AI and Robotics,* (2023), doi:10.4108/airo.3676

Figure 4.5. A higher proportion of respondents in Tamil Nadu and Maharashtra were unaware of the biometric status of their bank account and less likely to have such accounts compared to other states and UTs.

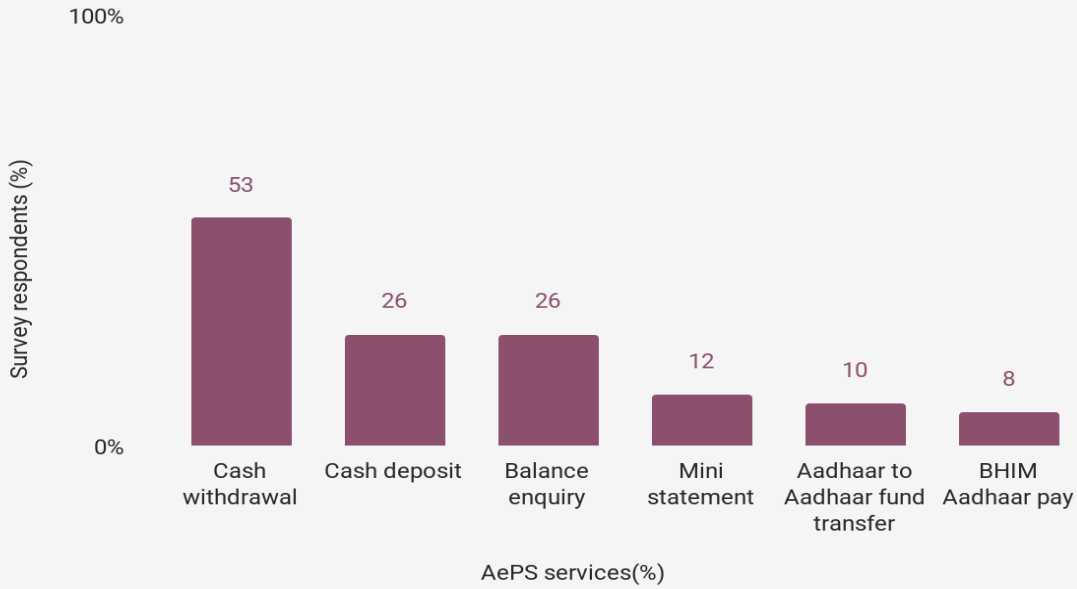
Status of biometric enabled bank account by states and UTs (percentage of respondents) [N = 3,784]



60% of respondents with biometric enabled bank accounts have used banking services provided through biometric and Aadhaar authentication via AePS, with cash withdrawal being the most commonly sought out service, as seen in **figure 4.6.**

Figure 4.6. Respondents largely used AePS enabled services for cash withdrawal.

Percentage of AEPS enabled services used by respondents (N = 3,784)



According to the NPCI, 618.32 million transactions were approved over the AePS network in October 2024. Interoperability of the network allows for improved service availability. 42% of these transactions valuing 31,720 crore rupees were off-us transactions,[142] facilitated by business correspondents for account holders from different banks.[143]

In 2024, 81.8% of business correspondent run banking outlets were opened in villages with a population under 2000.[144] This more cost-effective phygital infrastructure has been stepping in to make up for the lack of access to brick and mortar banking services in remote villages with low population density.

A researcher we spoke with sees this as an inevitable shift away from brick and mortar branches.

> Increasing reach through AePS needs lower levels of investment and infrastructure compared to banks. The pitfall of a bank is its distance and crowds. It has a higher cost per visit and most users' passbooks are never updated, because banks are short staffed and always very crowded.
>
> There are no easy tech fixes for inadequate capacity and infrastructure. This is going to lead to a shift to AePS.
>
> **— A researcher working with rights based campaigns to improve welfare delivery, in an interview**

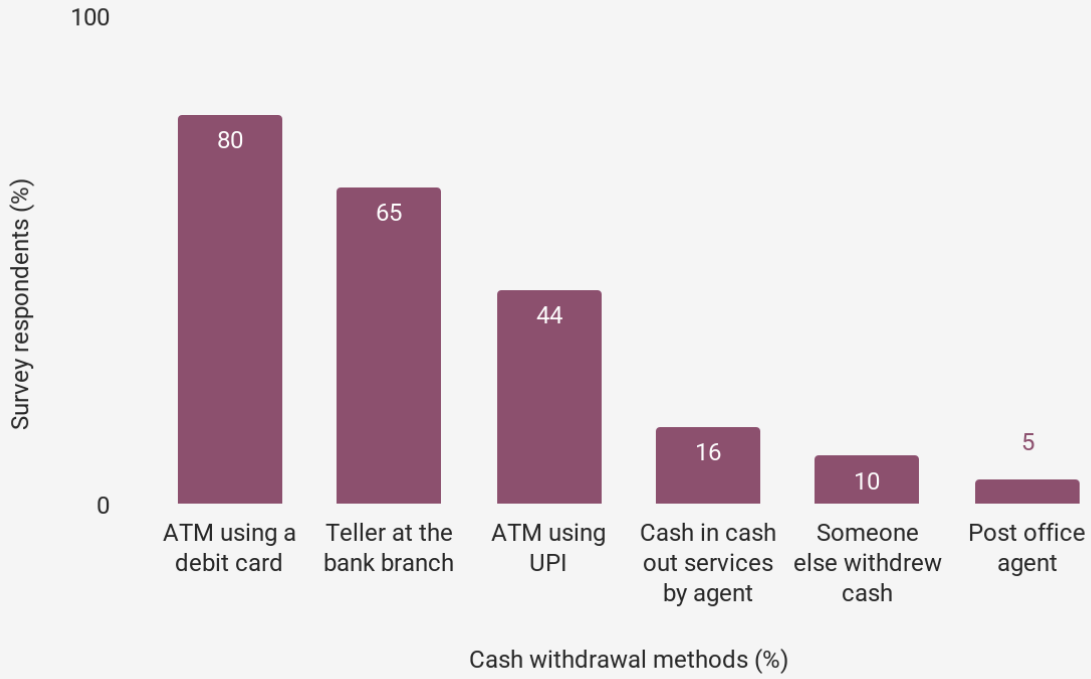
4.3.3. Accessing cash withdrawals through a range of physical and phygital services

Part of the network of banking infrastructure is the range of physical, phygital and digital points of service that offer consumers a range of options to conduct transactions like cash withdrawals. As **figure 4.7.** shows, visiting an ATM or bank branch for cash withdrawals was preferred over phygital services provided by banking agents/correspondents.

[142] An inter-bank (OFF-US) transaction is one where there is movement of funds from one bank to another necessitating an interbank settlement.
[143] "AePS 24-25 Product Statistics", *NPCI*, accessed November 2024, https://www.npci.org.in/what-we-do/aeps/product-statistics/2024-25
[144] "Operations and Performance of Commercial Banks", Reserve Bank of India, 26 December 2024, https://www.rbi.org.in/scripts/PublicationsView.aspx?id=23075

Figure 4.7. Only half as many respondents withdrew from an ATM using UPI as compared to a debit card.

Percentage of respondents by cash withdrawal methods (N = 3,784)



India lags behind when it comes to ATM penetration compared with other emerging markets, with the RBI reporting only 15 machines per 100,000 users in 2022.[145] The lack of physical infrastructure to support access to cash and banking services may also end up disincentivising cash and compel users to adapt to increasing digitalisation within this sector, even if they may otherwise prefer physical and phygital services. This shift towards digital transactions and a cashless economy has been stronger post demonetisation.[146] This is a difficult challenge to solve, since banks have not been able to keep up with targets for new branches in rural areas.[147] There may also be a slow shift away from ATM services due to operation costs, with a drop in ATM locations especially those not located alongside bank premises.[148]

[145] Saloni Shukla, "Digital payment's rise leads to shutting of ATMs", *Economic Times*, 7 November 2024, https://economictimes.indiatimes.com/industry/banking/finance/banking/digital-paymentss-rise-leads-to-shutting-of-atms/articleshow/115029507.cms?from=mdr

[146] C.P Chandrasekhar and Jayati Ghosh. "The Financialization of Finance? Demonetization and the Dubious Push to Cashlessness in India." Development and Change 49, no. 2 (March 2018): 420–36. https://doi.org/10.1111/dech.12369.

[147] "Role of ATMs in Financial Inclusion", ICRIER, 2024, https://worldtradescanner.com/Role_of_ATMs_in_Financial_Inclusion.pdf
Manoj Kumar, "Opening branches in rural India is a loss making venture for banks", *Firstpost*, 18 April 2018, https://www.firstpost.com/business/opening-branches-in-rural-india-is-a-loss-making-venture-for-banks-4437219.html

[148] Saloni Shukla, "Digital payment's rise leads to shutting of ATMs", *Economic Times*, 7 November 2024, https://economictimes.indiatimes.com/industry/banking/finance/banking/digital-paymentss-rise-leads-to-shutting-of-atms/articleshow/115029507.cms?from=mdr

A researcher expressed concern that this may lead to issues with cash availability in underbanked regions.

> ATM penetration has not grown in the country over the past 10 years, the digital push is behind this. The same level of availability of cash is not present in Tier 2 and 3 cities, where ATMs have not kept pace with growth.
>
> **— A digital payments researcher from a consumer collective, in an interview**

Researchers and community-based organisations we interviewed cautioned against the rapid push for digitalisation across services, and the techno-optimist view that it always leads to improved access and inclusivity. Such infrastructural decisions that reduce cash availability can force digitalisation on users who are ill-prepared for the shift, especially when other phygital alternatives like the banking correspondent network facilitating the AePS network are not preferred or reliable.[149]

Another issue that plagues ATM networks is the availability of accessible and inclusive interfaces.[150] While there are existing solutions to improve ATM accessibility for persons with visual impairments, such as talking ATMs,[151] these are not implemented across the network. This was highlighted in conversation with an interviewee with a visual impairment.

> At an ATM you have to depend on somebody to guide you through the process. Machine to machine, there are often variations. Now scrambled touchpads without tactile markings are common. These are inaccessible.
>
> Technology for talking ATMs is available, and rules have indicated that by 2018 machines should be all inclusive. Both my home and workplace are located in central urban locations,and there are many banks and ATMs but no talking ATMs. People need to be able to access this facility wherever they are, they shouldn't be concentrated next to the blind school.
>
> **— Social entrepreneur and disability rights activist with a visual impairment, in an interview**

[149] "Transaction failure rates in the Aadhaar enabled Payment System: Urgent issues for consideration and proposed solutions", Dvara Research, May 2020, https://dvararesearch.com/wp-content/uploads/2023/12/Transaction-failure-rates-in-the-Aadhaar-enabled-Payment-System-Urgent-issues-for-consideration-and-proposed-solutions.pdf

[150] Sudheesh Singanamalla, Venkatesh Potluri, Colin Scott, and Indrani Medhi-Thies, "PocketATM: understanding and improving ATM accessibility in India", *ICTD '19: Proceedings of the Tenth International Conference on Information and Communication Technologies and Development* (2019): 1-11, https://dl.acm.org/doi/10.1145/3287098.3287106

[151] 'Home', Talking Atms India, Xavier's Resource Center for the Visually Challenged (XRCVC), Mumbai. https://talkingatmindia.org/

4.3.4. Bank account ownership does not automatically translate into bank account usage

Access to banking services has remained uneven geographically and for vulnerable consumer groups, primarily due to gaps in banking infrastructure. We spoke with women who have been leading self-help group (SHG) activities, in their villages in Velhe and Khed Shivapur blocks in Maharashtra, to understand levels of access to banking services and their utility for rural women.

> We help people with getting their documents together to open their bank accounts at the co-operative bank which is closer. People sometimes also want help with getting their payments from government schemes directed to this account.
>
> **—Participant in a focus group discussion with SHG women in Velhe, Pune**

Being able to enroll for and ensure uninterrupted disbursal of direct benefit transfers under government schemes often acted as the primary incentive towards opening a bank account. While SHG members recognised other benefits of saving money in their bank accounts, these were difficult to realise for other women in their villages.

> Most people only visit the bank when they need to withdraw scheme money, but over time some have started seeing the benefits like security and being able to earn interest. But for most people the bank branch is too far for them to go alone, and they prefer to keep the money at home.
>
> **—Participant in a focus group discussion with SHG women in Velhe, Pune**

However, the list of challenges associated with regular banking transactions was longer. Since the nearest bank branch was generally located near the block development office, women had to take on significant transport costs for routine transactions. The number of banking personnel were often inadequate to service the volume of account holders, and general forms and deposit slips were not available in the local language used by most villagers. Such procedural and documentation barriers necessitated seeking support from trustworthy intermediaries like the SHG leaders to access offline banking services.

Accessing cash also involved a trip to the bank branch, because of lack of ATM machines, and inoperational AePS (Aadhaar enabled Payment System) services due to limited capacity of the banking correspondents servicing multiple villages spread over a large geographical area.

> No bank agent makes regular trips to our village. If we want to withdraw cash, we have to call a day in advance. He will not have the money otherwise. This service is also only provided by the post office workers. No one knows the number of the bank agent, or even knows who he is.
>
> **—Participant in a focus group discussion with SHG women in Velhe, Pune**

This disruption in services has discouraged regular cash deposits, beyond those made for savings, by women who rely on cash for day to day transactions. This will be discussed further in the following section.

According to the Findex 2021, 35% of bank account holders or 273 million people's accounts were dormant. This means they had not made any deposits or withdrawals over the past year.[152] Dormancy was observed in cases where proximity, convenience, and security of banking services were associated with a significant cost, time, or difficulty that became deterrents.[153, 154, 155]

While many barriers to traditional banking remain, many people need additional training and support to adapt to the digitalisation of financial services. As we heard from an interviewee, his organisation has had to shift gears when it comes to their digital literacy programmes, and bring in an increased focus on digital financial literacy.

> People are not equipped to adopt digital services, making these practices mandatory can lead to exclusions and a violation of human rights. The current environment necessitates participation in the digital ecosystem and creation of a personal digital footprint and having at least one family member who is digitally literate.
>
> About 5 years back, we weren't using financial inclusion based literacy and skilling, but now that has become a necessary ingredient of all our training and capacity building programs.
>
> **— Specialist on rural access to digital services in an interview**

In the next section, we will look at differences in the adoption of digital financial services, which can be affected by similar factors of convenience, accessibility and service quality.

---

[152] "The Global Findex Database 2021", *World Bank Group*, accessed November 2023, https://www.worldbank.org/en/publication/globalfindex/Data

[153] Suyash Rai, "Economic Development and Digital Transformation: Learning from the experience of Aadhaar and Financial Inclusion in India", *XKDR Forum Working Paper 35* (2024): https://xkdr.org/paper/economic-development-and-digital-transformation-learning-from-the-experience-of-aadhaar-and-financial-inclusion-in-india

[154] Microsave. "Account inactivity in India—is there a problem?", Microsave, 2023, https://www.microsave.net/wp-content/uploads/2023/05/Account-inactivity-in-India_Is-there-a-problem.pdf

[155] Microsave. "The real story of women's financial inclusion in India", Microsave, November 2019, https://www.microsave.net/wp-content/uploads/2020/01/191125_The-real-story-of-womens-financial-inclusion-in-India_Gender-research-report.pdf

4.4. Netbanking and digital payments

In this section we look at drivers and challenges in the adoption of net banking and UPI services, and how users who face language, digital access or literacy barriers navigate the need for support while using these services.

In our research, 65% of the respondents used netbanking.

- Fifty two percent of transgender persons and 60% of women used netbanking compared to 71% of men.
- Over 70% of those who earned an income over 18,000 INR used net banking services, compared to around 60% of users from all other income brackets.

User groups

- Around 55% of respondents who identified as gender and sexual minorities used netbanking.
- Around 47% of respondents with disabilities used netbanking.
- Age had an inverse relationship with net banking usage. Only around 47% of respondents above 45 years of age used netbanking compared to 75% of respondents between 18 to 30 years of age.

4.4.1. High need for support to facilitate netbanking

60% of surveyed netbanking users sought help to conduct online banking transactions.

Around 57% of those under 45 years of age sought help for netbanking. 55% of the men who used net banking needed support whereas 66% of the women and 61% of transgender respondents needed help. Over 73% of elderly respondents also reported needing help with netbanking.

One participant mentioned struggles with simple login procedures when registering for the online service. Lack of familiarity with digital interfaces, registration requirements and security features necessitated support when onboarding onto digital services.

> The YONO SBI app asked me to change the password. I didn't know how to do this, so my friend who was also using this app helped me. When they explained the steps and password requirements (characters, symbol, caps, etc), these technical requirements were new for me.
>
> —Participant in a focus group discussion with gender and sexual minorities in Chennai, Tamil Nadu

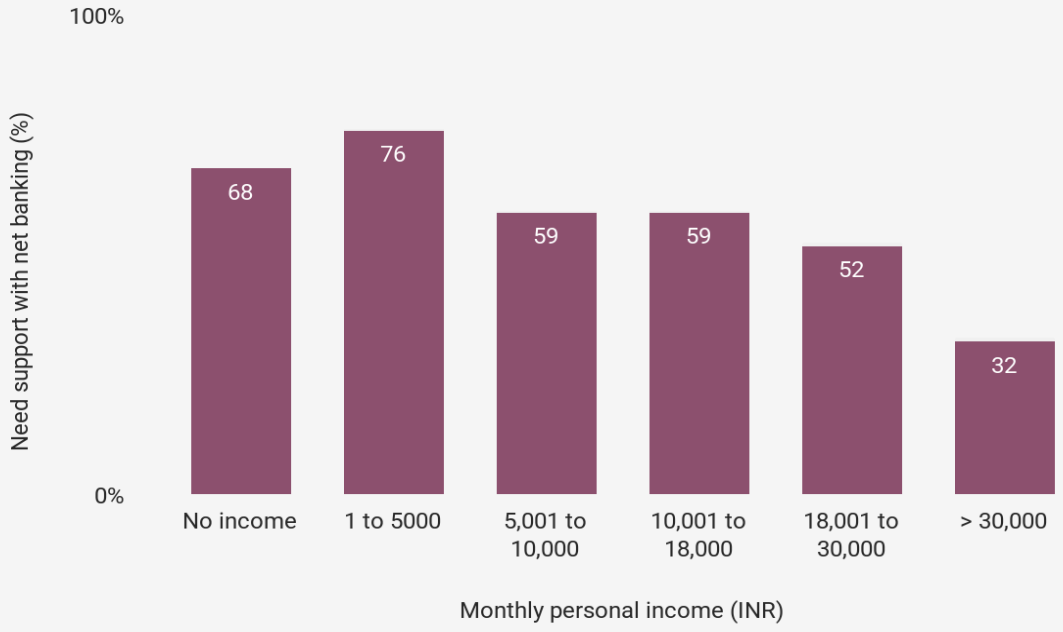
85% of respondents from Tamil Nadu shared that they needed support with net banking transactions. While many banking applications have begun offering multi-lingual services and support, this is often limited to a selected group of languages,[156] [157] with interfaces often first being developed in Hindi. Even for users who may have some comfort in mainstream languages, absence of adequate vocabulary for technical terms can create a challenge. It is worth investigating whether the limited availability of full-fledged translations in southern languages, and quality of translations on websites and mobile applications play a role in the high need for support. One example comes from a focus group participant:

> The app from my bank is not available in Tamil, so I have to sit with someone and they'll translate for me and guide me through the app.
>
> **—Tamil language speaker in a focus group discussion with gender and sexual minorities in Chennai, Tamil Nadu**

In our survey, respondents in lower income groups had a higher need for support for net banking as compared to other income groups. As **figure 4.8** suggests, 76% of respondents who had income less than or equal to INR 5,000 per month, shared that they needed support for netbanking.

Figure 4.8. A greater proportion of respondents who earn below INR 5,000 needed support with netbanking than other income groups

Percentage of netbanking users requiring support, by income range (N = 2,443)



Note: The chart reflects percentages for respondents who use netbanking

[156] BFSI Network, "Built for Bharat: FinTech startups nailing the multilingual game!", *BFSI Network*, 29 September 2022, https://bfsi.eletsonline.com/built-for-bharat-fintech-startups-nailing-the-multilingual-game/

[157] Sohini Mitter, "New mobile banking app supports 11 Indian languages and English", *Mashable*, 21 March 2017, https://mashable.com/article/india-largest-private-bank-multi-language-mobile-app

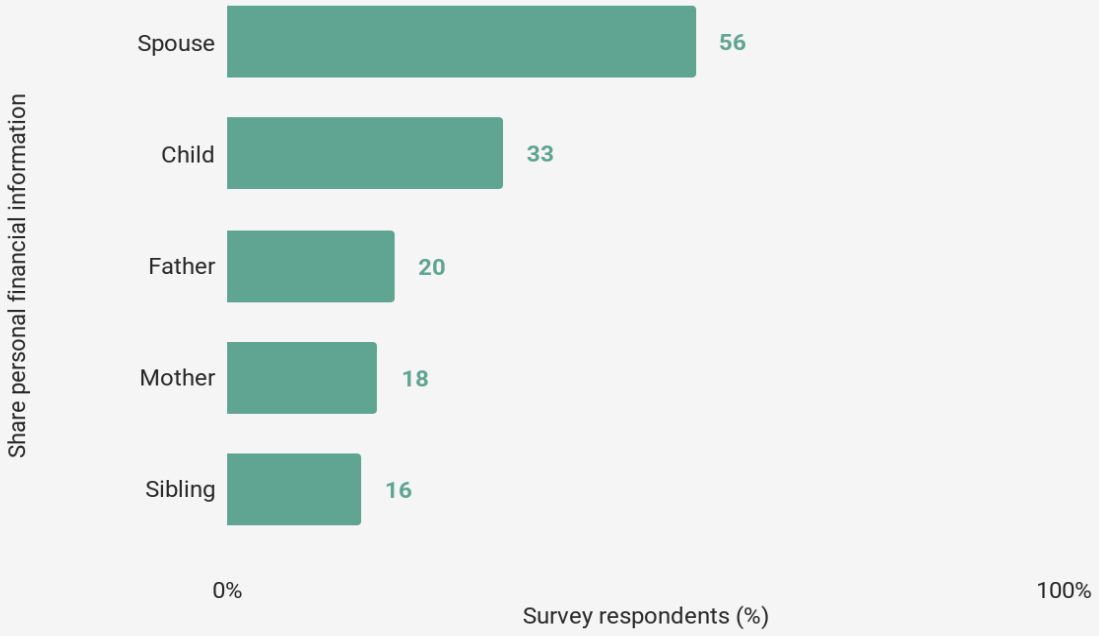
Sharing of personal financial information with others

Seeking support for online financial transactions may also require users to share account login and other information that compromises the privacy of their personal financial information, and provide others access to their money.[158]

As Figure 4.9 shows, 55% of users shared their banking information with family members giving them access to their accounts. Most respondents shared this information with family members.

Figure 4.9. Over half the respondents shared personal financial information such as bank account passwords or UPI pins with family members.

Percentage of survey respondents by who they share personal financial information with (N = 2086)



Note: The graph does not include others that respondents might share information with as they made up less than 5%

[158] Jaspreet Singh, Ritika Divekar, and Kaavya Arakoni. "Extending Trends in Savings and Digital Finance to Women's Economic Empowerment and Digital Savings: A Qualitative Study with Married Women in India ", Busara Center for Behavioral Economics, 28 November 2023, https://bigd.bracu.ac.bd/wp-content/uploads/2024/07/Working-Paper_Digital-Savings-and-Women-Empowerment.docx.pdf

- 63% of women shared personal financial information with family members, compared to 51% of men. Only 26% of transgender persons shared information with family members, indicating a lower level of support from familial networks.
- 70% of respondents over the age of 60 were sharing personal financial information.
- Respondents earning no income also shared this information at a higher rate of 68% when compared to respondents earning any income at all.
- 83% of unpaid workers employed within family businesses had shared financial information with their family members, as well as 70% of women in unpaid care work/ 'homemakers'.

84% of respondents mentioned that they shared personal financial information with others because of trust. Other reasons included the need to seek support in making good financial decisions (49%), social norms around information sharing (41% shared that financial information should be shared with family members), and the need to seek support to manage online financial accounts (20%).

4.4.2. High adoption of UPI platforms

Since the launch of UPI 2.0 in 2018, which allows users to connect their virtual payment address (VPA) directly to their bank account for digital transactions, the adoption of UPI has grown year on year, with an average of 16 billion transactions monthly in 2024. In the second half of 2024, UPI transactions accounted for 81% of digital payments across all digital payment systems.[159]

We surveyed people about the frequency of their UPI usage and ease of using UPI.

85%
of rural respondents used UPI compared to 91% of urban respondents

77%
of transgender persons used UPI compared to 86% of women, and 94% of men

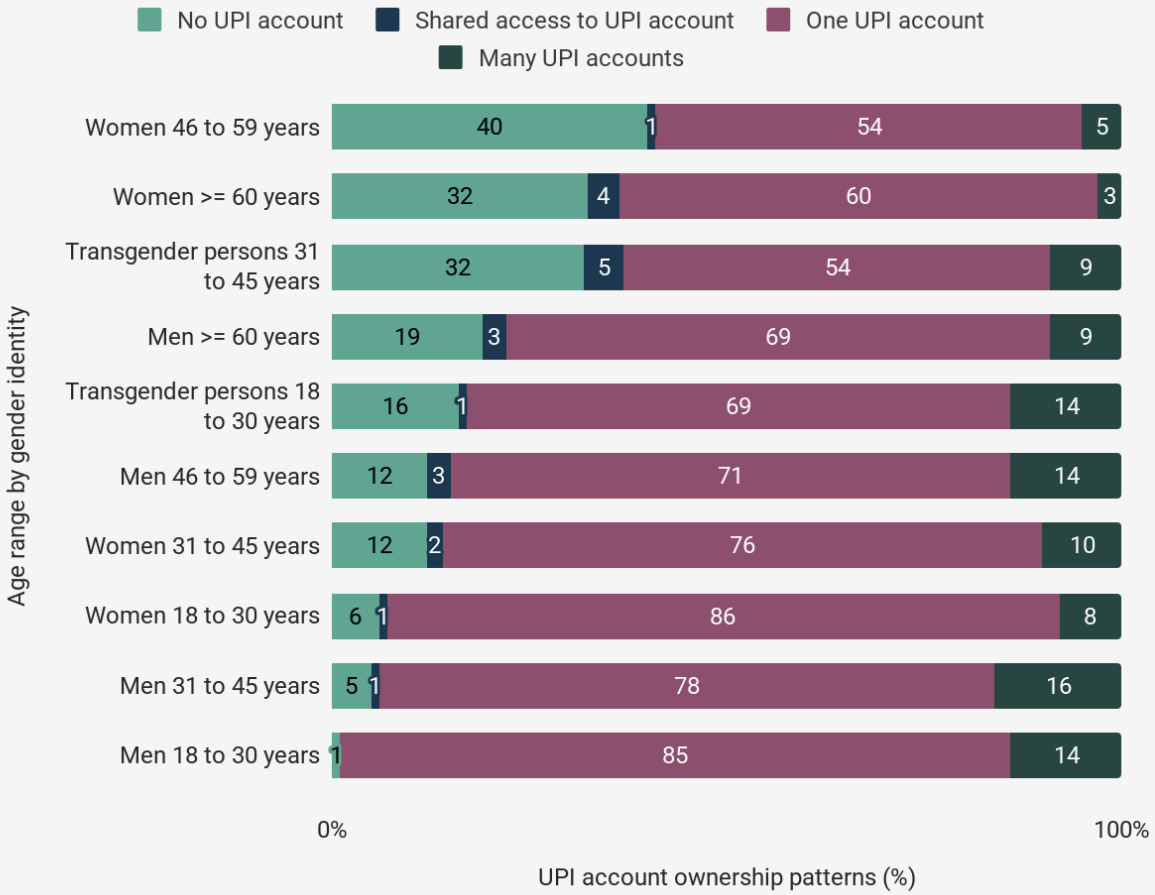
82%
of users were 45 years of age and under

[159] "Payment System Report", Reserve Bank of India, December 2024, https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=23127

As seen in **figure 4.10.**, gender and age were direct factors in determining UPI account ownership and usage.

Figure 4.10. Women and transgender persons over 45 years were less likely to have a UPI account

UPI account ownership patterns by age and gender identity (percentage of respondents, N = 3,784)



Note: Less than 1% of the respondents above 46 years were transgender persons and have therefore not been included as a category in this chart

We asked respondents to report frequency of use to understand UPI's utility for day to day transactions. While over 92% (3125 out of 3377) of the respondents reported frequent usage levels having used UPI at least once a week, only 56% of the respondents reported daily UPI usage.

Over 10% of women and transgender respondents fell in the category of infrequent users compared to only 5% of men.

13% of disabled respondents reported infrequent UPI use.

4.4.3. Various factors driving adoption of UPI

The proliferation of digital financial services (DFS), growing levels of smartphone usage, network effects in the high usage of digital public infrastructure and UPI, and policy mandates related to demonetisation have all played a part in increasing its usefulness for consumers.[160, 161, 162] Studies on consumers' adoption of UPI have also found that convenience, transaction speed, perception of security, innovation and trust also played a role.[163, 164] Improved accessibility for regional language users and interoperability have also simplified UPI usage for the everyday consumer in many ways as noted by a researcher in an interview.

> UPI and mobile penetration can facilitate various use cases, like migrant workers sending remittances, and increased access to e-commerce sellers.
>
> Smartphone based payments can also break down linguistic barriers, and allow people on both sides to conduct transactions in their own preferred language.
>
> **—A digital payments researcher, in an interview**

Getting people online was also driven by the uncertainty of this period, where people had to adapt rapidly to a changing economic scenario. Recalling the scurry during initial lockdowns in the wake of the COVID-19 pandemic, an interviewee told us:

> There was a lot of desperation during this time because of livelihood loss. There was no time or bandwidth to learn the risks of going online. You just migrated online if you needed the money.
>
> **— Lead at a cyber wellness and safety organisation, in an interview**

Since design and accessibility features vary from platform to platform, having a range of options can support consumers' variable needs when it comes to choosing a UPI platform. For one consumer with a visual impairment, finding built-in accessibility

---

[160] Fahad and Mohammad Shahid, "Exploring the determinants of adoption of Unified Payment Interface (UPI) in India: A study based on diffusion of innovation theory", *Digital Business* volume no. 2, issue no. 2 (2022): https://www.sciencedirect.com/science/article/pii/S2666954422000205

[161] Nidhi Singh, Neena Sinha and Nidhi Singh and Francisco J. Liébana-Cabanillas, "Determining factors in the adoption and recommendation of mobile wallet services in India: Analysis of the effect of innovativeness, stress to use and social influence", *International Journal of Information Management* volume no. 50, (2020): 191-205, https://www.sciencedirect.com/science/article/abs/pii/S0268401218310697

[162] Roopesh Kumar Shanmugasundaram. "Exploring the factors influencing Unified Payments Interface (UPI) adoption among senior citizens in India", University of Jyvaskyla, 2024, https://urn.fi/URN:NBN:fi:jyu-202406174709

[163] Ruchik Sunil More. "Understanding Factors Influencing UPI (Unified Payments Interface) user adoption levels and sentiments in India", NORMA eResearch @NCI Library, 9 August 2024, https://norma.ncirl.ie/7024/

[164] Piyush Kumar Mallik and Deepak Gupta, "A Study on Factors Influencing Consumer Intention to Use UPI-Based Payment Apps in Indian Perspective", *Information and Communication Technology for Intelligent Systems* ICTIS 2020 (2020): 445-452, https://link.springer.com/chapter/10.1007/978-981-15-7062-9_44

features was a process of trial and error. This has allowed him to be able to conduct financial transactions with much more independence and convenience.

> There is a lack of consistency across UPI platforms when it comes to accessibility. I have similar issues with banking apps. Sometimes I can make payments, but it is difficult for me to verify whether a payment has come.
>
> However, Google Pay's inbuilt screen reader has been consistently accessible and helped reduce mistakes. Everytime I swipe I am told what I am swiping on. When I am sending money using a phone number, it reads out the name and helps verify each step. Compare this to working with the soft copy of my bank statement. I have to pass through serial numbers and irrelevant information line by line with my screen reader. I handover all these statements to my accountant and am dependent entirely on him.
>
> **—Social entrepreneur and disability activist with a visual impairment, in an interview**

4.4.4. Challenges faced during UPI usage

In our survey, 64% of respondents who use UPI faced challenges. Users experienced challenges with both onboarding onto UPI platforms, unexpected lapses in account functionality, customer services as well as with conducting P2P (person-to-person) and P2M (person-to-merchant) transactions (see **figure 4.11.**).

Figure 4.11. Failed transactions were the biggest challenge for UPI users

Percentage of respondents who faced issues in using UPI [N = 2,159]

Registering and onboarding	Lapses in account functionality	Failed transactions	Customer service
5% experienced difficulty completing their digital identity verification.	**13%** had their UPI accounts frozen at least once.	**90%** experienced failed transactions.	**11%** experienced lack of customer support.
	9% could not carry out UPI transactions because their bank account was frozen.	**38%** experienced delayed refund for failed transactions.	
		11% experienced incorrect amounts being deducted from their UPI account.	

Note: This table reflects percentage of challenges in using UPI only among those reported facing challenges

One participant in a focus group discussion shared an instance where money was deducted from their account without showing up in the other person's account.

> I was unable to go to the bank immediately to check what the issue was, and this became quite a stressful experience. If transactions are not recorded, and you lose money it can be a stressful experience when you have no access to any explanation or support.
>
> **— Participant in a focus group discussion with gender and sexual minorities in Chennai, tamil Nadu**

Women and gender and sexual minorities, specifically shared their **fear of misdirected payments due to both platform or personal error.** The swiftness of UPI payments, and lack of simplicity in process to dispute or reverse payments was seen to compound this risk by many participants.

> My neighbour had to send the shopkeeper just 12 rupees. I am not sure how this happened but 4,500 rupees somehow went to the wrong account. She tried again, and the 12 rupees ended up going to this account again. When I hear of instances like this, then I have to wonder if I should use it or not, this fear gets built up.
>
> **—Participant in a focus group discussion with elderly SHG women in Khed Shivapur, Pune**

Most were unaware of in-app menus to raise issues and reverse payments and would try to work with the recipient directly instead.

> I was trying to send money to my friend, and the money went to a customer instead. He pretended to have never received the money, and then kept making excuses for three days. He sent me the money only after I told him I would go to the police.
>
> **—Transgender sex worker in a focus group discussion with gender and sexual minorities in Chennai, Tamil Nadu**

For some the lack of comfort and familiarity with digital interfaces, the risk associated with using digital financial services was compounded by negative consequences they may face at home if the money is not easily recovered. This also acted as a deterrent to adopting digital financial services.

4.5. Challenges that limit the use of digital financial services

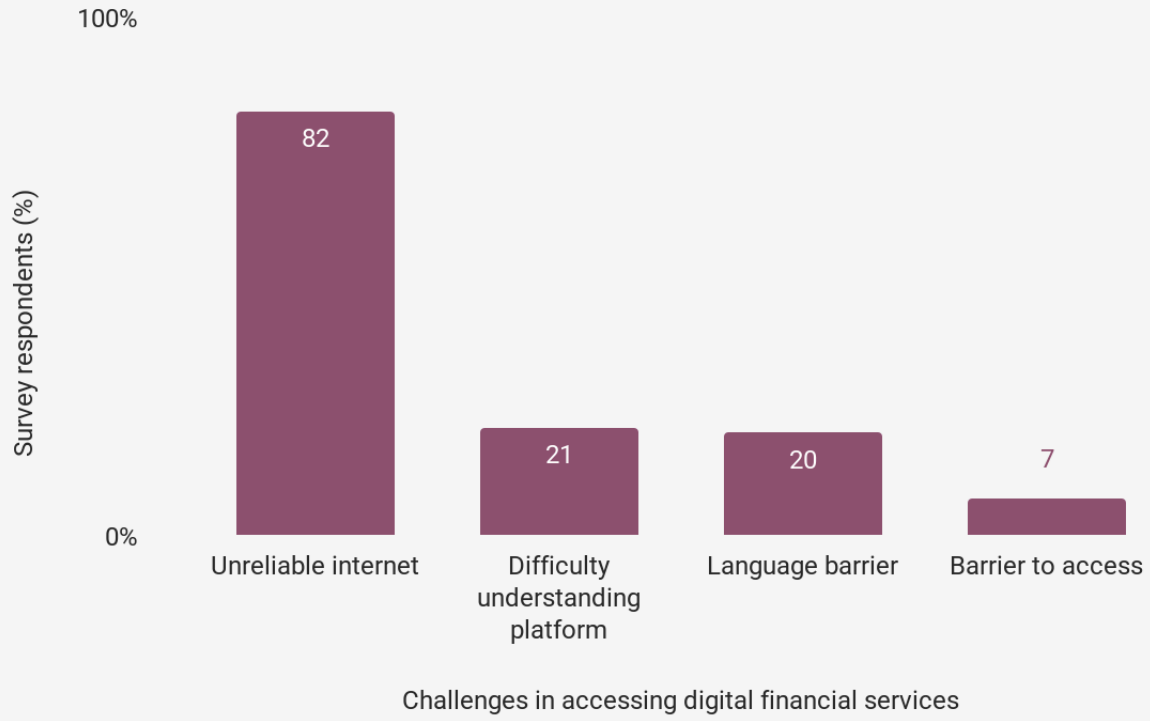
Financial inclusion through digital services has been marred by the lack of affordability, connectivity and limited access to personal devices.

Around 64% of respondents in our survey reported facing some challenges when accessing financial services online, via mobile applications or websites.

Figure 4.12. details these challenges, including connectivity issues and language barriers.

Figure 4.12. Unreliable internet, limited accessibility and navigation features were barriers to accessing digital financial services

Percentage of respondents who faced different challenges in accessing digital financial services [N = 2,437]



4.5.1. Issues with internet infrastructure

Internet infrastructure issues relate to experiencing problems while completing online financial transactions, due to the internet connection being weak or unreliable. This was one of the most common issues people faced while using digital financial services.

Low internet penetration can impact the uptake of digital financial services, and even act as a deterrent. A woman in her 30s, who leads her village's self-help group (SHG) told us:

> I have to walk to the road to get a reliable phone signal, and even that is not a sure shot. It (connectivity) is better here when I am at the centre. Other women in my village mostly work within the village and don't travel much outside. I don't know if they use the internet at all, using UPI is much further.
>
> **– Participants (SHG group members) in a focus group discussion with SHG women from Velhe, Pune**

Similar issues with internet connectivity can also lead to transaction failures over the AePS network, when the operation of the microATM or ePOS device used to facilitate transactions is impacted.[165]

Of the 79% of respondents who experienced issues with cash withdrawal, 65% of them had faced issues with internet connection.

4.5.2. Challenges in migrating to digital-first services

The move to digital interfaces is challenging for many user groups. Financial services still cater to those who already have a level of digital literacy and access. These platforms have not been designed to serve people at the last mile. While tech solutions are attractive for platforms given the large population, they may not allow everyone to participate effectively or feel their benefits, a participant observed in one of our focus group discussions.

> There are lots of issues with online transactions. If there are ten benefits then there are ten disadvantages as well. People keep asking everything to be online but how can those people who aren't as educated do things online?
>
> **—Participant in a focus group discussion with gender and sexual minorities in Chennai, Tamil Nadu**

In practice this means that the digital journey is not purely digital for many users, who require some level of support when onboarding to get them started, or continually for others, as an interviewee leading digital inclusion programmes explained.

> While we are talking about digital empowerment, these platforms are still not created to be user friendly for people at the last mile. There is a high preference for handholding among low-income customers; this isn't a purely digital journey for them.
>
> **—Digital financial inclusion specialist, in an interview**

[165] Ajay Ramanathan, "Multiple challenges plague AePS; lack of infrastructure and security risks, resulting in stalling of progress, say experts", *Financial Express*, 17 July 2023, https://www.financialexpress.com/money/aadhaar-card-multiple-challenges-plague-aeps-lack-of-infrastructure-and-security-risks-resulting-in-stalling-of-progress-say-experts-3173221/

Elderly users often have a preference for in person interaction when using financial services. The shift to digital has necessitated rapid adaptation for users who need to build familiarity and comfort with digital systems from scratch. An interviewee shared what she learned when helping older users build digital literacy during the pandemic,

> If you want to universalise something, you need to keep the last mile in mind. A lot of people can use these systems if they know how to, not everyone does. Digital functions in different ways, things like anonymity, working with machines only scare people who are used to primary human contact, it's not organic to them.
>
> **—Policy lead at a NGO working on issues tied to ageing, in an interview**

The **burden of proving identity is already much greater for transgender users.** Having limited comfort with digital interfaces and limited proficiency in English, might make registering for services difficult for transgender people. A community worker, who works with transgender community members in Karnataka and Telangana, has noticed:

> Filling out online forms and applications is something people need support with when they lack comfort with digital interfaces. This issue is exacerbated by the lack of availability of digital services and their platforms in regional languages. Even when platforms are made available in regional languages, the support lags and accessing some functions and information may still require knowledge of English.
>
> **— Project staff at a CSO working with gender and sexual minorities**

Even when the main or initial sections are available in multiple languages, key information is inaccessible or translated poorly. A 2019 study conducted by the Centre for Internet and Society found that privacy policies provided by most fintech platforms lacked clarity and readability, and in most cases were only made available in English.[166] A participant in a focus group discussion shared similar problems while trying to navigate her bank's net banking platform that only provided partial access in her preferred language.

> The language we use when we speak is of one type and the one that is technical is different. I navigate the app in English, but then the statement, saving books come in English. Some of it I don't understand, and it confuses me. When I am unable to understand, I forego making the transaction online.
>
> **—Participant in a focus group discussion with gender and sexual minorities in Chennai, Tamil Nadu**

[166] Aayush Rathi and Shweta Mohandas. "FinTech in India: A study of privacy and security commitments", Centre for Internet and Society, April 2019, https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf.

Some of these issues also stem from legacy challenges to language accessibility on the internet.

> There is a long road to building true inclusion for regional language users. There is a general assumption in app design that the user of digital services can read English. I have not seen any privacy pages actually translated. Many apps still don't adequately support regional languages. A simple example is UPI where the interface is available in regional languages. However, the transaction node, its record is still maintained in ASCII so remains in English.
>
> **—Cyber security engineer with experience working on a payment gateway, in an interview**

5.

Beneficiary experiences with digitalisation and social protection

Direct Benefit Transfer's (DBT) infrastructural and institutional interlinkages span the non-digital and the digital. These include the vast institutional set-up of social protection at central and state levels, digitalised government service access points, banking and financial infrastructures, internet infrastructures, and NPCI-and Aadhaar-linked Aadhaar Payment Bridge System (APBS) and Aadhaar enabled Payment System (AePS).

This chapter looks at the types of DBT schemes that beneficiaries in this research accessed, followed by specific focus on certain risks and challenges faced by certain vulnerable groups, at stages of DBT enrolment, payments and settlements, and withdrawal.

5.1. Types of DBT schemes and profiles of DBT beneficiaries

DBT beneficiaries in our survey were enrolled in various schemes spanning LPG cash transfer schemes, pensions, scholarships, and state-sponsored targeted schemes. Across groups, persons with no or low income, elderly persons, and women were more

likely to be DBT beneficiaries. The distribution of schemes and beneficiaries also depended, in part, on the social protection priorities and allocations of central and state governments. In line with this, DBT beneficiaries in our survey were relatively more socio-economically vulnerable in comparison with non-beneficiaries. We also found that, while substantial, digital and internet access and use among DBT beneficiaries was relatively lower than non-beneficiaries.

5.1.1. Socio-economic-digital profiles of DBT beneficiaries in our survey

DBT beneficiaries in our survey were considerably economically vulnerable. As we see in **figure 5.1**., 46% of respondents earned between 1 to Rs. 5,000 per month and 34% of respondents had no income. This finding follows broader patterns of DBT coverage, where a majority of DBT schemes are targeted or means-tested with income and other socio-economic factors forming crucial elements of scheme eligibility criteria determined by central or state governments. In our survey, 34% of Scheduled Tribe respondents and 33% of Other Backward Caste respondents received DBT. In addition, as we see in **figure 5.2.** and **figure 5.3**., a higher proportion of elderly persons received DBT among respondents across age groups; and a higher proportion of women received DBT among respondents across gender identity.

Figure 5.1. A higher proportion of respondents earning under INR 5,000 received DBT

Percentage of respondents who received DBT by income range (N = 3,784)

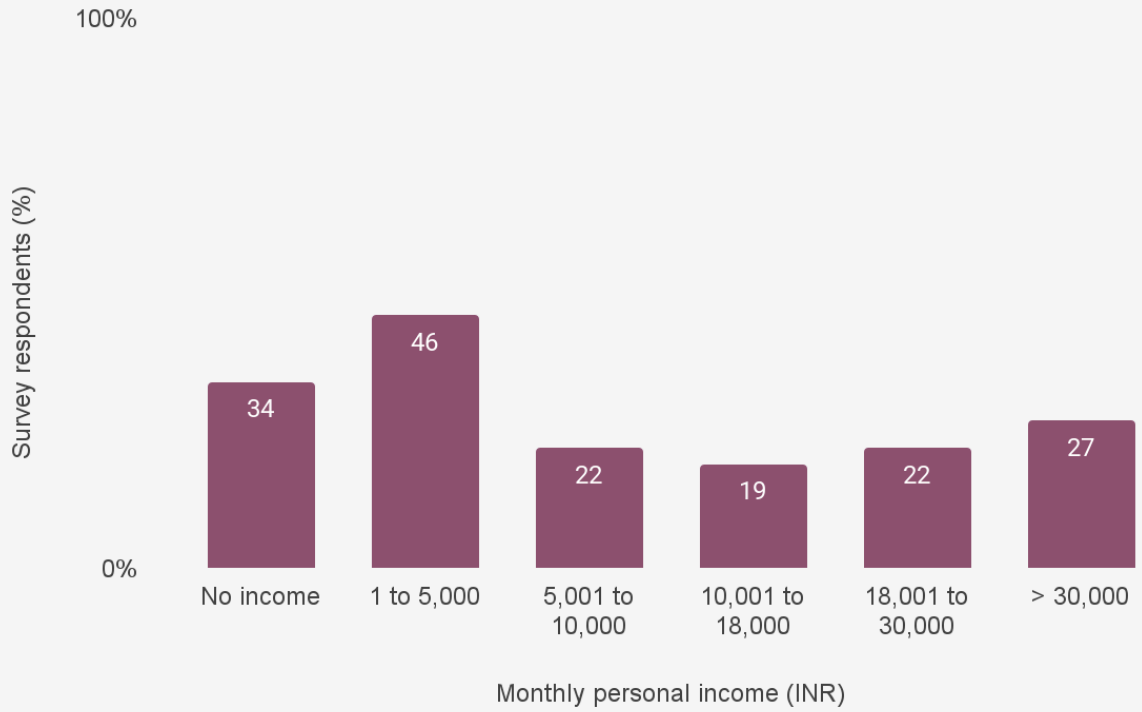


Figure 5.2. More than half of respondents over sixty years received DBT

Percentage of respondents who received DBT by age range (N = 3,784)

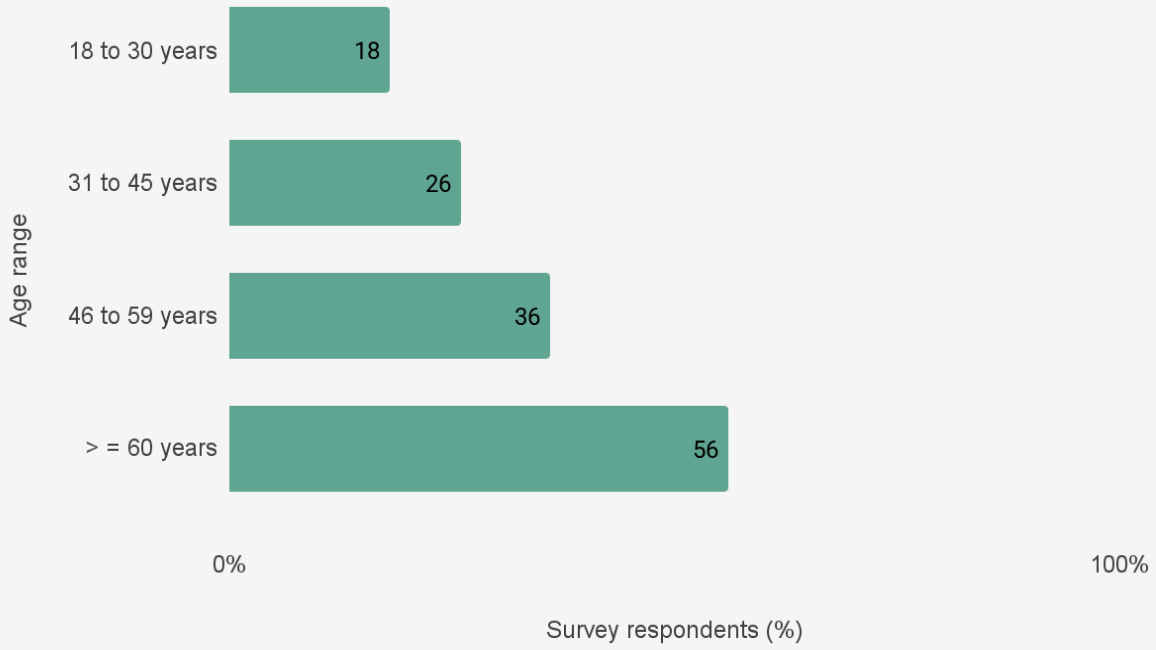
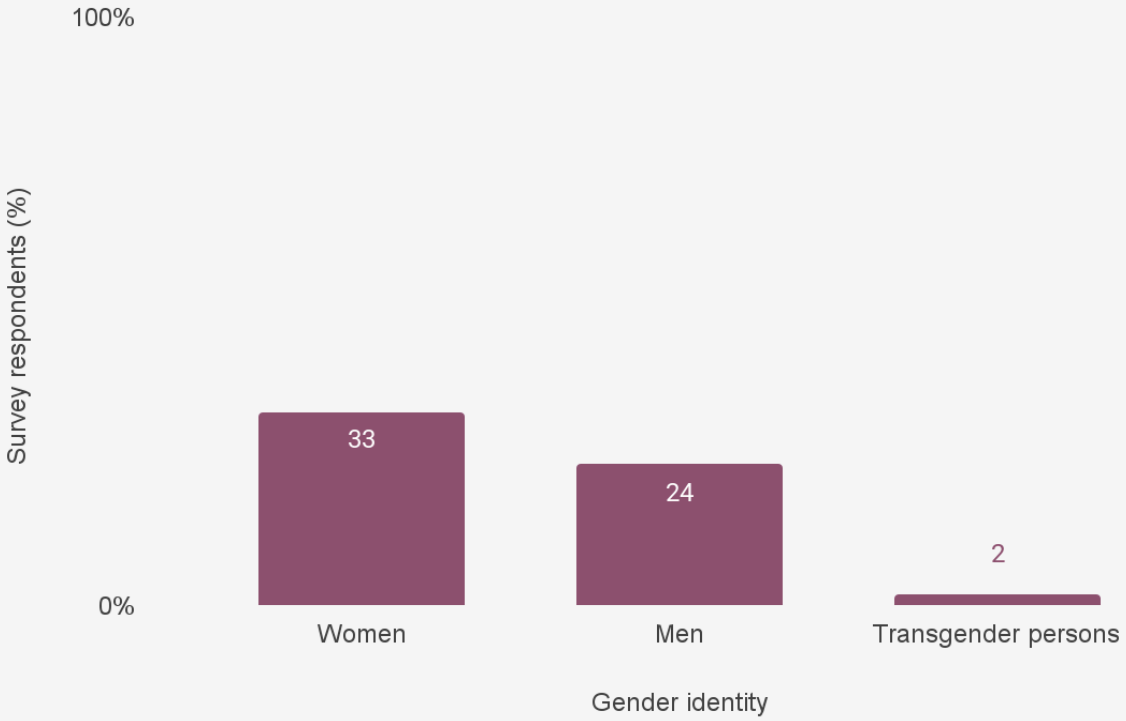


Figure 5.3. A higher proportion of women received DBT

Percentage of respondents who received DBT, by gender identity (N = 3,784)



Note: The higher representation of women is partly due to state-sponsored schemes that target women as eligible beneficiaries

Digital access and usage patterns of the DBT beneficiaries in our research shows that a majority of them were concurrently using other digital financial services such as net banking and UPI, and were frequent users of the internet.

Our survey also suggests that DBT beneficiaries had a higher incidence of shared use of digital devices. In addition, DBT beneficiaries comprised a relatively greater proportion of participants who had never used the internet, in comparison with all participants in our survey.

DBT beneficiaries in our survey (1,012 out of 3,784) ...

... had a higher proportion of persons who personally owned basic phones, and also shared them with family and friend
(6%)

... had a higher proportion of persons who personally owned smartphones, and shared them with family and friends
(33%)

... had a higher proportion of persons who never used the internet
(8%)

The socio-economic conditions of DBT beneficiaries in our survey and in secondary research show they already face vulnerabilities along income and literacy levels.[167, 168, 169] In addition, our survey shows that although digital device access and internet use of DBT beneficiaries is substantial, it remains relatively lower than what is observed for all survey respondents. This indicates further gaps that remain around accessing digital devices and services.

Amid these social, economic, and digital vulnerabilities, beneficiaries belonging to marginalised groups including elderly persons, transgender persons, persons identifying as gender and sexual minorities, persons with disabilities, women, regional language-first users, persons facing digital and economic vulnerabilities, and low-wage informal workers are at disproportionately higher risks of exclusion at multiple

[167] LibTech India. 'Length of the Last Mile: Delays and Hurdles in NREGA Wage Payments'. LibTech India, November 2020. https://libtech.in/wp-content/uploads/2020/11/LastMile_ReportLayout_vfinal.pdf.
[168] Sameet Panda. 'Data Systems in Welfare: Impact of the JAM Trinity on Pension & PDS in Odisha during COVID-19'. Centre for Internet and Society, 21 February 2021. https://cis-india.org/raw/sameet-panda-jam-trinity-pension-pds-odisha-covid-19.
[169] Sameet Panda. 'Digital Delivery and Data System for Farmer Income Support'. Centre for Internet and Society, 18 October 2023. https://cis-india.org/internet-governance/blog/cis-privacy-international-digital-delivery-and-data-system-for-farmer-income-support.

levels—DBT enrolment, payments and settlements, and withdrawal. We will map these compounded risks and harms in the sections that follow.

5.1.2. Scheme types across DBT beneficiaries in our survey

In our survey, out of 3,784 respondents...

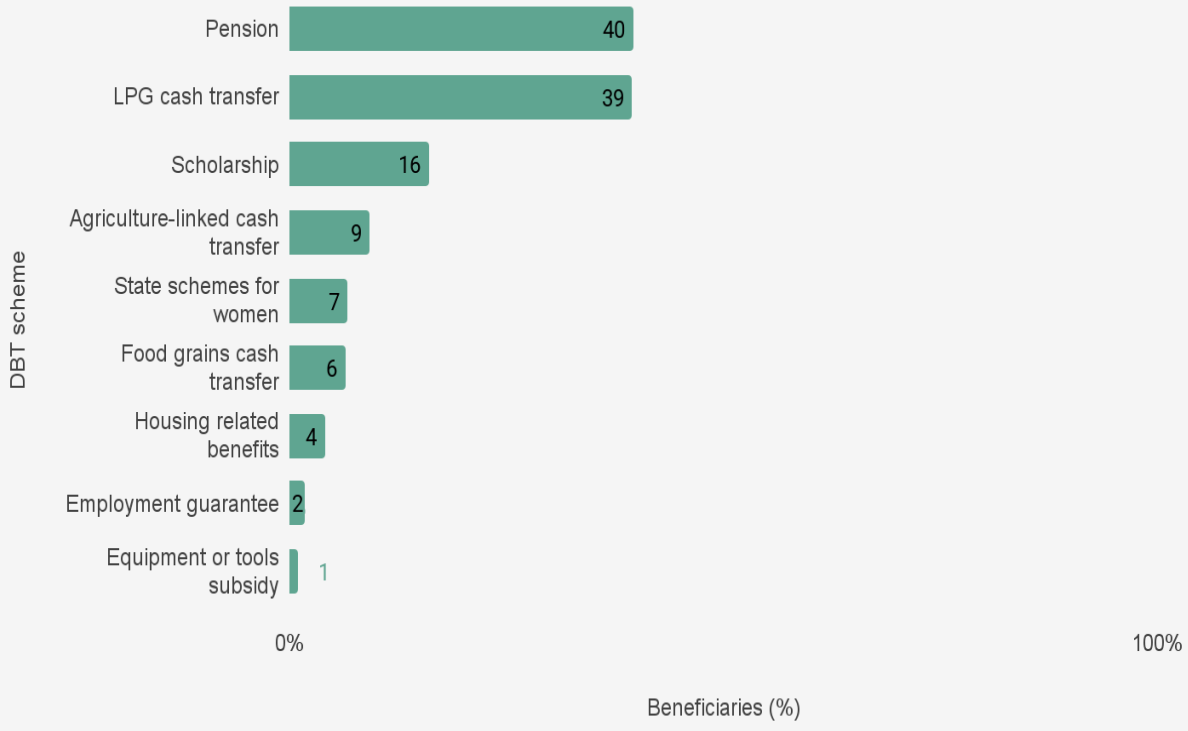
27%
of all respondents were enrolled under one or more DBT schemes. Of them, 60% resided in urban areas, and 57% identified as women.

56%
of elderly persons and persons with disabilities each were enrolled under DBT schemes.

Only 2.5%
of persons identifying as gender and sexual minorities were enrolled.

Figure 5.4. Around 40% of beneficiaries received LPG cash transfers and pensions

Percentage of respondents who received DBT, by DBT scheme N = 1,012



As seen in **figure 5.4.**, pensions and LPG cash transfers were the most common DBT schemes across all beneficiaries. A majority of beneficiaries, across specific user groups, received LPG cash transfers (see **figure 5.5.**).

Figure 5.5. Beneficiaries across specified user groups in our study received LPG cash transfer

Cash transfer schemes as accessed by user groups in the survey

Elderly persons (N = 249)	Person with disabilities (N = 127)	Women (N = 580)
LPG cash transfer **(29%)**	LPG cash transfer **(25%)**	LPG cash transfer **(42%)**
Agriculture-linked cash transfer **(8%)**	Pension **(25%)**	Scholarship **(16%)**
Food grains cash transfer[170] **(7%)**	Scholarship **(6%)**	State-sponsored targeted cash transfer **(11%)**

A percentage of women respondents were enrolled under various state-specific DBT schemes that specifically targeted women beneficiaries. Some of these schemes did not have an explicit income cap (Lakshmir Bhandar in West Bengal),[171] whereas others included an income cap as one of the eligibility criteria (such as Orunodoi in Assam[172] and Kalaignar Magalir Urimai Thogai in Tamil Nadu).[173] 11% of women beneficiaries in our survey were enrolled under these schemes. One such scheme, Lakshmir Bhandar, a cash assistance programme for women between 25 and 60 years residing in rural or urban West Bengal, offers tiered benefit amounts defined for each caste category.[174, 175] Although the scheme does not have an explicit income eligibility cap, women who are employed by the government or those who draw pensions are ineligible.

[170] This refers to the Anna Bhagya scheme introduced by the Karnataka government. At the time of writing this report, this scheme is to be discontinued: TNM Staff, 'Karnataka to Provide 10 Kg Rice Instead of Cash under Anna Bhagya Scheme'. *The News Minute*, 20 February 2025. https://www.thenewsminute.com/karnataka/karnataka-to-provide-10-kg-rice-instead-of-cash-under-anna-bhagya-scheme.

[171] Government of West Bengal. 'Lakshmir Bhandar | Government of West Bengal'. Accessed 5 April 2025. https://socialsecurity.wb.gov.in/login.

[172] Government of Assam. 'Assam Orunodoi Scheme | Assam State Portal'. Accessed 5 April 2025. https://assam.gov.in/scheme-page/154.

[173] Government of Tamil Nadu. 'Kalaingar Magalir Urimai Thogai, Tamil Nadu'. Accessed 5 April 2025. https://kmut.tn.gov.in/.

[174] Dipawali Mitra. '85.6% Women Surveyed Think State's Lakshmir Bhandar Scheme Empowered Them'. *The Times of India*, 22 May 2024. https://timesofindia.indiatimes.com/city/kolkata/85-6-women-surveyed-think-states-lakshmir-bhandar-empowered-them/articleshow/110319581.cms.

[175] Dwaipayan Ghosh and Debashis Konar. 'Lakshmir Bhandar to Include Additional 5L Women Says CM'. *The Times of India*, 22 November 2024. https://timesofindia.indiatimes.com/city/kolkata/west-bengal-expands-lakshmir-bhandar-scheme-to-include-5-lakh-more-women/articleshow/115540886.cms.

5.2. DBT enrolment: Digital identity and mobile linkages drive risks of exclusion

The reliance on Aadhaar (including biometric authentication and Aadhaar-linked identity documentation), and mobile phone linkages as the cornerstone of DBT enrolment and verification processes brings particular risks of exclusion for vulnerable groups.

As we see in the sections that follow, the increased reliance on digitalisation in enrolment processes does not match social realities of certain eligible beneficiary groups, particularly those who face varying marginalities.

As we see from experiences with gender and sexual minorities and persons with disabilities, eligible beneficiaries may be included within DBT at high cost to their personal safety, and after undergoing cumbersome processes. As we also see with experiences of eligible women beneficiaries, those who do not have the digital resources to shift to digitally-reliant systems may end up being excluded from DBT altogether.

5.2.1. Gender and sexual minorities and persons with disabilities expressed challenges in obtaining digital identity documentation

As we found in our research, documentation burdens are gendered, owing to cis-hetero-patriarchal norms that tie women's name and identity to marriage, which are further reflected in typical formats of official documentation. Women are required to undergo several cycles of identity verification: post-marriage, and in cases of separation, divorce, or widowhood.[176] Identity verification in these cases involve updates to identity documents to match their new marital status, and change in the status of familial ties. In the context of documentation requirements for DBT, each cycle of verification necessitates a change in identity documentation in order to remain eligible for benefits.[177]

A participant in our focus group discussion with SHG women in Velhe, Pune, has been a community support person working with married women in helping them change their documents to ensure that they do not face a stoppage of government benefits or services.

The participant supported women at her SHG in providing information on necessary documentation and procedures for changing their name for their Aadhaar and bank accounts. However, she also spoke of how these processes may be challenging when women have not changed their documents for several years after marriage:

[176] V. Kalyan Shankar, Ira Deulgaonkar, and Rohini Sahni. 'A Functional Typology of Exclusions: Why and How Women Fail to Access Government Schemes in India?' *Oxford Development Studies* 52, no. 3 (2 July 2024): 297–309. https://doi.org/10.1080/13600818.2024.2418382.
[177] ibid.

> There was one case where I helped a woman who had been married for 15 years but did not have appropriate documents. I have to first help her get a marriage certificate. The purohit who got them married had also passed away, so this was a challenging case. [...] One woman had been married for 20 years, but still wasn't even on the family ration card.
>
> **—Participant in a focus group discussion with SHG group members in Velhe, Pune**

As seen in chapter 4, persons identifying as gender and sexual minorities and transgender persons also face risks of being excluded from DBT schemes due to lack of documentation or issues with updating documentation. Our interview with the programme lead and programme staff at a community organisation working with gender and sexual minorities revealed that people from the community are unable to update Aadhaar and other identification documents due to risks of outing and to personal safety in the KYC process. Transgender persons face identity documentation barriers when accessing and using digital and financial infrastructures. These and other systemic barriers have resulted in compounded risks for exclusion from DBT for transgender persons.[178, 179]

Persons with disabilities are required to obtain separate digital identity documentation to "prove" eligibility for social protection such as disability pensions—the Unique Disability ID (UDID). The UDID was introduced in 2016 with the intended aim of streamlining the process for issuing disability certificates, along with a new universal digital ID through the UDID card.[180] This has meant that persons with disabilities must be registered under the new digitalised UDID system. In cases where persons with disabilities already have disability certificates, they may still have to undergo reassessment at the sole discretion of the medical authority or hospital. Moreover, if persons with disabilities have temporary UDID cards, they will be required to apply for renewals at regular intervals.[181]

Participants in our FGD with persons with disabilities described the function of the UDID in disability pension schemes:

---

[178] Priyanka Tupe. 'Transgender Women Are Being Excluded From Maharashtra's Cash Scheme For Women'. *BehanBox*, 29 August 2024. https://behanbox.com/2024/08/29/transgender-women-are-being-excluded-from-maharashtras-cash-scheme-for-women/.

[179] Eisha Hussain. 'India's New Transgender Portal Is Caught In Red Tape, Apathy and Bias'. *BehanBox*, 30 March 2022. https://behanbox.com/2022/03/30/indias-new-transgender-portal-is-caught-in-red-tape-apathy-and-bias/.

[180] Press Information Bureau. '100 Days of Modi 3.0: Empowering Lives: India's Dedication to Social Welfare Initiatives', 23 September 2024. http://pib.gov.in/PressNoteDetails.aspx?NoteId=152175.

[181] Department of Empowerment of Persons with Disabilities, and Ministry of Social Justice & Empowerment. 'UDID | FAQs'. Accessed 5 April 2025. https://www.swavlambancard.gov.in/faqs

> For disability pensions, we need the Unique Disability ID Card. This is only for persons with disabilities. They will mention the type and percentage of disability on the card. If a person has a hearing impairment they will mention that in the ID, and also mention that this person has this much percentage of hearing loss. If it is determined by the government (through medical evaluations) that a person has less than 40% disability, then they receive a lower amount of pension, and above 40% they receive the full amount.
>
> **—Participant in a focus group discussion with persons with disabilities in Bengaluru, Karnataka**

Experiences of persons with disabilities through ground reports show that they still have to contend with cumbersome processes, with new barriers and delays emerging from the introduction of the UDID system. These barriers include a new requirement of mandatory Aadhaar, a digitalised registration process plagued by issues of frequent server downtime and technical glitches, and the continuation of medical evaluation processes that are rife with violence and discrimination against persons with disabilities.[182, 183, 184, 185, 186] UDID has also been made mandatory to avail benefits, despite there being a high backlog and prolonged waiting period to receive UDID cards.[187]

A central test to "prove" eligibility through the UDID process for persons with disabilities that FGD participants mentioned is medical evaluations that determine the percentage of disability, and consequently, the amount of pension that a beneficiary is eligible for. Participants in our FGD with persons with disabilities further elaborated how they are sometimes charged by the government hospitals in order to receive their medical evaluations, despite no such fees having been notified by the government[188]:

---

[182] Shreya Raman. 'Tangled In Red Tape, The Disability ID Card Process Is Steeped With Gender Barriers'. *BehanBox*, 10 February 2022. https://behanbox.com/2022/02/10/tangled-in-red-tape-the-disability-id-card-process-is-steeped-with-gender-barriers/.

[183] Ibid.

[184] Shivraj Sanas. 'Disabled Individuals Face Hurdles in Obtaining Mandatory UDID Cards'. *The Bridge Chronicle*, 26 July 2024. https://www.thebridgechronicle.com/news/disabled-individuals-face-hurdles-in-obtaining-mandatory-udid-cards.

[185] Nisha Nambiar. 'State Brings Technical Snags on UDID Portal to Centre's Attention'. *The Times of India*, 2 August 2024. https://timesofindia.indiatimes.com/city/pune/maharashtra-disability-commissioner-writes-to-centre-about-technical-issues-on-udid-portal/articleshow/112208408.cms.

[186] Transgender persons are similarly required to obtain digital identity documentation to "prove" eligibility for DBT schemes. Prior research has shown that processes to obtain the Transgender Certificate and Identity Card" are arbitrary and harmful. For more on these risks and harms, see here and here.

[187] Vrinda Tulsian. 'House Panel Flags Issues with UDID Card for Persons with Disabilities'. *Hindustan Times*, 18 March 2025. https://www.hindustantimes.com/india-news/house-panel-flags-issues-with-udid-card-for-persons-with-disabilities-101742269708653.html.

[188] Ministry of Social Justice & Empowerment, Government of India. *The Rights of Persons with Disabilities (Amendment) Rules, 2024*. https://depwd.gov.in/the-rights-of-persons-with-disabilities-amendment-rules-2024/.

> To get the certificate and ID we have to go to the government hospital. They conduct a medical evaluation and sometimes ask money about INR 500-1,000. For many people, they'll have to think twice before paying this amount. Then while going for renewal [of the UDID card], the people there again ask for money about INR 400-500.
>
> **— Participant in a focus group discussion with persons with disabilities in Bengaluru, Karnataka**

These prolonged procedures involved with the UDID have ultimately discouraged many persons with disabilities who are eligible beneficiaries from obtaining benefits. As a focus group participant told us:

> There are server and network issues also [at the local government services centres]. There is no one single window to do all this. The whole process takes very long and you have to go to the centres multiple times. Because of all the troubles involved, many people don't end up going and lose access to the disability pension.
>
> **— Participant in a focus group discussion with persons with disabilities in Bengaluru, Karnataka**

5.2.2. Shared access to mobile phones impact DBT enrolment and verification processes

The DBT infrastructure, alongside linkages with Aadhaar, is reliant on linkages with mobile numbers for enrolment, beneficiary verification processes and notification of payments. Shared ownership and use of mobile phones, whether basic phones or smartphones, create disruptions in the enrolment, verification, and notification processes. As we heard from a participant in a focus group discussion,

> OTPs depend on our Aadhaar card. If the mobile number is linked to the card and we have updated the number, then it will work fine and you receive OTPs properly. Otherwise there will be issues.
>
> **— Participant in a focus group discussion with persons with disabilities in Bengaluru, Karnataka**

As we have seen in chapter 4, women were more likely to not own smartphones, and were more reliant on shared usage of smartphones in everyday digital and digital financial use. For women residing in rural areas, more often than not, the phone is owned by the head of the household and shared with other members for use.

Prior on-ground research has shown how eligible women beneficiaries are sometimes excluded from schemes due to the lack of access to phones to complete verification and

KYC processes.[189] When women beneficiaries have been able to enrol in schemes despite hurdles with shared access, they still face risks of not being able to receive or verify important information relating to updates such as credit of benefit payments, which are primarily notified through SMSes sent on the linked mobile phone. As we heard from a focus group participant in Velhe, Pune:

> If [women in our village] don't have a mobile they use their children's or husbands phone number. Then when the benefit is deposited, their children or husband are alerted [through SMS] rather than the woman who is the direct beneficiary.
>
> **— Participant in a focus group discussion with SHG women in Velhe, Pune**

5.3. DBT payments and settlements: Risks of information asymmetries and disruptions

The Aadhaar Payment Bridge System (APBS) and its payments and settlements infrastructure, alongside system-wide opacity in administrative and KYC processes, has created risks of information asymmetries for beneficiaries, particularly when benefits are delayed or paused. When faced with these critical payment disruptions and other challenges with the DBT infrastructure, beneficiaries are also faced with often inaccessible grievance redressal mechanisms, with disproportionate risk for vulnerable groups in particular.

5.3.1. Opacity and payment disruptions in payments and settlements

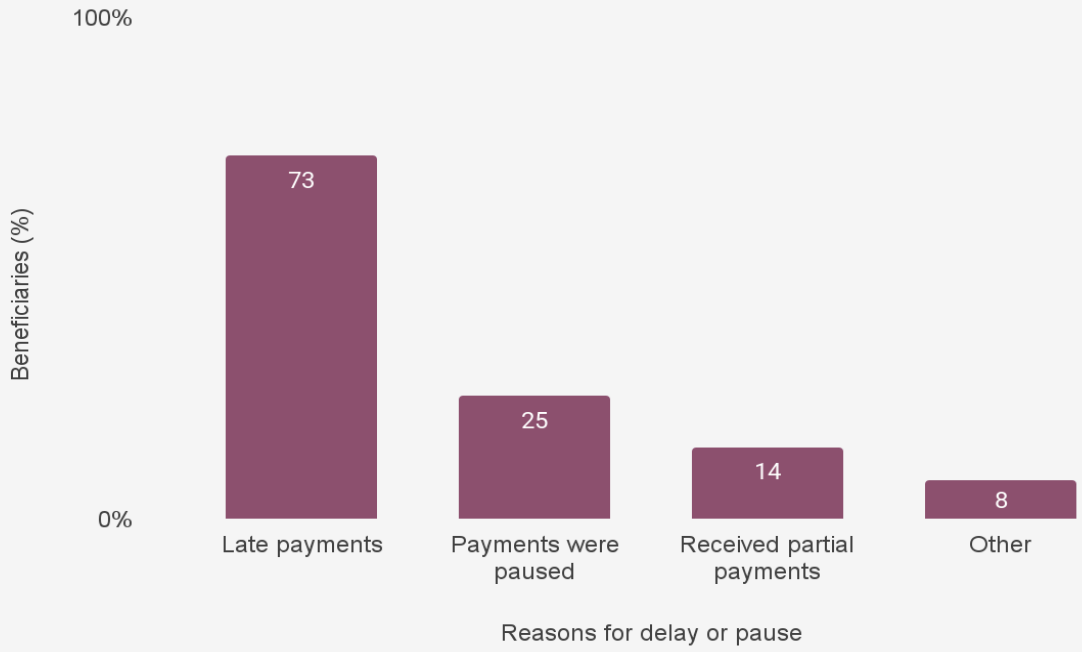
A majority of DBT beneficiaries did not experience a delay or pause in receiving benefits. However, some gaps remain: For 14% of DBT beneficiaries in our survey who faced delays or pause in their benefit payments, late credit of benefits was the most common payment issue faced by beneficiaries (see **figure 5.6.**).

For beneficiaries who are from socio-economically vulnerable groups, a delay or pause can cause particularly high economic distress and impact their financial security.

[189] Sameet Panda. 'Data Systems in Welfare: Impact of the JAM Trinity on Pension & PDS in Odisha during COVID-19'. Centre for Internet and Society, 21 February 2021. https://cis-india.org/raw/sameet-panda-jam-trinity-pension-pds-odisha-covid-19.

Figure 5.6. Almost three-fourths of the beneficiaries who experienced a pause or delay in benefits faced late payments

Percentage of beneficiaries by reasons for delay or pause in receiving DBT benefits (N = 146)



Note: Other reasons include: no payments since enrollment, removal from beneficiary list, payment to another account

Of those who experienced delays or pause of benefits in our survey...

68% (100 of 146) of beneficiaries mentioned that they did not know the reasons for the pause or delay.

In our interview with a researcher working with rights-based campaigns for welfare delivery, they explained some of the possible reasons for payment transfer failures, through their extensive field research on the payments infrastructure under MGNREGA. These are shared in the table that follows:

What DBT payment transfer failures may occur under APBS?	
Rejected or blocked payments	DBT payments that have been blocked or paused, most likely due to issues with Aadhaar seeding and the NPCI mapping of Aadhaar based accounts of beneficiaries, other technical issues with the payments infrastructure, bank account problems, or data entry errors.

Diverted payments	DBT payments that have been transferred to another bank account of the beneficiary, without their knowledge.
Misdirected payments	DBT payments that have been transferred to another person's bank account

Note: These categories of payment transfer failures have been adapted from insights from a key informant interview with a researcher working with rights-based campaigns for welfare delivery.

5.3.2. Need for additional documentation a key reason for delays and pauses in benefits

Of those who experienced delays or pause of benefits in our survey...

14% (20 of 146) of beneficiaries had their benefits paused because additional documents were required to restart benefits.

Blocked payments due to KYC processes that are incomplete or have to be renewed may be one key reason for payments disruptions, as also seen in other on-ground research on challenges with stringent KYC and 're-KYC' processes.[190] Participants in our FGDs with persons with disabilities in Bengaluru, Karnataka and with SHG women residing in Velhe, Pune experienced payment disruptions due to KYC issues in a number of schemes, including disability pensions, PM KISAN and LPG cash transfer schemes.

> There have been cases where women started receiving benefits, but payments stopped after 2 or 3 months. The bank would tell them that your mobile is not linked. They gave a form, and after filling it the payments resumed and pending payments were also received. [...] The problem is that some people don't know what action to take, or whether their mobile numbers are linked or not. Banks may also tell them to get KYC done, but do not explain what this means.
>
> **—Participant in a focus group discussion with SHG women in Velhe, Pune**

> What has happened now is that since the past 3-4 months the disability pension has stopped for everyone [in our group]. If you go to the bank, they say the pension has not been claimed by the beneficiaries and that is why it has been stopped. So they ask us to send details and documents again for eKYC.
> **— Participant in a focus group discussion with persons with disabilities in Bengaluru, Karnataka**

[190] Jean Drèze. 'KYC, Unlock Kar Diya Jaye: Customer ID verification framework is making life difficult for the poor'. *The Economic Times*, 12 February 2025. https://economictimes.indiatimes.com/opinion/et-commentary/kyc-unlock-kar-diya-jaye-customer-id-verification-framework-is-making-life-difficult-for-the-poor/articleshow/118186588.cms.

As FGD participants indicated, KYC involves challenges such as the lack of information or support provided on the requirements of completing KYC processes. Vulnerable beneficiary groups such as women and elderly persons are more likely to require informational intermediaries to support them with KYC processes. Across focus groups, participants emphasised that KYC processes and other processes relating to records and data entry corrections are not as quick and seamless as they are made out to be. They tended to require multiple visits and escalation at multiple levels, resulting in a time consuming and costly experience.

As seen in section 5.2, transgender persons, persons identifying as gender and sexual minorities, and persons with disabilities faced hurdles with the KYC process owing to documentation burdens.

Digital-first grievance redressal mechanisms can be exclusionary for certain beneficiaries

Official grievance redressal mechanisms vary across DBT schemes, but have increasingly involved digital mechanisms such as online platforms and helpline numbers.[191, 192]

Digital mechanisms become immediately exclusionary for beneficiaries who are more likely to have lower levels of digital use and digital literacy.[193] Helpline numbers as grievance redressal mechanisms can pose challenges due to language accessibility. As a researcher working with rights-based campaigns for welfare delivery narrated in our interview, helpline centres may be based in larger cities within a state. As a result, language capabilities of helpline representatives may not include regional languages that are predominantly in use in other districts of the state. As a result, beneficiaries cannot effectively use helplines as a means of seeking redress.

> Channels of grievance are there in theory but not in practice. There could be helplines in place. But, say in certain districts of Jharkhand most people can only speak Santali. They have the option of reaching out to a helpline which is based in a major city in Jharkhand, where the helpline contact can only speak Hindi.
> **—Key informant interview with a researcher working with rights-based campaigns for welfare delivery**

[191] Dvara Research. 'State of Exclusion: Delivery of Government-to-Citizen Cash Transfers in India'. Dvara Research, 2022. https://dvararesearch.com/wp-content/uploads/2024/01/State-of-Exclusion-Delivery-of-Government-to-Citizen-Cash-Transfers-in-India.pdf.

[192] Sameet Panda. 'Digital Delivery and Data System for Farmer Income Support'. Centre for Internet and Society, 18 October 2023. https://cis-india.org/internet-governance/blog/cis-privacy-international-digital-delivery-and-data-system-for-farmer-income-support.

[193] Ibid.

5.4. DBT withdrawal: Challenges with access to withdrawal mechanisms

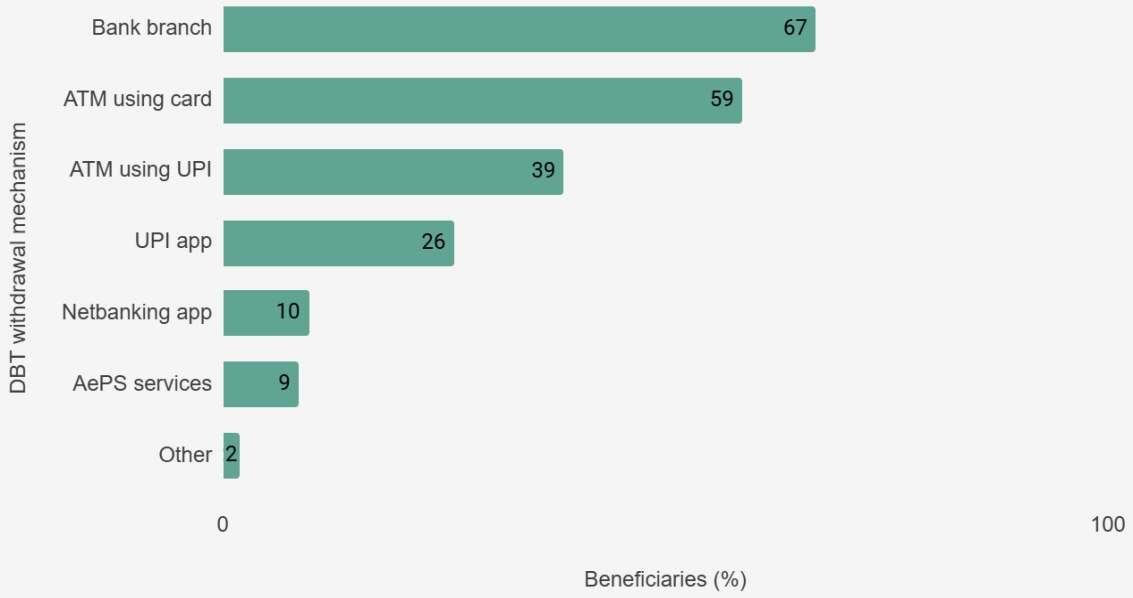
DBT beneficiaries relied on various digital and non digital mechanisms to withdraw DBT payments and risks and challenges in withdrawal may arise for each of these mechanisms.

5.4.1. Comparative risks and harm from DBT withdrawal mechanisms

As seen in **figure 5.7.**, bank branches and ATM withdrawals were the most commonly used mechanisms for beneficiaries. Further, direct usage of benefits through UPI was an important usage mechanism where more than a quarter of beneficiaries used this mechanism. As **figure 5.7**. shows, the use of AePS was lower, with less than 10% of beneficiaries using this mechanism to withdraw DBT payments.

Figure 5.7. Beneficiaries mostly relied on bank branches and ATMs for DBT withdrawal

Percentage of beneficiaries by DBT withdrawal mechanism (N = 1,012)



In our key informant interview with a researcher working with rights-based campaigns for welfare delivery, they spoke of the limitations of DBT withdrawals through AePS and through bank branches, especially for beneficiaries residing in rural areas.

As seen in chapter 4 through experiences of participants in our FGD with women residing in Khed Shivapur village, Pune, there are barriers to accessing AePS due to limited capacity of banking correspondents who have to service multiple villages. Participants also mentioned not having information about which correspondents serviced their village in order to contact them in advance and arrange for AePS withdrawals.

In our interview, the researcher working with rights-based campaigns for welfare delivery described broader structural factors and risks relating to fraudulent activity and "petty corruption" with AePS that may drive lower preference for the service in withdrawing DBT payments:

> One of the pitfalls of AePS is that there is no monitoring framework, and there is no way for anyone to catch petty corruption. It is routine that banking correspondents charge a "transaction fee", depending on the amount of money withdrawn although it's supposed to be a free service, since correspondents are paid by the bank [through a commission-based model].
>
> The fact that there is no monitoring of banking correspondents is a big problem [...] Banking has regulation through an ombudsman, and so on. There is nothing like that for banking correspondents.
>
> **—Key informant interview with a researcher working with rights-based campaigns for welfare delivery**

Aside from challenges with using AePS, our interview with the researcher revealed that withdrawing DBT payments from bank branches is not without challenges. Beneficiaries, particularly those residing in rural areas, face challenges relating to overcrowding at the banks, inadequate staff and technical capacity, and gaps in banking infrastructure penetration. As a result, there is a large time cost incurred when visiting bank branches in rural areas. These costs further have an adverse impact through lost wages, increased commute expenses due to multiple visits to verify whether payments have been credited,[194] and heightened time burdens for women beneficiaries who disproportionately bear greater unpaid care burdens.

[194] LibTech India. 'Length of the Last Mile: Delays and Hurdles in NREGA Wage Payments'. LibTech India, November 2020. https://libtech.in/wp-content/uploads/2020/11/LastMile_ReportLayout_vfinal.pdf.

6.

Digital financial frauds: Risk and vulnerabilities

As shared in the background section, while the primary focus has been on promoting innovation, financial inclusion and ease of doing business, the growth of digital financial services has also led to a rise in frauds and scams. While regulatory frameworks for the fintech industry are continuing to develop in reaction to emerging harms, users' digital and financial literacy levels have not maintained pace with the swift adoption of mobile internet and digital financial services. The Reserve Bank of India (RBI) has also noted how these conditions have allowed bad actors to take advantage of vulnerable users in a developing ecosystem.[195] As we heard from a digital payments researcher:

> Along the line threat vectors have been added across these scenarios, each access layer adds a threat layer alongside it. The access layer benefits a significant chunk of the population, one can also see million people being subjected to digital harms, which they were not previously exposed to.
>
> **—A digital payments researcher in a key informant interview**

[195] Reserve Bank of India. 'BE(A)WARE: A Book on Modus Operandi of Financial Fraudsters'. Reserve Bank of India, March 2022. https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf.

An interviewee from the fintech sector similarly commented on the impact digitalisation has had on the ease with which a scammer can reach people and access sensitive information.

> The surface area for potential fraud touch points are far greater now, on apps, social media, email, etc. All these scams and their modus operandi fundamentally already existed before, but due to digitisation, this fraudulent activity is far easier and greater than ever before.
>
> —Business analyst working at an electronic trading platform, in an interview

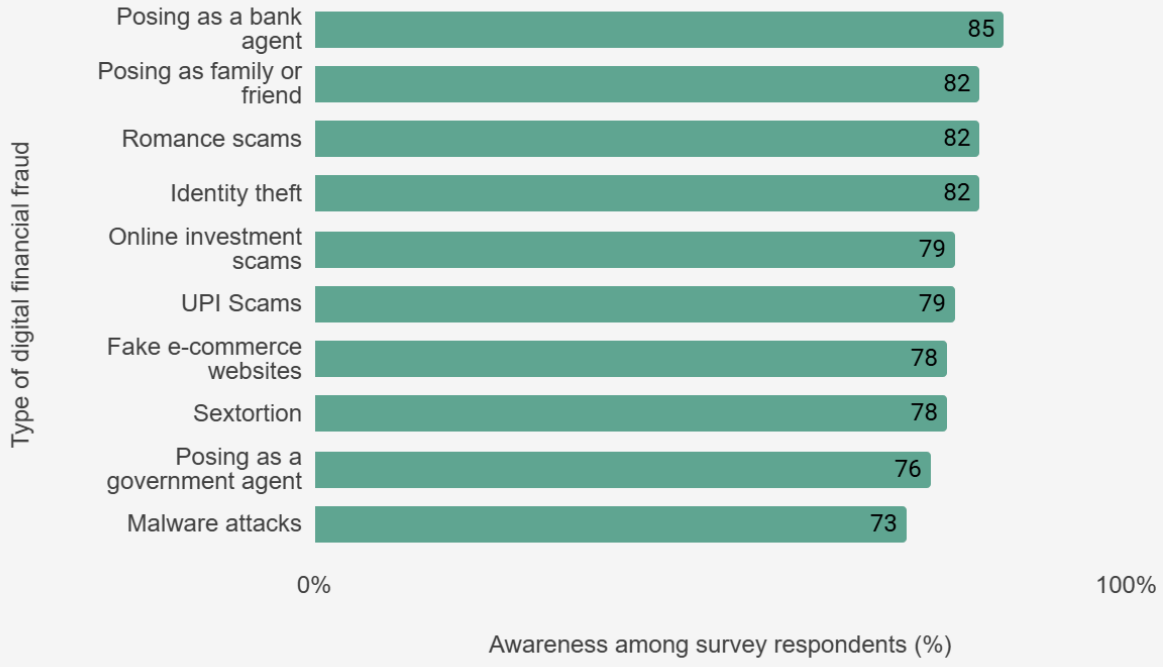
This chapter delves into users' experiences of fraud starting from initial contact to accessing grievance redressal mechanisms. We discuss how levels of awareness, and socioeconomic factors may interact with risk, vulnerability, and the impact on victims, especially in terms of financial loss, and user well being.

6.1. Awareness of digital financial frauds

In our survey, we found a high degree of awareness about frauds. As we see in **figure 6.1.**, nearly three quarters of respondents had heard of the range of digital financial frauds included in the survey like impersonation fraud, romance scams, identity theft, malware attacks and more.

Figure 6.1. More than 4 out of 5 respondents had heard of impersonation related frauds

Digital financial fraud awareness, by percentage of respondents (N = 3,784)



Social media platforms are filled with posts that try to bring awareness about the newest modus operandi being adopted to con users. Often operating in organised groups, scam operations leverage their individual skills to create believable interactions via messages, voice and video calls, social media and web-based journeys. As we heard from a journalist;

> What we learned from speaking to victims is that scammers have become very sophisticated. They are really able to instil a great deal of fear in the victim. They know about police personnel and are able to impersonate them believably. Educated urban elite are also falling for the Fedex scam. It just appears so real. A victim told me they fell for it, because the scammer spoke flawless English.
>
> **—Journalist reporting on scams, in an interview**

One of the challenges to maintaining consumer awareness of frauds is the ability of actors to adopt new tactics and narratives. As we heard from an interviewee;

> The modus operandi changes every 3-4 months. People are also at risk of falling prey to the fraud yet again because of this. Lack of awareness and education are factors, however the pace at which tech and cyber fraud is evolving, even literate populations are falling prey to these frauds.
>
> **—A founder of a digital safety initiative, in an interview**

Scammers working in teams[196] may even utilise multiple stock narratives once they gain someone's confidence to continue extracting money from the same victim. This is especially likely for impersonation scams, which were the most reported in our sample.

> I got a call a few months ago offering me a brand new car. He said, "Ma'am, I am calling you from the lucky draw in Delhi. You have won an offer for a car. If you want it, please send over your documents." Then he told me to send INR 10000 for the car's documents. I gave him INR 5000, and he continued speaking to me nicely and asked for another 2000. When I stopped responding, I received a video call from someone in a police officer's uniform.
>
> **—Participant in a focus group discussion in a Hijra community in Patna, Bihar**

[196] Kapil Kajal. 'The Sextortion Scammers of Rural India'. *Rest of World*, 21 December 2022. https://restofworld.org/2022/sex-scam-village-india/.

As a journalist shared, the spread of text and audiovisual content across regional languages also presents a challenge for detecting and curbing fraudulent content on social media platforms.

> Social media platforms can't monitor the scams in Indian languages, they do not have the skill-sets for this in languages other than English. The detection tools also often cannot detect deep fakes. So a lot of scams in Indian languages go undetected.
>
> — Journalist reporting on impersonation in financial frauds, in an interview

Another development that makes impersonated content easy to create is the availability of voice data that AI voice cloning tools use to enhance fraud operations.[197] Indian users have a much higher incidence of sharing voice online on social media and messaging platforms with 86% doing this at least once or twice a week.[198] 47% of 1,010 respondents in a McAfee survey said they had either been a victim themselves (20%) or knew somebody else who had fallen victim to a scam involving voice cloning (27%)."

6.2. Experience of digital financial frauds

6.2% (234 out of 3784) of the respondents in our survey had experienced fraud online.

Of this group, 15% (35 out of 234) experienced financial loss from an online fraud more than once.

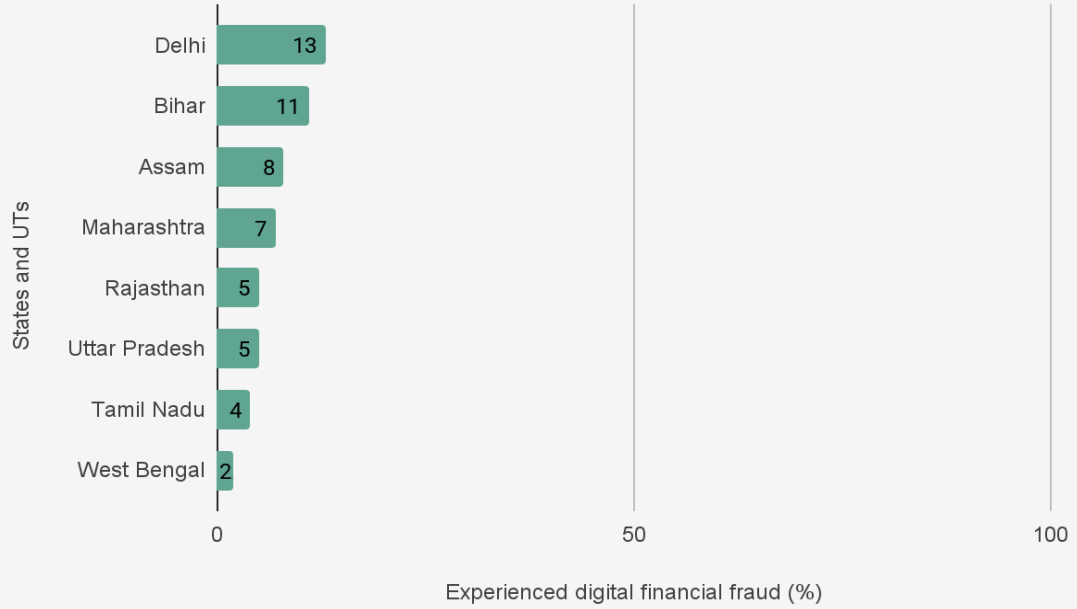
The Reserve Bank's survey on awareness and use of digital payments, similarly found that 94.5 per cent users reported that they have not experienced any fraud. They also found that attempted fraud was lower in metros at 4.1%, relative to semi-urban areas at 6.4%.[199]

When it came to the experience of frauds by state, we found that more than 10% of respondents experienced digital financial frauds in Delhi and Bihar (see **figure 6.2.**)

[197] Indian Cyber Crime Coordination Centre, Ministry of Home Affairs. 'Cyber Digest 17.01.2025 CD-544'. Ministry of Home Affairs. January 2025. https://i4c.mha.gov.in/cyber_digest/jan_2025/Daily%20Digest-17.01.25.pdf.
[198] Amy Bunn. 'Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam'. *McAfee Blog* (blog), 15 May 2023. https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/.
[199] "Report on Currency and Finance 2023-24", Reserve Bank of India, 29 July 2024, https://rbi.org.in/Scripts/PublicationsView.aspx?id=22459

Figure 6.2. A greater proportion experienced digital financial fraud in Delhi and Bihar

Experience of digital financial fraud by State and UTs, by percentage of respondents (N = 3,490)

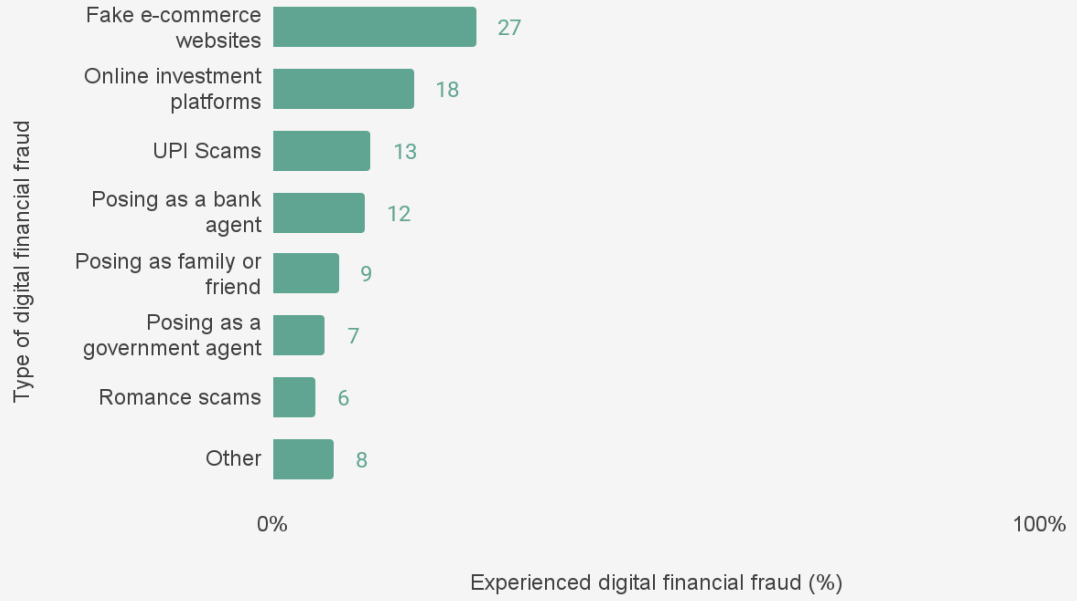


Note: In Karnataka, there was no fraud reported and as such the state has been excluded from the analysis in this chapter

As we see in figure 6.3., fake e-commerce site related frauds, online investment platform frauds, and UPI scams were the top 3 forms of scams, experienced by respondents in our survey.

Figure 6.3. A greater proportion experienced digital financial fraud while using fraudulent e-commerce sites and online investment platforms

Types of digital scams by percentage of digital financial fraud respondents (N = 234)

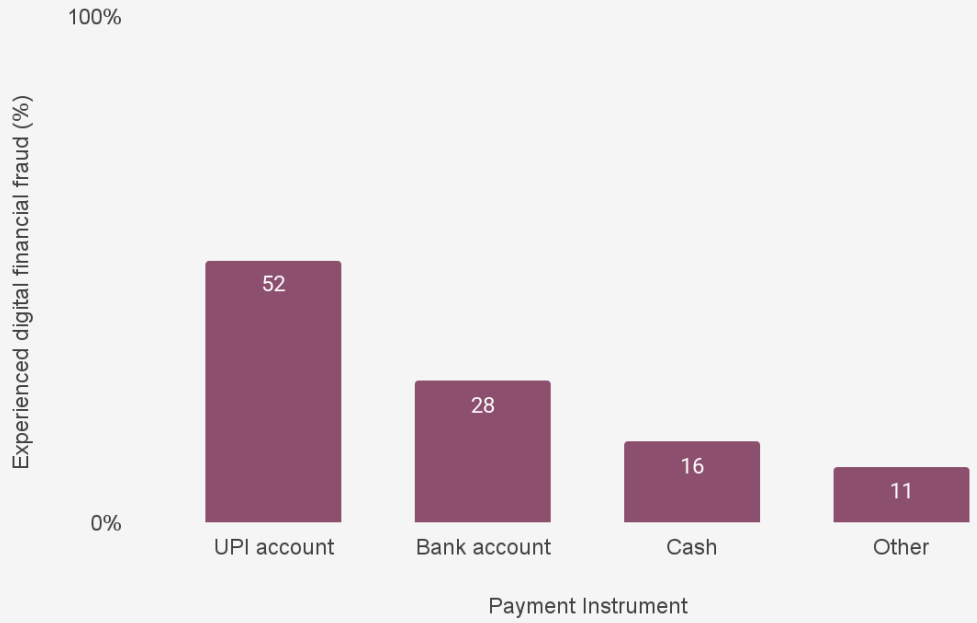


Digital financial frauds lean on UPI transactions

In our qualitative and quantitative data, we found overlaps between experience and awareness of frauds and the use of UPI as a medium (either through direct transfer by the victim or through other mediums highlighted above). As seen in **figure 6.4.**, over half the respondents lost money through UPI transactions, compared to which only half as many people lost money directly through their bank accounts.

Figure 6.4. UPI and bank accounts were two common payment instruments through which respondents lost money

Percentage of digital financial fraud respondents by payment instrument through which they lost money (N = 234)



Note: Other includes Aadhaar pay, credit card, cryptocurrency wallet, prepaid wallet

A cyber security engineer we interviewed who was formerly working on a payment gateway suggested that UPI's design flaws may also be contributing to the higher rates of fraud associated with this payments network:

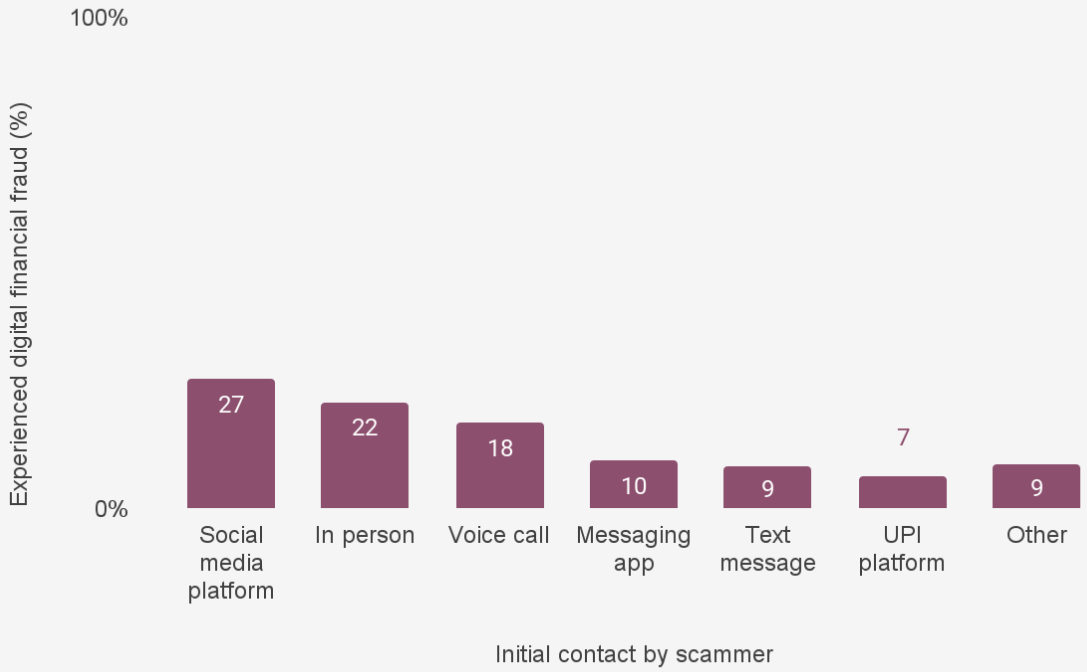
> Payments companies have observed that when it comes to frauds, it often comes down to user error. UPI's evolution has brought in these design flaws. Previously you needed to have a registered merchant account to accept payments. Now, UPI allows for payments to both customers and merchants, and there is no need for registration at certain thresholds. This makes it a very easy tool to use to orchestrate fraud in such a scenario.
>
> **—Cyber security engineer with experience working on a payment gateway**

However, a report by the Standing Committee on Communications and Information Technology suggests that the ratio of frauds to genuine payments over UPI has not shifted drastically between FY 21-22 and FY 23-34.[200]

Scammers contact victims through a range of offline and online channels. When asked how the scammer contacted them initially, the majority reported being scammed through social media, followed by in-person, and over a phone call (see **figure 6.5.**).

Figure 6.5. Defrauded respondents were primarily approached by scammers on social media or in-person

Methods of initial contact by scammer, by percentage of digital financial fraud respondents (N = 234)



Note: Social media platforms such as apps like Instagram, Facebook, Twitter, Chingaari and MX TakaTak. Messaging apps such as Whatsapp and Telegram.

Participant stories

The need for support to access services and finances via digital platforms has also created additional risk for anyone who relies on third party services to bridge the digital divide. Scammers may exploit this lack of familiarity with institutional portals and create clone webpages to mislead people.

[200] Standing Committee on Communications and Information Technology. "Fifty-Fourth Report: Standing Committee on Communications and Information Technology (2023-24): Digital Payment and Online Security Measures for Data Protection", Lok Sabha Secretariat, New Delhi, February 2024, https://sansad.in/getFile/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_54.pdf?source=loksabhadocs

OTP Fraud

A friend filled out an online form to withdraw her PF (provident fund). She got a message to click on the link to get an OTP to withdraw her PF. Instead she lost that money. She wanted to put together funds for her marriage and was focused on this, and instead ended up losing it.

—Journalist and Youtube segment host for a grassroots news platform in an interview

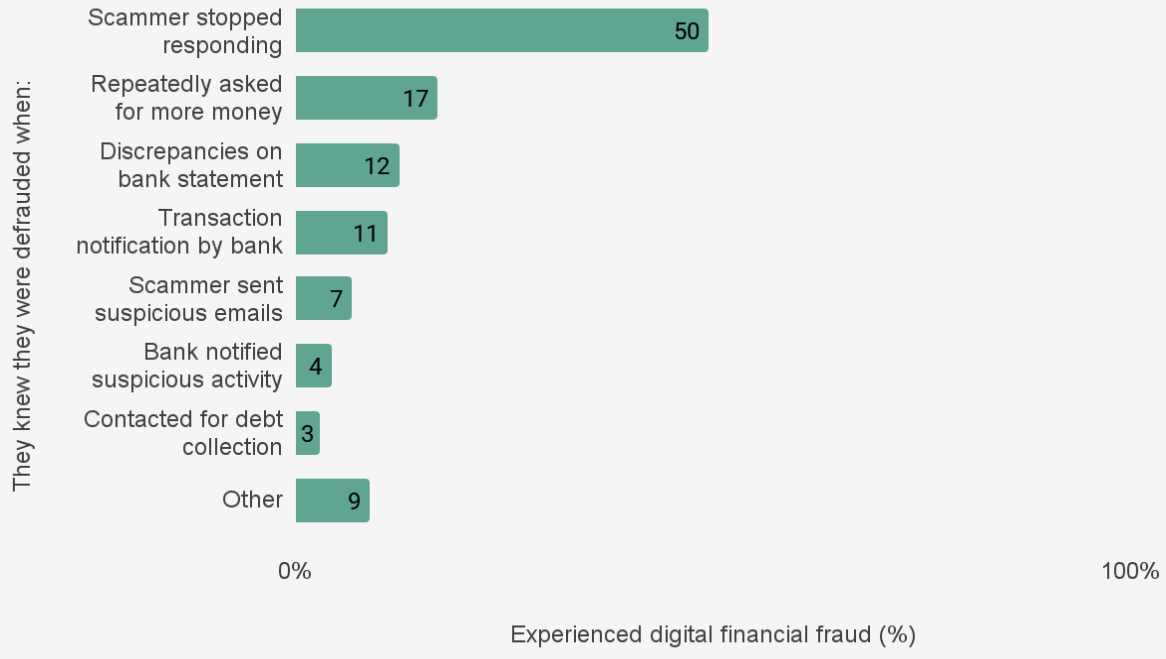
A community lead explained how many members of the LGBTQIA+ community come across links and ads from fraudulent companies and illegal loan apps when searching for related information. Others also fell victim to fraudulent websites and customer service numbers masquerading as their legitimate counterparts, or built a trusting relationship with someone they met on social media.

There are also cases where scammers develop a friendship or relationship with them online. These perpetrators initially build trust and manipulate people to gain access to their private and financial information. Once they have transferred money to their own accounts they will then abscond. We have encountered many such crisis situations.

—Social worker supporting gender and sexual minorities in a key informant interview

Figure 6.6. 50% of the respondents realised they had been defrauded when the scammer stopped responding

Percentage of digital financial fraud respondents by when they realised that had been scammed (N = 234)



47% (109 out of 234) of those who experienced online fraud found out within hours of the incident, 38% (89 out of 234) of them realised within a week. As seen in **figure 6.6**., 1 in 2 respondents realised they had been defrauded once the scammer stopped responding.

As seen in **figure 6.7.**, a majority of respondents were influenced/tricked into depositing money directly into scammers' accounts (46%) or making payments via a fraudulent payment link(16%). Another 12% ended up sharing sensitive information like an OTP that eventually led to a financial loss. The tactic of social engineering for building trust between the scammer and victim was a large component of frauds reported in our survey.

Figure 6.7. Nearly half of respondents who were defrauded deposited money to the scammer's account

Percentage of digital financial fraud respondents by how the scammer collected money (N = 234)

Note: Other methods include screen mirroring app, sharing login pin/passwords

6.3. Economic factors and harms associated with digital financial fraud

Survey respondents reported financial losses ranging from INR 55 to INR 5,00,000. Geographical variations were observed with higher financial losses reported from eastern states of Bihar and Assam, which also reported the highest amounts lost in a single incident. States of Delhi and Maharashtra, where the survey was conducted in metropolitan cities followed right after.

As figure 6.8. suggests, in several states, the median financial loss reported is almost 50% of the median personal income for those that reported having experienced fraud online (see Maharashtra, Uttar Pradesh, for example). This could signal significant financial burden, irrespective of the amount that was lost to frauds.

Figure 6.8. Respondents from Maharashtra and UP reported the highest median financial loss, whereas Bihar had the highest amount lost to digital financial fraud.

Median, range of financial loss by state and UTs, median personal income of each state and UT (N = 234)

States and UTs	Lowest financial loss (INR)	Highest financial loss (INR)	Median financial loss (INR)	Median monthly personal income (INR)	N
Maharashtra	500	50,000	5,500	10,000	52
Uttar Pradesh	250	25,000	5,000	10,000	35
Assam	600	90,000	4,500	10,000	21
Bihar	350	5,00,000	4,000	12,000	43
Delhi	300	50,000	2,200	8,000	37
Tamil Nadu	900	20,000	2,000	18,000	15
West Bengal	250	14,015	2,000	10,000	9
Rajasthan	55	10,000	800	3,000	22

Note: In Karnataka, there was no fraud reported and as such the state has been excluded from the analysis in this chapter

In our survey, income did not seem to have a correlation to the amount of financial loss experienced across groups. Our surveys also show that financial loss faced by victims of digital financial fraud across income ranges is considerable (see **figure 6.9.**).

Figure 6.9. Respondents earning above INR 5,000 reported median financial loss between INR 3,000 and INR 5,000.

Median, maximum financial loss by monthly personal income (N = 234)

Monthly personal income (INR)	Median financial loss (INR)	Maximum financial loss (INR)
No income	2,000	40,000
< 5,000	1,500	20,000
5,001 to 10,000	5,000	5,00,000
10,001 to 18,000	4,500	50,000
18,001 to 30,000	3,000	5,00,000
> 30,000	5,000	90,000

The median financial loss was relatively lower for victims who had no personal income or a monthly income less than INR 5,000. Nevertheless, victims in these income ranges faced financial losses up to INR 40,000 and INR 20,000, respectively. The median financial loss for victims in income ranges from INR 5,000 to INR 1,00,000 were similar with some variation. Therefore, our survey indicates that financial losses through digital financial fraud were not dependent on income. However, economic vulnerabilities in terms of lower personal income ranges implied disproportionate financial impact and reduced capacity to cope with burdens of financial loss emerging from digital financial fraud.

While a majority reported experiencing hardship because of the financial loss, men reported this at a slightly higher degree of 87% compared to 76% of women and 67% of gender minorities. This may be related to gendered differences in the regularity with which respondents may contribute to household financial expenses. 81% (74 out of 91) of respondents reported they faced financial hardship after losing money through an incident of digital fraud.

Of those who had lost money to an incident of fraud in our survey...

82% (75 of 91) also reported that the incident caused stress, anxiety and damage to their emotional wellbeing.

Victims over the age of 60 experienced emotional stress at a higher rate at 90%, and the same was reported by 77% of fraud victims in the ages of 18 to 30 years.

6.3.1. Unemployment and economic vulnerabilities shaping fraud related risks

Economic vulnerabilities can influence increased risk of exposure to and experience of digital financial fraud in multiple ways. The long-term unemployed are at higher risk of experiencing digital financial fraud through employment scams owing to a higher likelihood of interacting and complying with scammers' monetary demands in the hope of addressing prolonged financial uncertainty.

Employment scams have taken on elaborate mechanisms to convince users of the supposed legitimacy of online employment agencies and job boards. In our key informant interview with a programme lead and programme staff at a community organisation for gender and sexual minorities, they described the high incidence of this type of scam, and elaborated on how initial contact is made through fake online job boards, followed by requests for personal information.

An interviewee who is a journalist and YouTube segment host for a grassroots news platform spoke of how these scams are perpetrated:

> A friend of mine received a call, she got a call that she will get a job of 4 lakhs per annum, but she would need to pay INR 50,000. Being from a Dalit background, she thought she may not get another good opportunity, so she sent the money. She had a similar situation where the scammer then vanished after turning off their number.
>
> **—Key informant interview with a journalist and YouTube segment host for a grassroots news platform**

Frauds on digital lending apps: Economic vulnerabilities also comprise structural exclusions from economic institutions. 'Traditional' banking and credit institutions typically use economic indicators in assessing borrowers' creditworthiness. These include credit scores (commonly referred to as CIBIL scores)[201], personal income, regularity of income, and stability in employment. Low income users, and those employed in informal work are therefore much more likely to be deemed 'thin file borrowers' and have their loan applications rejected.

As a result, these users are more likely to obtain 'small ticket' loans from digital lending apps. However, as several ground reports have shown, an ecosystem of fraudulent digital lending apps has proliferated in recent years, bringing risks of prohibitive charges

[201] TransUnion CIBIL (previously Credit Information Bureau (India) Limited) is one of four credit bureaus operating in India. A 'CIBIL score' is a 3 digit summary of an individual's credit history, and ranges from 300 to 900. This and similar credit scores are meant to indicate an individual's creditworthiness.

and predatory lending abuses for already economically vulnerable users.[202, 203, 204] In an interview, a journalist reporting on technology startups and policy described:

> They target those who are desperate for money but have no formal means of getting them, those that have no credit history to get money from banks. The general target of these lending apps are persons in the lower strata of financial income, have lower levels of financial literacy and cannot distinguish/verify the authenticity of the app.
>
> **—Key informant interview with a journalist reporting on technology startups and policy**

6.4. Gendered risk and harms associated with financial frauds

Collective user experiences through our focus group discussions and narratives from interviews with community organisations revealed gendered risks for users identifying as women, gender minorities, and sexual minorities through certain forms of digital financial fraud.

These risks emerge from technology-facilitated sexual violence that forms a key component of victimisation in digital financial fraud, perpetrated by individual or networks of scammers, as well as by institutional scammers.[205, 206, 207, 208]

Image-based sexual abuse (IBSA) is one way through which acts of technology-facilitated sexual violence are perpetrated and become embedded within

[202] Prateek Goyal. 'The Death Trap That's India's Illegal Loan Apps'. *Newslaundry*, 24 September 2022. https://www.newslaundry.com/2022/09/24/the-death-trap-thats-indias-illegal-loan-apps.
[203] Kiran Parashar, and Johnson T A. 'Fast and Furious: When Instant Loan Apps Turn to Abuse, Morph Photos to Blackmail'. *The Indian Express*, 29 July 2023. https://indianexpress.com/article/cities/bangalore/fast-and-furious-when-instant-loan-apps-turn-to-abuse-morph-photos-to-blackmail-8865532/.
[204] Anil Kumar Tiwari. 'The Dark World of Illegal Loan Apps in India'. *Al Jazeera*, 25 December 2023. https://www.aljazeera.com/economy/2023/12/25/the-dark-world-of-illegal-loan-apps-in-india.
[205] Rohini Lakshané. 'IBSA Incidents in India and Impact on Victims: Random Sample'. Zenodo, 17 August 2024. https://doi.org/10.5281/zenodo.13335997.
[206] Anil Kumar Tiwari. 'The Dark World of Illegal Loan Apps in India'. *Al Jazeera*, 25 December 2023. https://www.aljazeera.com/economy/2023/12/25/the-dark-world-of-illegal-loan-apps-in-india.
[207] Rahul Sinha-Roy and Matthew Ball. 'Gay Dating Platforms, Crimes, and Harms in India: New Directions for Research and Theory'. *Women & Criminal Justice* 32, no. 1–2 (4 March 2022): 49–65. https://doi.org/10.1080/08974454.2021.1970696.
[208] Express News Service. '"US Model with Chiselled Body": Delhi Man Who "Blackmailed" over 700 Women on Multiple Dating Sites Lands in Police Net'. *The Indian Express*, 4 January 2025. https://indianexpress.com/article/cities/delhi/delhi-man-blackmailed-women-dating-sites-police-9759951/.

digital financial fraud. [209, 210, 211, 212] IBSA is perpetrated with the primary motive of monetary gain in digital financial fraud by extortion through threats of publishing and distributing IBSA content, and harassment (often repeated and prolonged) for money transfers in return for not publishing IBSA content.

In our focus group discussion in Chennai with gender and sexual minorities, a participant described how IBSA is perpetrated in romance frauds, involving threats of distributing (real or digitally altered) sexually explicit or intimate content on social media platforms like Facebook and Instagram:

> On sites like Facebook, scammers will interact and engage with you with the intention of love. After some days, they will say "give me some money". Once that is done, they will film your videos. After filming the videos, they will send it to you on WhatsApp with a one-time view, and then say "if you don't send me money now, I will create this profile of you on Instagram or Facebook, and I will upload all of these videos with you not wearing your clothes." So they threaten you like this and take money.
>
> **— Participant in a focus group discussion with and gender and sexual minorities in Chennai, Tamil Nadu**

Research and ground reports show that women and gender and sexual minorities who have experienced IBSA face distinct risks and harm while attempting to seek redress and in terms of its prolonged impact.[213, 214]

Gender and sexual minorities who have experienced digital financial fraud involving IBSA also face an increased risk of losing anonymity, and of being outed, which may leave them vulnerable as targets of sexual extortion on dating and social media

---

[209] IBSA involves all non-consensual acts of (including threats of) creating, capturing, publishing, and/or distributing (real or digitally altered) sexually explicit or intimate images/videos.
[210] Nicola Henry, and Asher Flynn. 'Image-Based Sexual Abuse: A Feminist Criminological Approach'. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, edited by Thomas J. Holt and Adam M. Bossler, 1109–30. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-319-78440-3_47.
[211] Rohini Lakshané. 'The Crying Shame of Image-Based Abuse'. *Factor Daily*, 29 August 2024. https://factordaily.com/the-crying-shame-of-image-based-abuse/.
[212] Rohini Lakshané. 'Non-Consensual Intimate Imagery: An Overview'. Take Back The Tech, 21 March 2024. https://www.takebackthetech.net/blog/non-consensual-intimate-imagery-overview.
[213] Rohini Lakshané. 'The Crying Shame of Image-Based Abuse'. *Factor Daily*, 29 August 2024. https://factordaily.com/the-crying-shame-of-image-based-abuse/.
[214] Chandan Bose, and Vishnu Teja. 'Menace of Fraud, Blackmail Plagues Queer Dating Apps'. *The Times of India*, 15 April 2023. https://timesofindia.indiatimes.com/india/menace-of-fraud-blackmail-plagues-queer-dating-apps/articleshow/99506360.cms.

platforms.[215, 216] As a programme lead and programme staff at a community organisation for gender and sexual minorities described in a key informant interview:

> When there are any financial harms that gender and sexual minorities encounter in online spaces, they're in a dilemma of how to resolve the issue or whether to seek redress through the police and so on, because they're living closeted outside of their online persona. In order to resolve the issues, they would have to reveal their identity and they would get outed. So most of the time, they may pay off the money to scammers as a better option rather than facing the risk of being outed to [hostile or abusive] family members.
>
> **—Key informant interview with project lead and project staff at a community organisation for gender and sexual minorities**

6.4.1. Limited digital literacy shaping exacerbated risk

The interconnected ecosystem of institutions and actors mediating digital financial fraud, coupled with constantly evolving modus operandi of frauds, has meant that even digital-first users face a high risk of attempts of fraud or experiencing fraud. These vulnerabilities are further compounded for women, elderly, and low income users who are more likely to have limited digital literacy.[217, 218, 219] Interviews with representatives of community organisations pointed to increased risk of experiencing fraud in comparison to attempts, owing to limited awareness of digital safety information and practices.

> A lot of issues on the supply side have to do with the rapid advancement of technology, and these scams can tend to be pretty sophisticated; this is hard even for a native digital user to identify. There is a narrowing gap between the sophistication on the fraud side, and the fact that there are users with low levels of digital and financial literacy as well, making them more vulnerable to these kinds of attacks.
>
> **–Key informant interview with a digital financial inclusion specialist**

---

[215] Gisela Priebe and Carl Göran Svedin. 'Online or Off-Line Victimisation and Psychological Well-Being: A Comparison of Sexual-Minority and Heterosexual Youth'. *European Child & Adolescent Psychiatry* 21, no. 10 (1 October 2012): 569–82. https://doi.org/10.1007/s00787-012-0294-5.

[216] Manuel Gámez-Guadix, Carmen Almendros, Erika Borrajo, and Esther Calvete. 'Prevalence and Association of Sexting and Online Sexual Victimization Among Spanish Adults'. *Sexuality Research and Social Policy* 12, no. 2 (1 June 2015): 145–54. https://doi.org/10.1007/s13178-015-0186-9.

[217] ASER Centre. 'ASER 2023 Evidence Brief: Digital Readiness of India's Youth'. ASER Centre, March 2024. https://asercentre.org/wp-content/uploads/2022/12/EB_Digital-Readiness-of-Indias-Youth_11.03.2024.pdf.

[218] Tshepo Mokuedi Rasekaba, Pratibha Pereira, Vinaya Rani. G, Riya Johnson, Rebecca McKechnie, and Irene Blackberry. 'Exploring Telehealth Readiness in a Resource Limited Setting: Digital and Health Literacy among Older People in Rural India (DAHLIA)'. *Geriatrics* 7, no. 2 (April 2022): 28. https://doi.org/10.3390/geriatrics7020028.

[219] HelpAge India. 'Special Edition: Impact of COVID 19 Pandemic on Older Persons in India'. HelpAge India, May 2023. https://web.archive.org/web/20240228092013/https://www.helpageindia.org/wp-content/uploads/2023/07/Vol-26-No-2-HI-RD-Journal-May-2023.pdf.

In our key informant interviews, representatives of organisations who worked with women and gender and sexual minorities spoke from their experiences of community members who had faced digital financial fraud.

> Many members of the community may not have the awareness and knowledge to use digital financial apps. In these cases, they're vulnerable to impersonation calls where someone pretends to help them use UPI and other apps. OTP scams happen through this way, as well as attempts at sending phishing links under the guise of sending money to UPI accounts.
>
> **—Key informant interview with a programme lead and programme staff at a community organisation for gender and sexual minorities**

> Vulnerability is tied to digital literacy as well. If they receive calls, then people may be convinced to share details through the promise of loans and so on. Once, a woman signed up for online tutoring classes for her son, and they asked for Aadhaar and PAN details, and an OTP she received from her phone. They took money from her bank account through this. She had only given them her information since she trusted the caller, but there needs to be general awareness about what data needs to be protected and kept private.
>
> **—Key informant interview with programme staff running a helpline for women and GSM facing digital harms**

Users also faced digital financial fraud when they attempted to access and begin usage of digital financial services such as UPI. A participant in a focus group discussion with women users in rural areas faced one such experience when she attempted to set up a UPI account:

> I didn't know that OTP should not be shared. So, when the [UPI registration] process was done and the account was set up, in two minutes they emptied the account and took INR 7,500.
>
> **— Participant in a focus group discussion with SHG women residing in Velhe,Pune**

> ⚠ **Content warning**
> As we've discussed here, consequences of being targeted by digital financial fraud may go beyond the immediate financial loss. The following discussion also includes experiences of victim blaming taking the form of intimate partner and familial violence, and can be distressing for some readers.

6.5. Barriers to reporting and challenges with grievance redressal

Despite experiencing high financial and emotional distress owing to their experiences of digital financial fraud, a majority of respondents in our survey had not reported the fraud to authorities such as law enforcement officers, online cybercrime portals, or banks and other fintech institutions.

Of those who experienced digital financial fraud in our survey...

39% (91 out of 234) of victims reported the fraud to authorities.

6.5.1. Reasons for low reporting of frauds

Across our focus group discussions and interviews with community organisations, a key reason for low reporting was the further risk and harm that marginalised users may face when they actually report or attempt to report digital financial fraud to authorities.

Fear of members in the family or household finding out: In a key informant interview with programme staff running a helpline for women and GSM facing digital harms, they spoke of instances when women had called their helplines after having experienced digital financial fraud. In these cases, the primary concern for the victims was fear that their spouses or other members of their households would find out that they have lost money through financial fraud. It is important to note that this fear was also tied to financial control and violence that the victims may already be facing, which risks being further intensified. In some cases, the interviewees narrated that victims also faced risks of domestic violence as retaliation for having experienced financial fraud.

> A lot of women fear their spouse finding out that they faced a fraud and lost money. Some have said: "Agar mere husband ko pata chal gaya toh woh mujhe maar daleingey." [translation: "If my husband finds out about this, he will kill me."]
> A lot of times, women look for work-from-home opportunities to support the family, but they are unable to express this in their household. They end up losing money due to these scams and are left distressed and helpless. This kind of pressure is not experienced by the men [who have called the helplines].
>
> —Key informant interview with programme staff running a helpline for women and GSM facing digital harms

Risks of facing victim blaming, harassment, and trivialisation of digital financial fraud: is another major hurdle towards reporting and seeking redress for persons who experience digital financial fraud. Across focus group discussions, participants also revealed the victim blaming and trivialisation of digital financial fraud by law enforcement. In some cases, police officers had themselves discouraged participants from filing a complaint and seeking redress after experiencing financial fraud.

> When we file a complaint, they [the police] are not taking it. They blame us saying, "We are putting all this on TV. We keep announcing everywhere that if you receive an OTP, you should not share with anyone, and that you should not share your Aadhaar, PAN, or bank account details."
>
> In police stations they are avoiding filing complaints. Even if they do accept, only in 10 out of 100 cases do they investigate and retrieve the money. But, my money that is gone, is gone.
>
> **— Participant in a focus group discussion with gender and sexual minorities in Chennai, Tamil Nadu**

Problems within law enforcement: For some victims, digital financial fraud was treated as low-priority by the police, and recovery processes as futile and unworthy of time and attention. A participant in a focus group discussion with women in rural Pune described an instance where she faced UPI fraud and attempted to seek redress. She had complained at the police station but the police officers did not do anything. The officers told her, *"You won't get the money back anyway, what is the point in filing the complaint?"* and did not end up registering a written complaint.

6.5.2. Challenges with grievance redressal mechanisms

When victims of digital financial fraud do seek redress and report the fraud to authorities, they are faced with redressal mechanisms that may ultimately be rendered ineffective and non-responsive.

Of those who reported digital financial fraud to authorities in our survey...

Only 11% (10 out of 91) recovered all the money they lost
65% (59 out of 91) were unable to recover their money
13% (12 out of 91) stopped pursuing recovery

Across focus group discussions, participants who were victims of financial or digital financial fraud had reported the fraud to their banks, or law enforcement, or in some cases, sought the help of their kinship and community networks to recover money.

Redressal through financial platforms: None of the FGD participants had reported fraud to platforms when the fraud was mediated through UPI or social media platforms. This low reliance on platforms may indicate a lack of awareness on available redressal mechanisms. As a cyber security engineer who was formally working on a payment gateway told us in an interview—grievance redressal mechanisms for financial platforms can be complex. They further explained:

> A user needs to be very deeply embedded in the fintech ecosystem to seek and understand the redressal mechanisms. The user will need to stay up to date with all the RBI Guidelines around redressal, and go by the book.
>
> **—Key informant interview with a cyber security engineer with experience working on a payment gateway**

In our interviews, cyber security experts expressed concerns around the regulatory preference for self regulation by platforms (including for grievance redressal). A cyber security expert described to us how features for effective grievance redressal have not been baked into the design of the fintech and self-regulatory ecosystem:

> Grievance redressal wasn't baked into the design of financial platforms. This is true for the payment ecosystem, where you need to have a nodal officer and an escalation matrix. The system where the regulator is also the point of the last resort doesn't work out well.
>
> **—Key informant interview with a cyber security engineer with experience working on a payment gateway**

Redressal through banks: Some of the FGD participants in our study who were victims of financial or digital financial fraud sought redress from banks, only to be met with inordinate delays in recovering money, or worse, received no acknowledgement from their bank.

A participant in an FGD with elderly persons told us:

> No payment was made by me, but INR 5,000 rupees was withdrawn from my account, and I got a message about this. I checked with the bank, but I have not got the money back. The bank also never told us anything.
>
> **— Participant in a focus group discussion with elderly persons in Lucknow, Uttar Pradesh**

In our interview, lead at a non-profit organisation advocating for cyber wellness and safety similarly spoke of inaction from banks when victims face financial or digital financial fraud:

> Banks as well have not at all been responsive even in terms of registering a complaint. Just yesterday a woman lost INR 50K because she mistakenly called a fraudulent bank helpline, but the bank refuses to take responsibility for this despite complaints they receive. Banks are doing a lot in terms of cybersecurity but there is nothing done in terms of customer safety
>
> — Lead at a cyber wellness and safety organization, in an interview

Paradoxically, ground reports have shown that people's accounts were wrongfully frozen when a cybercrime investigation was triggered for unrelated digital financial frauds. Much of the harm to users in these cases ends up being a byproduct of law enforcement efforts to address digital fraud.[220]

Redressal through law enforcement: A key informant interview with an interviewee working at a non-profit organisation advocating for cyber wellness and safety shed light on the **capacity and coordination limitations in the law enforcement and investigative agencies that play a role in ineffective redressal for digital financial fraud**.

The interviewee explained that law enforcement and investigative agencies are very **low on funding and manpower** when it comes to investigating digital financial fraud. They further described that typically, officers at these agencies are unable to travel to other states or regions to conduct an investigation due to the lack of funding.

On-ground reports of conversations with law enforcement and investigative officers similarly highlight **challenges with lower staff-case ratios, coordination with banks and financial institutions, delayed reporting, and the wide geographical spread of certain frauds spanning interstate or transnational regions**.[221]

These institutional constraints on coordination and capacity, in turn, have implications on the ways in which agencies determine the priority of complaints, and decisions on investigative processes.

---

[220] Neha Madaan. 'Citizens Suffer as Police Freeze Bank Accounts Chasing Frauds' Money Trail'. *The Times of India*, 15 December 2024. https://timesofindia.indiatimes.com/city/pune/citizens-suffer-as-police-freeze-bank-accounts-chasing-frauds-money-trail/articleshow/116325729.cms.

[221] Prajwal D'Souza. 'Bengaluru Police Staff Stretched Thin by Soaring Cybercrime Cases'. *Deccan Herald*, 5 January 2024. https://www.deccanherald.com//india/karnataka/bengaluru/bengaluru-police-staff-stretched-thin-by-soaring-cybercrime-cases-2836131.

> We cannot expect the police to handle 50,000 cases per day—there is no bandwidth for those many economic frauds. Then how do they decide whom to let go and whom to handle? For one person, their loss of INR 5,000 may be as dear as another person's loss of INR 5 lakhs? So, then how does the police make a decision on segregating and prioritising which frauds will be addressed? These decisions then inform how people will be treated differently at the police station during reporting.
>
> — Lead at a cyber wellness and safety organization, in an interview

Redressal through 'unofficial' mechanisms: Across focus group discussions, some participants who were victims of financial fraud or digital financial fraud ultimately sought 'unofficial' redressal mechanisms, relying on kinship and community networks to recover the money they lost. While support from these networks helped victims recover their financial losses, increased reliance on 'unofficial' redressal mechanisms also individualise the risk, and burden of redress after experiencing digital financial fraud to the victims themselves and their immediate networks.

In some cases where victims seek redressal through 'unofficial' mechanisms, this may bring in increased risks of re-victimisation through an emerging form of digital financial fraud—recovery scams.[222]

In our interview with programme staff running a helpline for women and GSM facing digital harms, they narrated how victims may then be re-victimised through **recovery scams** when they contact scammers posing as 'support organisations' and file complaints with them. Victims who may turn to 'unofficial' redressal mechanisms due to discrimination by law enforcement, as with a majority of experiences of victims who identify as gender and sexual minorities may be at higher risk of being exposed to this form of fraud. Moreover, the interviewees highlighted that victims who have limited awareness of official redressal mechanisms may also face higher risks of recovery fraud.

[222] Recovery scams are a form of advance-fee fraud targeted at previously defrauded victims, where scammers ask for an upfront payment from the victim under the pretence of supporting them with recovery of the money they lost in a previous scam. Scammers may pose as support organisations and list fake websites on search pages.

7.

Discussion and recommendations

As observed in our research, while digitalisation and the growth of fintech has enabled better access to financial services including banking and payments and increased convenience for many users, there has also been a rise in different risks and harms, especially for those at different axes of marginalisation. These are further compounded by a persistent digital divide, and differing levels of media and financial literacy. The digital world is an evolving medium, and concerns related to the design, usability and accessibility of platforms, privacy and security of transactions, and the changing regulatory considerations in the fintech sector also add to the challenges experienced by various users. The prevention and mitigation of digital financial harms therefore requires solving issues at various levels, right from socio-technical factors to regulatory responses.

In this chapter, we discuss our findings and offer some recommendations for various actors in the ecosystem, including financial institutions and platforms, regulators and policymakers, and law enforcement, among others.

7.1. Create meaningful connectivity and access to digital platforms

A number of interviewees pointed out how the shift to digital platforms introduces a new vector of social privilege in the form of access to public infrastructures and services.

These are perpetuated both due to lack of access for specific user groups to digital platforms, due to linguistic, social and economic barriers, including the lack of digital and financial literacy, and as a result of increasing and sometimes forced digitalisation, which create newer forms of vulnerability to harm. The lack of, or limited access to the digital world could lead to a compounding of harms, especially in interaction with other vectors of privilege and access for certain marginalised groups.

Improving public infrastructure: As digitalisation of services becomes pervasive it is important to ensure adequate infrastructure is made available to support undisrupted connectivity to the internet and online services for populations across urban and rural geographies, e.g. through strengthening fiber optic cabling networks. In locations that are considered remote or commercially non-viable, public infrastructure would need to be developed to ensure access. Similarly access to transaction points should be available within settlements, so users do not have to travel long distances to avail of basic financial and welfare services. Some researchers suggested that they be made available as panchayat based services to build onto existing infrastructure.

Addressing challenges of mediated use: Many of the user groups mentioned above inevitably rely on family members, friends or other individuals for use of digital financial services, either due to lack of access to devices themselves, or due to limited digital and financial literacy. This also opens up the potential for misuse, including fraud and economic abuse, often as a result of sharing sensitive financial information. Any measures to address digital financial harms through capacity-building will need to factor in these challenges of meaningful access and use of digital financial platforms.

7.2. Improve platform design, accessibility, and usability

The role of design in mediating experiences with digital platforms has more often than not been quite poorly understood. Our research highlighted several areas where platform and interface design may be improved to foster better access, accessibility and usability of digital financial services, and in the process, help mitigate the possibility of frauds and harms. At the onset, using disability justice principles in design (this includes principles such as *'nothing about us without us'*[223]*)* and adopting feminist design thinking[224] can go a long way in designing more inclusive digital platforms. These comprise a focus on identifying the intersectionality of socio-economic and linguistic barriers to access to digital technologies, and exploring community-led or mediated (through engagement with a diversity of collectives and practitioners) forms of design and technology development that may help mitigate harms resulting from structural

[223] James I. Charlton. *Nothing About Us Without Us: Disability, Oppression and Empowerment.* University of California Press, 1998.
[224] Sasha Costanza-Chock. *Design justice: Community-led practices to build the worlds we need*. The MIT Press, 2020.

inequalities. Further, all digital financial platforms need to undergo design audits at various stages of development and deployment to ensure that barriers to access, breaches or vulnerabilities are not a systemic design flaw, and that some gaps that we mention below, may be addressed in a timely manner.

Assessing ease and accessibility of information on platforms: Content available on financial platforms and apps are not often presented in the most accessible manner, especially for people with limited digital and financial literacy. Improvements here include using visual/audio cues that make sense in particular socio-economic contexts, minimising legalese, and ensuring that crucial information is shared early in the workflow, such as before the KYC process. Privacy features and risks, for instance, should be presented to users in simple language, replacing hidden and inaccessible legalese, and be available in regional Indian languages above and beyond official state languages.

Implementing assistive technologies: There are a number of assistive technologies available in the market for persons with disabilities, such as talking ATMs, Braille displays, speech recognition etc.[225] Better and widespread implementation of these technologies, including integrating screen readers into apps and websites, and retaining facilities like phone banking would help this section of users in navigating digital platforms much better.

Developing digital financial services in Indian languages: There is an urgent need to ensure availability and usability of digital financial services across the larger number of Indian languages, accounting for their diversity while including low-resource ones by designing specifically for them. This comprises addressing both technological challenges with Indic language software and fonts, and bridging socio-linguistic gaps in translation and design. Collaborations with projects on translation and natural language processing (NLP) such as Bhashini, developed by the Ministry of Electronics and Information Technology (MeitY)[226] which are also available through open Application Programming Interface (APIs) would facilitate wider availability of financial information in Indian languages.

Creating friction on digital payment platforms: As observed by some of the interviewees, sometimes losses on payment platforms are due to the ease of onboarding and transactions, as a result of convenient design. This can lead to users making payments quickly, without being nudged to verify or cross check their transaction. There may be merit in thinking about introducing some friction in the design of these platforms

[225] Louise Puli, Natasha Layton, Diane Bell, and Abu Zafar Shahriar. "Financial Inclusion for People with Disability: A Scoping Review." *Global Health Action* 17 (1).2024. doi:10.1080/16549716.2024.2342634.
[226] 'Bhashini'. Ministry of Electronics and Information Technology, accessed April 2, 2025 https://bhashini.gov.in/

such that users are able to pause and cross check their payments before actualising them.

Mitigating unique concerns of mediated use: As many people use digital services with mediation or support from time to time, it is important to understand the unique security concerns that may emerge here through consultations with users. This is necessary to develop a more safe and inclusive design for platforms. For example, a visually impaired user shared that the time-limit for sharing OTPs is too short for them to complete a transaction with assistance from the screen reading software alone. Other times the speech-to-text feature is not available in financial applications. So they seek support from others here, and end up sharing sensitive information.

Implementing trust signals on platforms: Beyond just consumer awareness of frauds and privacy risks, digital financial platforms also need to proactively add 'trust signals' to their websites, apps and products to ensure trustworthiness and ensure confidence among users. Some examples include Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates, security seals, accreditation badges, customer reviews etc. which demonstrate that a platform or product has been vetted by third parties for legitimacy and safety.[227] A related point here is to also build digital literacy and awareness of these trust signals through public campaigns so that consumers are also able to identify and look out for them when undertaking financial transactions.

User-friendly and accessible reporting methods: Mechanisms to report digital financial harms need to be accessible to a wider diversity of users. This includes making them more visible on apps and platforms, available in Indian languages, accessible to persons with disabilities, and available both online and offline. Reporting methods need to be culturally sensitive and user-friendly so as to encourage vulnerable user groups to come forward, without fear of retaliation, shame or judgement.

7.3. Build awareness and capacity across user and stakeholder groups

While a considerable part of time and effort on this study was focussed on understanding the prevalence and forms of digital financial harms, there were also a number of recommendations on their prevention and mitigation. These are measures addressed towards some key stakeholders, including but not limited to government and regulatory bodies, banking and financial institutions, fintech platforms, civil society organisations and users themselves.

[227] Luis-Alberto Casado-Aranda, Angelika Dimoka, and Juan Sánchez-Fernández. Consumer Processing of Online Trust Signals: A Neuroimaging Study. *Journal of Interactive Marketing,* 47(1), 2022. 159-180. https://doi.org/10.1016/j.intmar.2019.02.006 (Original work published 2019)

Customising capacity building efforts: An overwhelming concern among many research participants in using digital financial services, particularly UPI, was related to payments going to the wrong person, and the potential for misuse and fraud due to their own limited knowledge of these technologies. Capacity building programmes should be designed to cater to a range of user groups - this is particularly important for vulnerable groups like low-income users, women, persons with disabilities, gender and sexual minorities, the elderly and regional language users.

Diversifying skills training: While previous government initiatives for capacity building focused on training one individual within each family, it is important to ensure people with limited access to digital devices and the internet, e.g. married women, are included in such efforts to reduce their dependence on others. Further, gaps in understanding related skills like financial literacy, fraud awareness and media literacy should be addressed during digital literacy training as well.

Evaluating programmes and foster community participation: Past programmes for financial literacy have been criticised for focusing solely on numbers enrolled. However, to ensure a basic level of understanding, and that people are able to detect and avoid risks, an evaluation of learnings should also be conducted. Financial institutions can partner with non-profit organisations who have expertise in engaging with communities on designing, implementing and evaluating inclusive capacity building programmes to improve community participation, and bolster community-led efforts.

Mandating anti-discrimination/sensitivity training for employees: For certain groups their access to basic financial services might be limited by the attitudes of employees at their local bank branch or an algorithm judging their credit worthiness. This is often the experience for persons with disabilities and trans people, who may be excluded from services due to discriminatory attitudes or assumptions about their individual capabilities. Sensitivity training for employees in financial services sectors such as banks, and in law enforcement would enable users, particularly those from marginalised groups to access services and reporting and redressal mechanisms with confidence.

Building user awareness of sensitive information: Users may not understand the sensitivity of certain identity documents and financial information, and may need to build awareness on data sharing and associated risks. These can present further nuanced challenges for specific groups; such as sharing sensitive financial information within the family may create vulnerability to financial exploitation and disempowerment. For example, societal norms around managing money lead to presumptions that women are incapable of managing their own finances. When working with women elderly it is also important to unpack the dynamics of power and trust within families, so they can make informed decisions about their financial information.

7.4. Centre consumer protection in regulatory interventions and approaches to law enforcement

As shared in the background section, various steps are being taken both at the level of regulation and law enforcement to prevent as well as mitigate harms resulting from digital financial frauds. However, given the fast paced shifts in the fraud ecosystem, and the new tactics that get continually adopted, coupled with overlapping jurisdictions amongst regulatory bodies, regulatory interventions continue to be lagging.

Regulating authorised but unintentional payments: One of the major challenges remains the unintentional sending of money to fraudsters by the victims. There are some regulations being tested in different jurisdictions that we could look at. For example, the UK's Payment Systems Regulator (PSR) requires banks to reimburse victims of authorised push payment (APP) fraud, where victims are tricked into sending money. Effective since October 2024, the protections apply to individuals, microenterprises and charities and includes all types of APP fraud, including impersonation or romance scams.[228] By placing accountability on banking institutions and fintechs, such responses may create more ex-ante measures to protect consumers and prevent fraud in the first place.

Curbing fraud calls and messages: A large number of research participants, especially in the focused group discussions, asked for a stronger check and prevention of fraud calls and messages, identifying government, regulatory and banking authorities as mainly responsible for this task. While the role of telecom and internet services providers, and other such intermediaries such as big-tech and social media platforms did not come up directly in these discussions, they are also key stakeholders in the collective responsibility to weed out bad actors utilising these platforms and networks to run frauds and scams. Some examples of state-led interventions here include Telecom Regulatory Authority of India (TRAI)'s Mobile Number Revocation List (MNRL) hosted on the Digital Intelligence Platform (DIP) to enhance fraud risk monitoring and prevention,[229] fraud reporting facilities like Chakshu-Sanchar Saathi,[230]and the National Cyber Crime Reporting Portal and helpline.[231]

Ensuring redressal mechanisms are robust and time-sensitive: A large number of digital financial harms go unreported both due to a lack of awareness but also trust in reporting and redressal mechanisms to effectively resolve the issue. This also includes

[228] "APP Fraud Reimbursement Protections." Payment Systems Regulator, accessed April 5, 2025. https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protection
[229] "Home" Mobile Number Revocation List Portal, Telecom Regulatory Authority of India, Government of India, accessed April 5, 2025. .https://mnrl.trai.gov.in/homepage.
[230] "Home", Chakshu, Sanchar Saathi, Department of Telecommunications (DoT), Government of India, accessed April 5, 2025. https://sancharsaathi.gov.in/sfc/
[231] "Home" National Cyber Crime Reporting Portal, Ministry of Home Affairs, Government of India, accessed April 5, 2025. https://cybercrime.gov.in/.

fear or reluctance to engage with authorities like law enforcement, or concerns about liability due to their own limited knowledge of digital financial services. There is a need therefore to engage with a larger community of users to build trust in existing redressal measures, and ensure that these are also robust and time-sensitive. This would not only serve as a deterrent to fraudulent actors, but also reinforce faith in timely resolution of matters.

7.5. Measure, evaluate, and improve digital public infrastructures for maximising public value

Digital public infrastructure (DPI), when built well, can generate value and benefit society at large. As we saw in our research, while UPI and DBT disbursals through digitised pathways have had some successes, it has also led to some challenges and specific types of exclusions. As research and policy discourse has pointed out, hyper focus on technological systems without adequately considering broader institutional structures and the political economy in which the systems are being deployed,[232]particularly with the existing social inequities, may leave those at the margins further susceptible to harm. For DPI to work in the public interest, it will be necessary to enable certain monitoring and evaluation frameworks that can iteratively support improvement of these systems with the goal of public benefits and maximising public value. Several issues raised earlier about design, access, privacy and security, as well as connectivity also apply to digital public infrastructures and hence are not repeated in this section.

Creating transparent governance and public oversight: This can allow for greater trust in DPI and ensure that it operates while balancing the interest of private sector actors with that of the wider public, and ensures their participation with equitable access.[233] Further, promoting just and detailed internal governance mechanisms including robust decision-making processes, updating of risk management frameworks[234] as the digital financial landscape transforms, and encouraging multi stakeholder participation and

[232] Suyash Rai, "Economic Development and Digital Transformation: Learning from the experience of Aadhaar and Financial Inclusion in India" xKDR Forum, 2024. https://papers.xkdr.org/papers/2024Rai_ecoDevelopmentDigitalTransformation.pdf.

[233] David Eaves, Diane Coyle, Beatriz Vasconcellos, and Sumedha Deshmukh. "The Economics of Shared Digital Infrastructures: A framework for assessing societal value." UCL Institute for Innovation and Public Purpose. IIPP Policy Report (2025) https://www.ucl.ac.uk/bartlett/public-purpose/publications/2025/mar/economics-shared-digital-infrastructures.

[234] G20 Global Partnership for Financial Inclusion, Policy Recommendations for Advancing Financial Inclusion and Productivity Gains through Digital Public Infrastructure (New Delhi: Department of Economic Affairs, Ministry of Finance, Government of India, 2023), https://dea.gov.in/sites/default/files/G20%20Policy%20Recommendations%20for%20Advancing%20Financial%20Inlcusion%20and%20Productivity%20Gains%20through%20DPI.pdf.

engagement, where appropriate, could help improve greater transparency and accountability.

Measuring impacts of DPI: It will be critical to measure and evaluate the impact of DPI to ensure that it continues to not just work in public interest, but is also able to specifically include those most marginalised. A recent report by the Digital Impact Alliance offers several suggestions towards how this impact, specifically for UPI may be measured, right from having avenues for continuous impact measurement as opposed to a one time activity, to incorporating subjective parameters such as trust in DPI. In particular and from the lens of financial inclusion, the report specifically suggests that efforts should be made to measure the impact specifically on underserved sections of society.[235] As our study highlighted, women, gender and sexual minorities, and persons with disabilities may be experiencing very specific kinds of barriers in adoption of digital financial services, which need careful consideration.

Actively promoting further research: Given the fast-paced and evolving nature of digital technologies being deployed in the finance sector, and introduction of regulatory interventions, it is imperative that knowledge gaps are identified and addressed in a timely manner. Promoting and undertaking research in these areas on an ongoing basis, may help clarify impacts of existing DPI deployments. It can also point to specific adjustments that may be needed in the DPI ecosystem to improve coverage and ease of use, across a diverse set of stakeholders.

[235] Venkatesh Hariharan, "Digital Payments Are Boosting Global Financial Inclusion. As They're Integrated in DPI Efforts, Understanding Their Impact Is Crucial," Digital Impact Alliance, March 25, 2025, https://dial.global/digital-payments-impact/.

Conclusion

The digital transformation in the Indian finance sector has been rapid, especially in the last couple of decades, along with advancements in the models for financial inclusion and welfare delivery. However, the concomitant rise in digital financial harms, seen in the increasing prevalence of frauds and scams, financial mis/disinformation, predatory loan apps, sextortion and economic abuse has also urged a closer look at the digitalisation of financial services and platforms, and the existing guardrails against such harms. As illustrated in emerging research, and corroborated by findings in this study, digital financial harms, while a recent phenomenon, cannot be understood in isolation as they are linked to larger changes in the financial and technological ecosystem in India.

Further, even as digital financial harms may affect anyone across socio-economic strata, including educated, digitally literate, young, and socially mobile consumers (contrary to popular perception), specific user groups such as women, elderly, gender and sexual minorities, persons with disabilities, regional language users, and low-income groups face several differential impacts with respect to these harms, and unique challenges in both their prevention and redressal. As observed earlier, the trajectory of vulnerability, risks and harms related to digital financial services operates within a complex context of socio-technical factors that determine both access to and meaningful use of these services.

The challenges posed by the lack of digital infrastructure, whether devices or the internet, continue to determine access to digital financial services, even in terms of basic banking facilities. While the growth of the agent-based banking model, and later services such as APBS and AePS have aimed to make banking services more responsive to the needs of a wider population, this requires consistent upgrade in public infrastructure and outreach, keeping pace with technological advancement as well as regulatory interventions to address challenges of privacy and consumer protection more broadly. The continued prevalence of mediated use practices, especially among specific user groups mentioned above, and the role of digital and financial literacy in preventing and mitigating financial harms are both areas for research and active intervention in terms of building capacity and awareness.

Finally, in addition to the implementation and strengthening of digital public infrastructure to address some of the above challenges, including improvements in design and cybersecurity, there is a need to develop robust regulatory interventions with a community-facing approach, including but not limited to preventing financial harms. This would also help address the challenges of reporting and redressal of digital financial harms, especially among the most vulnerable groups.

The fintech sector in India is expected to grow significantly by the end of the decade to an estimated value of USD 420 billion, spurred by digital payments but also the interconnection of multiple financial ecosystems through tokenisation, unified ledger, FINTERNET, and developments in artificial intelligence.[236] While the sector is one of the most heavily regulated and closely watched, and a lot is already being done by key regulatory stakeholders, regulatory developments still struggle to keep pace with infrastructural and technological advancements. Regulatory interventions could also include reviewing current frameworks around governance and digital financial inclusion, and exploring models that are open, inclusive and fostered through community participation.[237] These would offer better insights and solutions to prevent and mitigate digital financial harms and develop a more robust and accessible digital financial ecosystem.

We hope that this research project and its findings can help in creating more understanding of risks and harms as experienced by specific marginalised user groups and also contribute to discourse on design, regulatory and policy interventions.

[236] National Payments Corporation of India, 'Fintech Sector – Catalyst to Growth', Keynote Address by Shri Ajay Kumar Choudhary, Non-Executive Chairman and Independent Director, National Payments Corporation of India, ASSOCHAM's 2nd India International Fintech Festival in New Delhi, July 18, 2024. https://www.npci.org.in/PDF/npci/chairman-speeches/2024/Special-Keynote-Address-delivered-by-Shri-Ajay-Kumar-Choudhary-Non-Executive-Chairman-and-Independent-Director.pdf

[237] Suyash Rai and Anirudh Burman, "Financial Inclusion and Digital Transformation in India | Understanding Indian Cities", Carnegie India, September 6, 2023. https://carnegieendowment.org/india/ideas-and-institutions/financial-inclusion-and-digital-transformation-in-india-or-understanding-indian-cities?lang=en

Annexures

Annexure A: Survey socio-demographic profiles

Figure A.1. Percentage of respondents by gender identity

Gender identity	N	Percentage
Man	1,795	47
Transgender persons	252	7
Woman	1,737	46
Total	**3,784**	**100**

Figure A.2. Percentage of respondents by caste category

Caste category	N	Percentage
General	1,354	36
Other	105	3
Other Backward Classes (OBC)	1,410	37
Prefer not to disclose	25	1
Scheduled Castes (SC)	687	18
Scheduled Tribes (ST)	203	5
Total	**3,784**	**100**

Figure A.3. Percentage of respondents by religious identity

Religious identity	N	Percentage
Buddhist	119	3.1
Christian	52	1.4

Hindu	3,129	82.7
Jain	9	0.2
Muslim	453	12
Other; please specify	7	0.2
Prefer not to disclose	11	0.3
Sikh	4	0.1
Total	**3,784**	**100**

Figure A.4. Percentage of respondents by migrant status

Migrant status	N	Percentage
Not a migrant	3,175	84
Inter-state migrant	221	6
Intra-state migrant	388	10
Total	**3,784**	**100**

Figure A.5. Percentage of respondents by extent of familiarity with English

Regional language speakers	Speak, read and write	Speak and read but not write	Only speak	Understand some words and phrases	Do not use this language	N
Assamese	48%	3%	4%	20%	25%	255
Bangla	51%	1%	2%	31%	15%	297
Hindi	54%	10%	4%	20%	12%	1,922
Kannada	57%	3%	6%	23%	11%	294
Marathi	38%	1%	1%	36%	25%	653
Tamil	44%	19%	6%	28%	3%	357
Total	**50%**	**8%**	**4%**	**25%**	**14%**	**3,784**

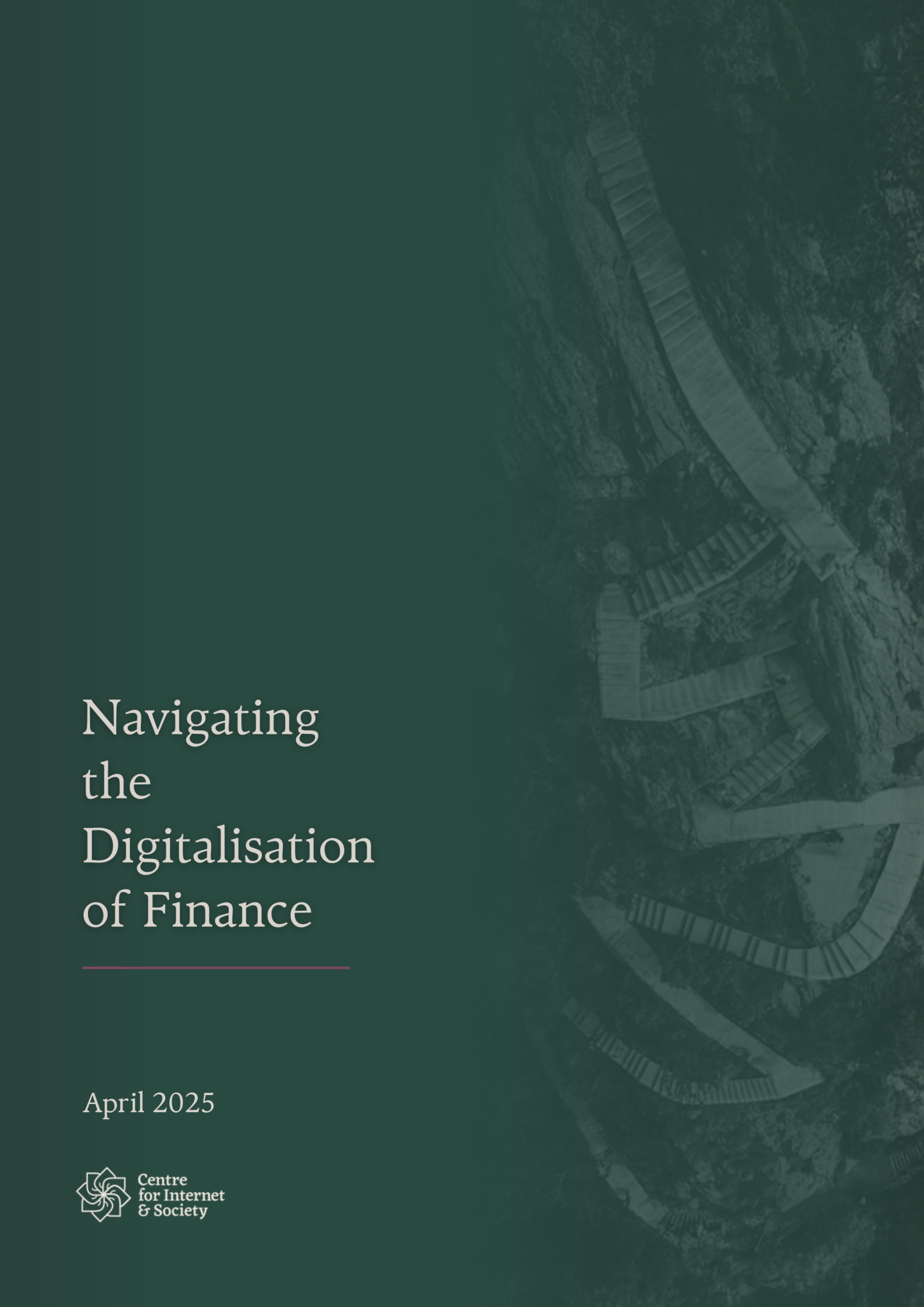
Annexure B: Survey data verification

Data Verification: Data verification was carried out in tandem with the data collection, and continuous feedback was provided to the agency to improve data quality of subsequent phases.

Data quality checks by CIS were run to identify and correct data errors, monitor survey progress, measure enumerator performance. Entries that were flagged were sent to the data collection agency for removal and/or revalidation.

- Data errors for categorical variables were captured by investigating the entries for low response rates, uneven distributions, monitoring frequency of skip questions and conditional questions. We evaluated summary statistics and outliers to identify errors in numerical variables.
- Checks on logical consistency were conducted to flag impossible/improbable responses by cross tabulating responses across comparable questions.
- Length of survey was monitored and entries with duration less than 15 minutes were dropped, along with duplications of IDs, and monitoring for specific user group quotas determined in survey sample.
- Enumerator checks were done on skip questions, key multi-select questions, survey length.
- Back checks and spot checks were conducted by the data collection agency and monitored by CIS through frequent calls.

Data cleaning strategies involved data transformation including cleaning text entries, generating new variables, dealing with missing values, renaming variables to prepare the dataset for analysis.



Navigating the Digitalisation of Finance

April 2025

Centre for Internet & Society