USER EXPERIENCE WITH DIGITAL PAYMENTS IN INDIA

KOAN

Authors

Shivangi Mittal, Varun Ramdas
Research support from Ishita Kirti.
Design by Drishti Khokhar.

Acknowledgement:
We thank Youth ki Awaz for conducting the survey for this report. The authors are grateful to Mr. Vivan Sharan, Dr. Vikash Gautam, and Mr. Aayush Soni for their feedback. All views expressed here, as well as errors therein are the authors' alone.

contactus@koanadvisory.com | www.koanadvisory.com

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Full Form
AePS	Aadhar enabled Payment System
FY	Financial Year
GDP	Gross Domestic Product
ITU	International Telecommunications Union
MDR	Merchant Discount Rate
NEFT	National Electronic Funds Transfer
PoS	Point of Sale
PSD2	Payment Services Directive 2
QR Code	Quick Response Code
RBI	Reserve Bank of India
RTGS	Real Time Gross Settlement
UK	United Kingdom
UPI	Unique Payments Interface
USA	United States of America

TABLES

FIGURES

EXECUTIVE SUMMARY

India has witnessed a sharp increase in the number of users who conduct digital payments, since 2016. Technological innovations, regulatory changes and policy efforts have driven these efforts to formalise the economy. The COVID-19 pandemic has also encouraged digital transactions, as consumers increasingly purchase commodities online and strive to maintain social distancing. Now that the market has expanded to include many first-time users, it is important to ensure that they use digital services consistently to sustain the growth of these instruments.

This report presents findings from a survey of approximately 5,000 individuals to evaluate users' experiences with digital payments, and identify necessary reforms to encourage usage. The first chapter dwells on the developments in the Indian digital payments market. Chapter two describes the survey sample and details user characteristics and preferences. Chapter three demonstrates that before transacting, users consider whether digital payments are likely to be as easy, safe, and reliable as cash. Almost a third of survey respondents reported that they checked whether the basic requirements to transact digitally were in place. These included access to a secure internet connection or using the same payment system as the party they were transacting with.

Privacy and security were other factors that most respondents considered before transacting digitally. Very few of them reported transacting digitally if they felt that their privacy or security was compromised. Next, most respondents cared about factors of convenience, such as discounts for digital payments, and whether the transaction amount is easier to pay in cash or digitally.

Chapter four reveals that during a transaction, most users reported facing transaction failures and network-related problems across all instruments. It also discusses user experience with the grievance redressal process. Over two-thirds of survey respondents reported that their grievances were resolved within a week. However, 48 percent of them had a negative experience with the process, which include inadequate explanations, unsatisfactory resolutions, and the inability to recover their money. The survey results also indicate that there is great variance in the grievance redressal process. Most people contacted payment service providers, e-commerce platforms, and banks when they faced problems. Among the various parties that users contacted for grievance redressal, e-commerce platforms seem to have the easiest processes, whereas police had the most cumbersome one.

Chapter five summarises key survey findings and recommends efforts to improve quality of service. If deficiencies and variations in the consumer's quality of experience have to be addressed, then current mechanisms should be strengthened and new measures should be ushered in. Regulatory interventions can help remedy lapses in service quality, to ensure that users feel secure about a safe and trustworthy transaction experience. The quality of experience framework for digital payments could be maintained by prescribing standards, enhancing user awareness and access to infrastructure. Global best-practices suggest that these should include measurement of completion of transfers, transfer declines, a turnaround time, and norms for grievance redressal. Enhanced consumer awareness can ensure that users exercise the rights and options provided to them by the regulatory framework.

CHAPTER 1: INTRODUCTION

Promoting digital payments is a top priority for India since the demonetisation of currency notes in 2016. They enable transparency, reduce the cost of handling and storing cash, and allow a wider set of merchants and consumers to transact. Efforts to promote digital payments comprise technological innovation, regulatory changes, and financial assistance from the Union Government and the Central Bank (Table 1). The State's attempts to formalise the economy, such as the implementation of the Goods and Services Tax and Direct Benefit Transfers, have complemented these efforts. Digital transactions have increased at a CAGR of 61 percent and 19 percent, in terms of volume and value respectively, between FY 2014-15 and FY 2018-19[1]. In FY 2014-15, digital transactions were valued at 660 percent of GDP and in FY 2018-19, this number increased to 862 percent[2].

Table 1: Recent Policy and Regulatory Interventions

TOPIC	INTERVENING AUTHORITY	INTERVENTION
Acceptance of digital payments	Government of India	Budget FY 2020 mandated that merchants with turnover exceeding Rs. 50 crore must provide facilities to accept digital payments.[3]
	Government of India	Subsidised cost of accepting payments on UPI and Rupay through Merchant Discount Rate waivers.[4]
	Reserve Bank of India (RBI)	Announced a Payments Infrastructure Development Fund[5]
Digital Infrastructure	RBI	The RBI's Vision 2021 seeks to promote the development of low cost acceptance devices, and promote the use of Bharat QR.[6] The Report of the Committee on Analysis of QR codes has also recommended that interoperable QR codes such as Bharat QR and UPI QR should be promoted[6].
Consumer confidence	RBI	Notified reforms in grievance redressal such as Turn Around Time framework for grievance redressal to be implemented by Dec 31 2020.[7]
	RBI	Implemented Ombudsman Scheme for digital payments, banks and NBFCs.[8]
	RBI	Amplified consumer awareness and information initiatives.[9]

Security	Reserve Bank of India	Established explicit consent based function for card not present transactions[10]
	Reserve Bank of India	Announced the creation of a Central Payments Fraud Registry for tracking payment system frauds.[11]
	Reserve Bank of India	Facilitated tokenisation for storing customer data[12]

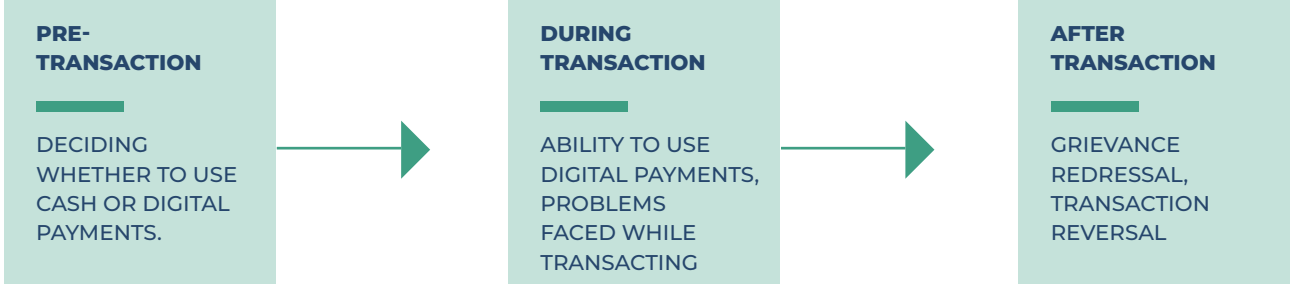
Despite the focus on progressing towards a "Less Cash Society", cash remains the dominant mode of transacting in India. 72 percent of transactions in November 2018 were done in cash[13]. In addition, instruments which can be used for both cash withdrawals and for digital transactions are used for the former more often than they are used for the latter. For example, in FY 2019, 62 percent of all debit card transactions were cash withdrawals[14]. In fact, cash in circulation in the Indian economy is currently at an all-time high. Bank notes in circulation in FY 2019-20 were valued at Rs. 21.1 trillion, which is 28.59 percent higher than in FY 2016-17[15]. Thus, the increasing use of digital payments co-exists with persistently high cash usage in the Indian economy.

Studies have attributed this to multiple factors, which include deficiencies in digital infrastructure, low user confidence, low digital literacy, low levels of acceptance of digital payments, and security-related concerns[16]. Improvements in cost, infrastructure, and security are easy to discern, but convenience and confidence are intangible constructs that are inextricably linked to user experience. However, they are among the most important factors to consistently enhance digital payments usage in India. If users are unconvinced about the benefits that digital payments offer, or do not trust digital transactions, improvements in other aspects of digital payments will not help. The quality of experience depends on factors like safety, transparency, ease, cost, reliability, and privacy.

Promotional offers and demonetisation provided great impetus to adopt digital payments. Encouraging new users to continue using them entails ensuring that bad experiences do not prevent users from transacting in the future[17]. For example, victims of fraud or identity theft may not be comfortable using digital payments again. Similarly, people who are unable to recover their money after they cancel an order on an e-commerce platform, may always opt for "cash on delivery" in future. This is reiterated by the Committee on Analysis of QR Codes[18]- "Interactions and engagement create a kind of 'track record' with consumers, and repeated successful interactions build trust, which in turn helps to build habits."

The RBI announced its Payment and Settlement Systems Vision 2021, on May 15, 2019. It envisages improvements in competition, cost, convenience and confidence and plans to achieve these by December 2021. August 2020 marked the halfway-point for realising this vision, and at this juncture it is pertinent to assess user experience to inform policy and regulatory design in the future.

Figure 1: Elements of user experience while transacting



CHAPTER 2: USER CHARACTERISTICS

The survey results are based on 4,727 unique responses from cities across the North, South, East and West India. The majority of survey respondents were conversant with digital payments. The problems that these users face could be major impediments for others who do not have access to the same information, infrastructure, and technologies as them. Therefore, their experience is instructive for policy and regulatory design, at a step after inclusion and digital literacy. Some key characteristics of the survey are:

- The survey was conducted online, in the first phase of the Covid-19 pandemic in India, between April 23 to July 31, 2020
- It was conducted in English, Hindi written in Devanagari script, and Hindi written in Roman script, while a majority (96.2 percent) took the survey in English
- 95 percent of survey respondents reported using digital payments in the last three months;
- Approximately 79 percent of respondents were between 18-30 years in age, and approximately 97 percent were able to use digital payments without any assistance;
- Over half reported their monthly household income to be between Rs. 20,000 and Rs. 75,000 while around a third earned above Rs.75,000;
- Around 91 percent of the respondents reside in cities having population over 5 lakh persons (i.e. Tier X and Tier Y cities).

Figure 2: Age (% of respondents) (N = 4,727)

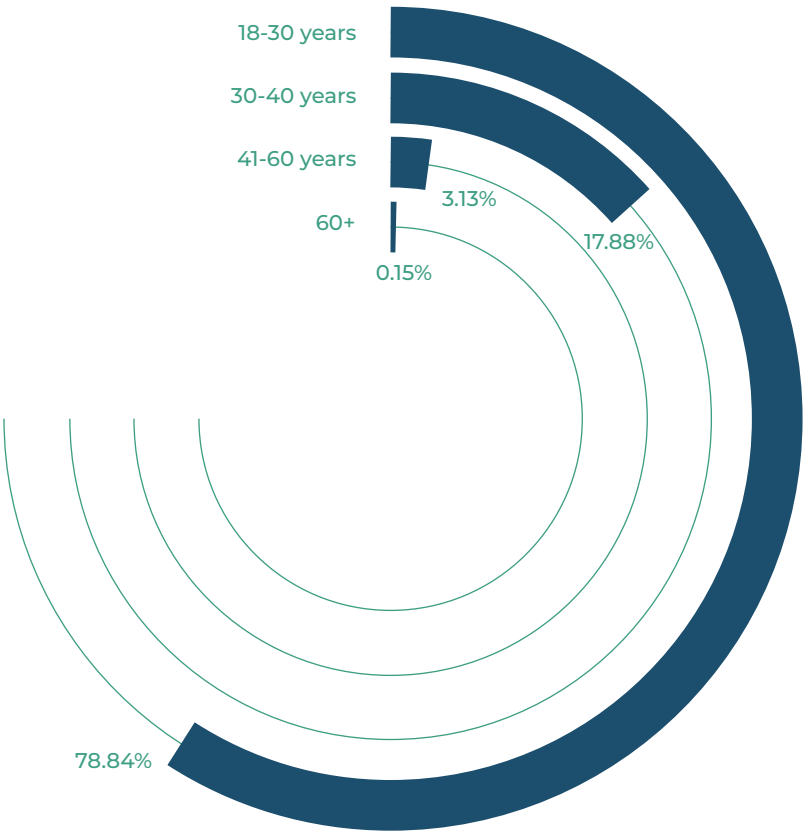


Figure 3: Monthly Household Income (% of respondents) (N = 4,726)

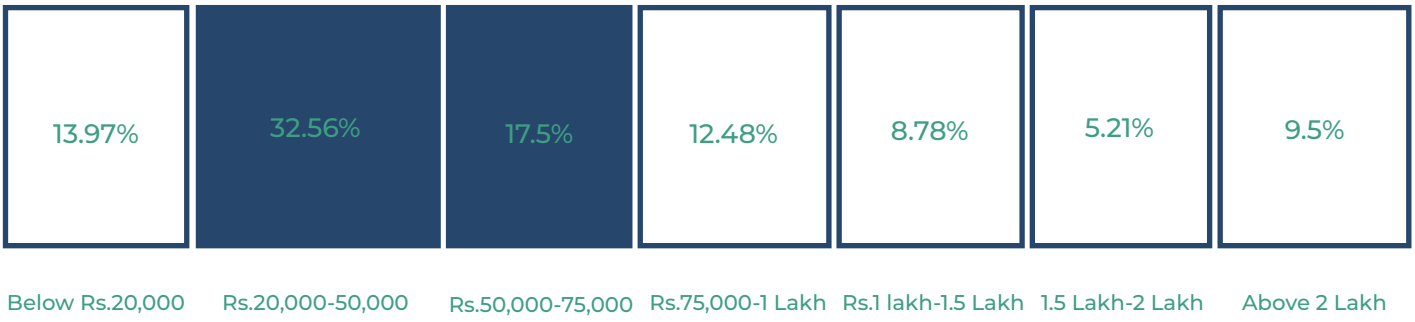
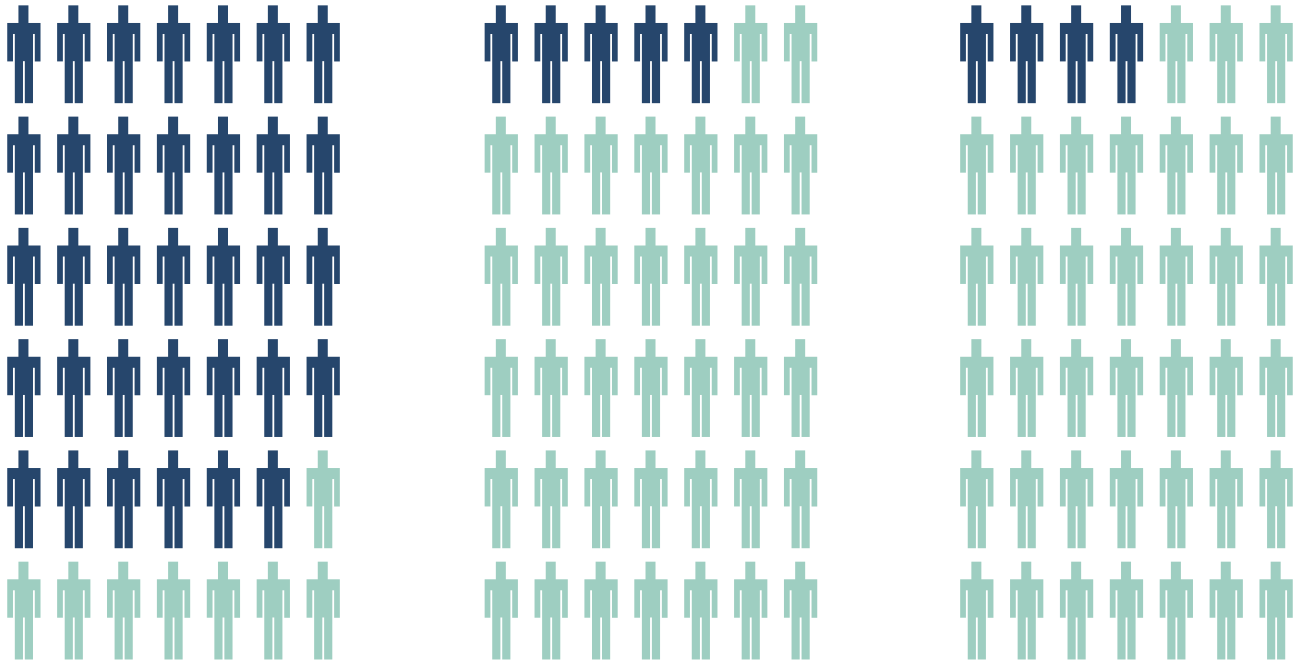


Figure 4: City Tier as per HRA Classification (% of respondents) (N =4,727)



79.82%

TIER X

11.17%

TIER X

9.01

TIER Z

The surveyed demographic is typically better informed about digital payments and their benefits relative to other groups. Illustratively, Bangalore, Hyderabad and Delhi accounted for over a third of digital payments to merchants in India between February 24, 2020 to April 23, 2020[19]. This is due to a combination of factors such as economic development and connectivity, the availability of digital infrastructure, and consumer awareness and preferences. For example, **digital infrastructure is much better developed in urban areas than in rural areas.** Urban tele-density was 140.06 percent as opposed to rural tele-density of 58.85 percent[20].

The majority of respondents took the survey in English, which increases the likelihood that they are able to use digital payment apps in the language. **English-speaking users can use a wider variety of digital applications, as digital payment services are not widely available in other Indian languages.**[21] In addition, **urban consumers are better informed about their rights and are better equipped to navigate grievance redressal processes.** For instance, in 2018-19, over three-fourths of complaints received by the Offices of the Banking Ombudsman were from metropolitan cities and other urban areas[22].

Figure 5: Purpose for using digital payments (% of respondents) (N=13087)

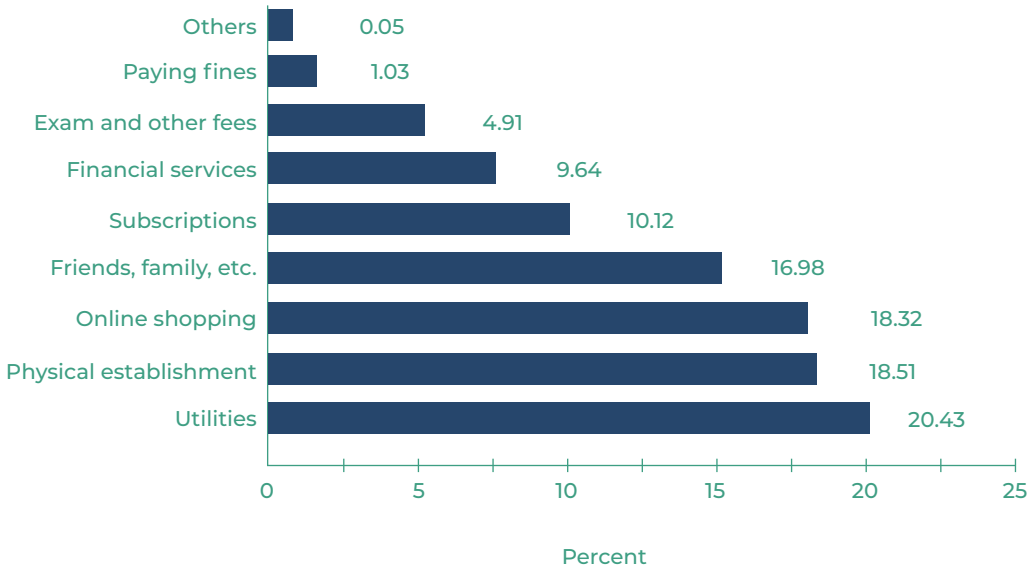
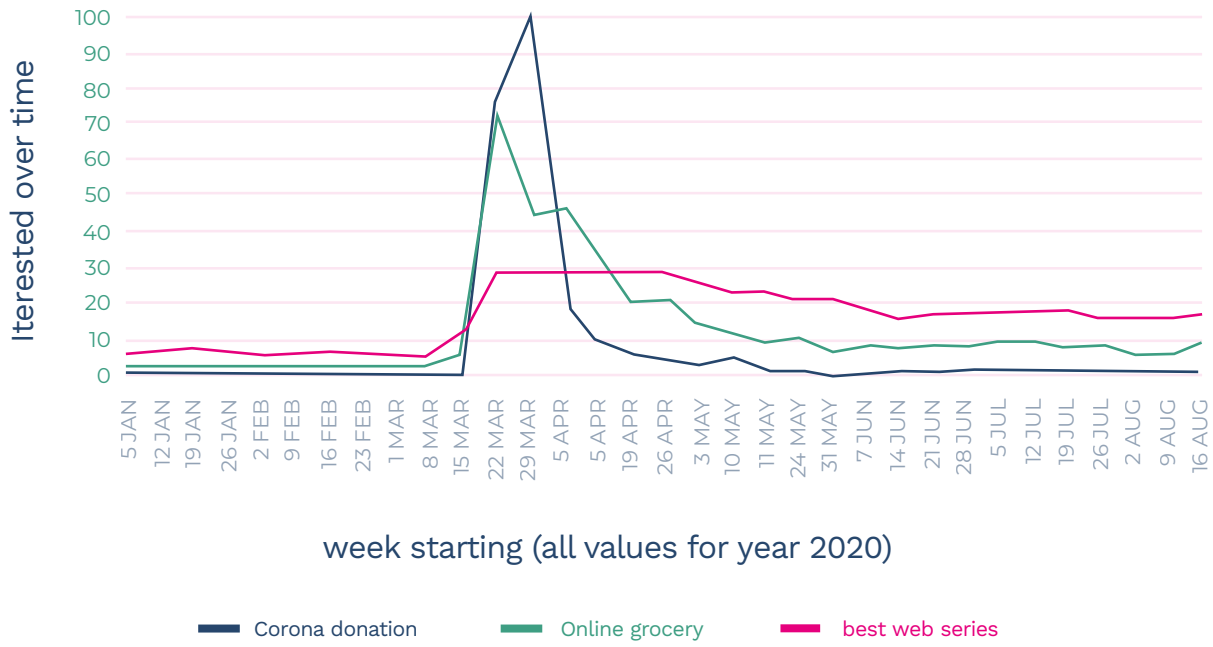


Figure 6: Google searches for online services

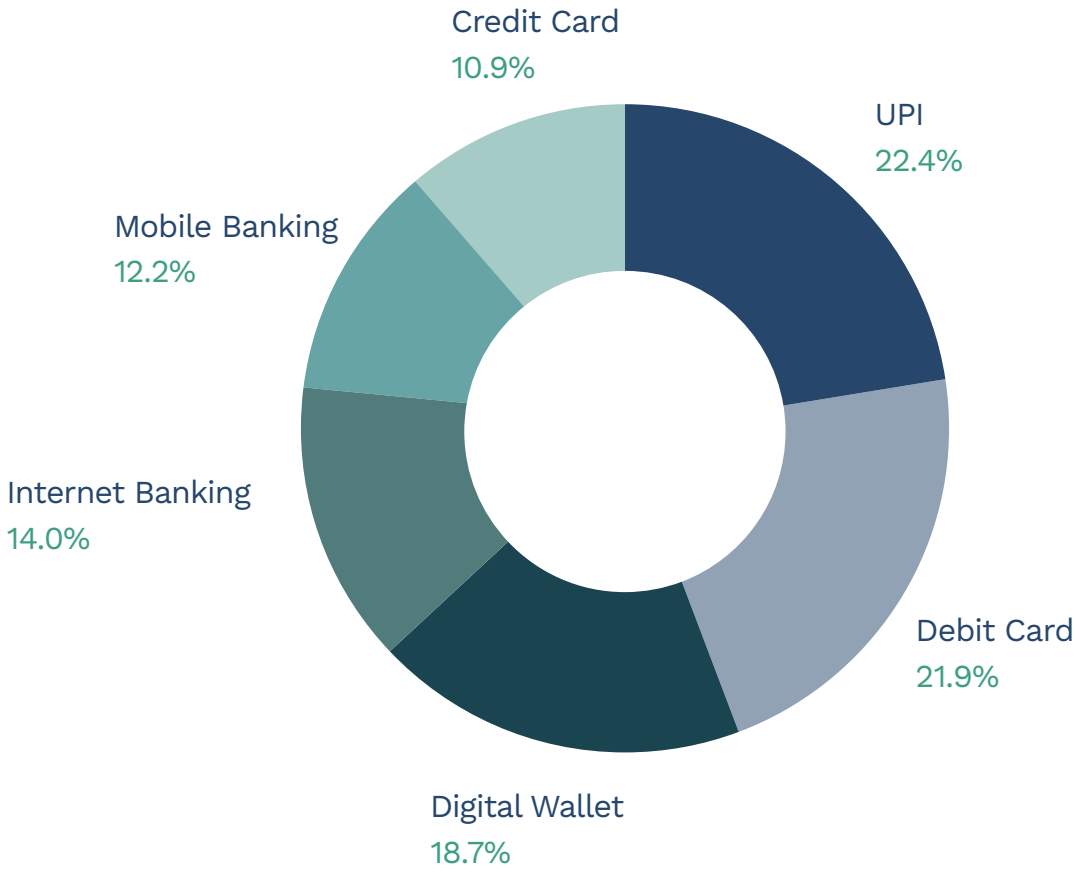


Source: Google Trends accessed on August 20.

In this survey, the most cited purpose for using digital payments was utility payments, while an equal share of respondents paid digitally for purchases at physical establishments or online. During the lockdown, consumers also paid digitally for things that they would have purchased in cash earlier. Figure 6 shows that Google searches for online services increased steeply during the week that the lockdown was announced. The value of transactions on the Bharat Bill Payment System, which enables digital payments for utilities, increased by 113 percent in July 2020 over the same month in the preceding year, and 89% over February.

2.1. SERVICES AND INSTRUMENTS USED

Figure 7: Digital payments instrument used



UPI, Debit Cards and Digital Wallets were the most commonly used instruments, and 64 percent of respondents used at least one of these in the last three months. This is consonant with the overall digital payments market in India. These three instruments facilitated 64.87 percent of digital payments during April - June 2020 in terms of volume and 2.78 percent in terms of value in the same period, according to the RBI[23]. In terms of value, transactions through the NEFT and RTGS payment systems account for the largest share of digital payments in India and are likely to constitute high-value business payments including payments to vendors and employees. Many high-value financial services are also facilitated by these modes. These transactions are usually conducted through mobile or internet banking (Table 2). Google Pay, Paytm and card networks Visa and Mastercard emerged as the services that respondents used most frequently.

Table 2: Instrument-wise Distribution of Digital Transactions in India (March - June 2020)

	BY VOLUME (IN LAKHS)				BY VALUE (IN RS. CRORES)			
PAYMENT SYSTEM INDICATORS	March 2020	April 2020	May 2020	June 2020	March 2020	April 2020	May 2020	June 2020
CREDIT CARD	1638.57	768.53	1028.86	1248.55	50574	20765	32225	42773
INTERNET BANKING*	2530.82	1597.63	2003.48	2431.49	3420971	2246296	2478416	3123215
DIGITAL WALLET	3178.6	1841.26	2532.2	2905.67	13111	8693	11080	12132
DEBIT CARD	3716.28	2095.3	2723.3	3090.54	65303	29043	48049	62494
UPI	12468.45	9995.74	12344.96	13369.31	206462	151141	218391	261835
MOBILE BANKING **	13830.33	11276.04	14622.03	16188	520199	364031	485513	599381

Source: RBI Bulletin dated August 13, 2020. Note: *includes only e-commerce transactions through 'net banking' and any financial transaction using internet banking website of the bank; **includes transactions done through mobile apps of banks and UPI apps.

Figure 8: Services used most frequently in last 3 months

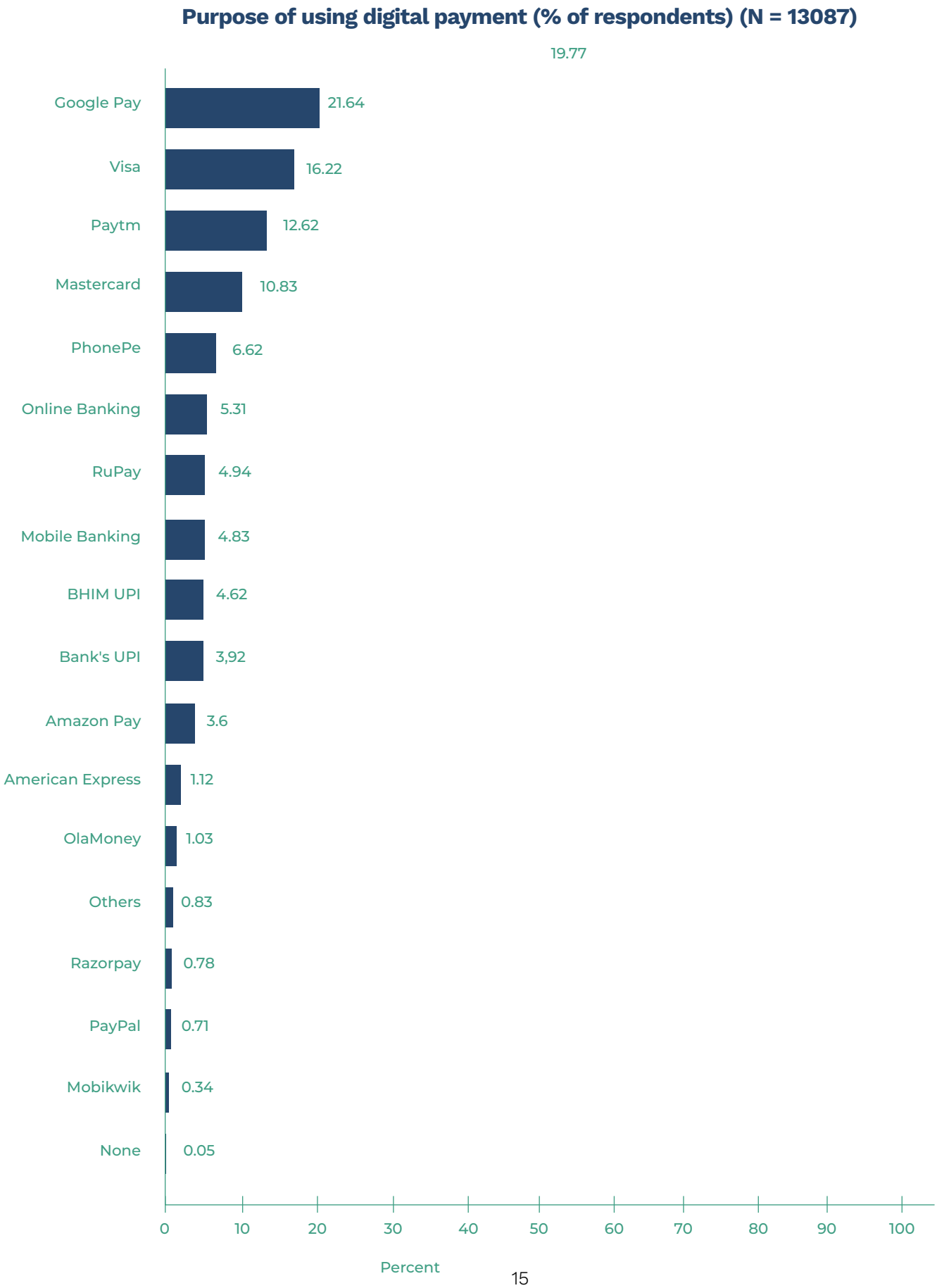
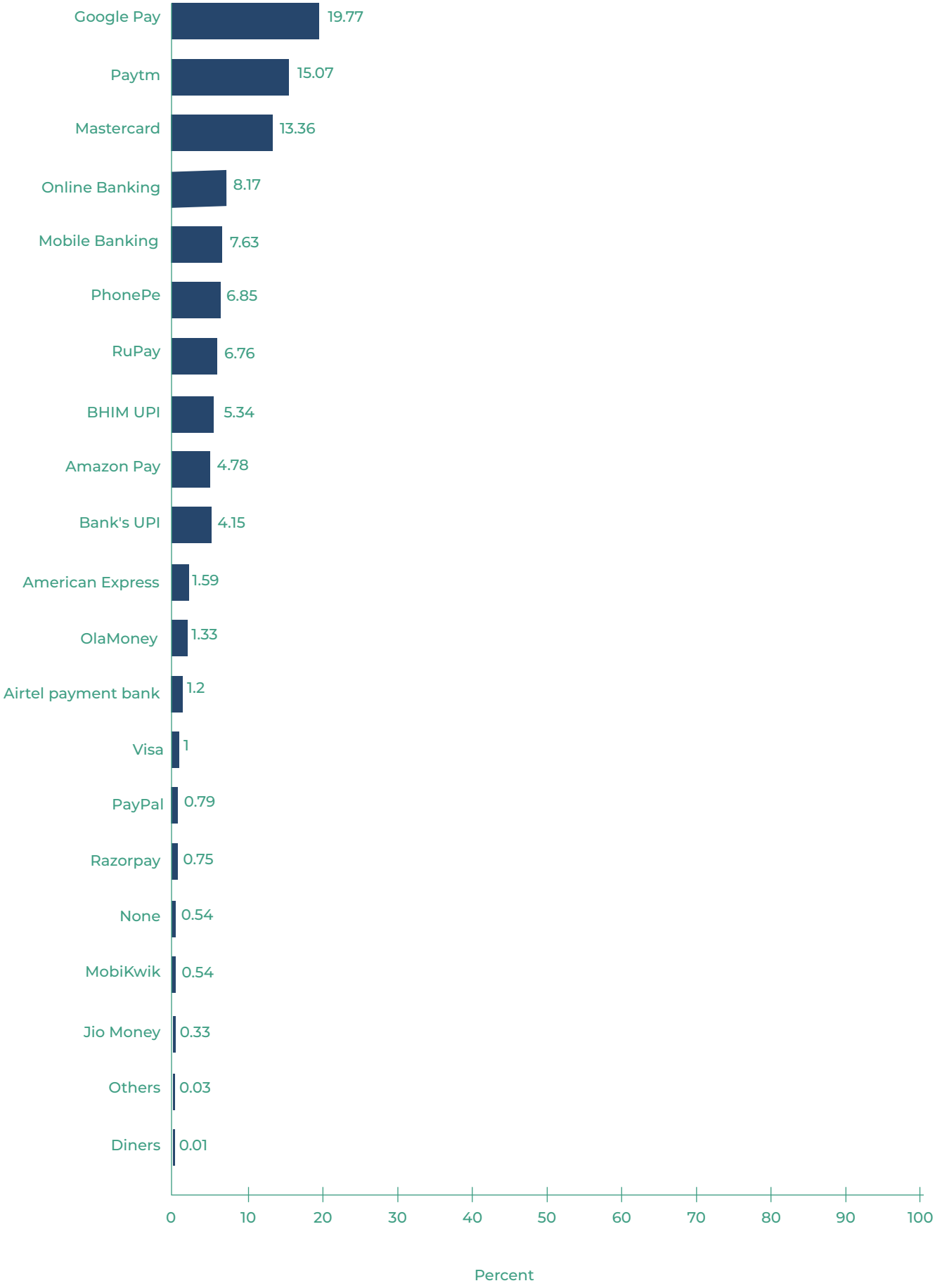


Figure 9: Other services used in the last 3 months

(% of respondents) (N = 6671)



CHAPTER 3: USER PREFERENCES FOR TRANSACTING DIGITALLY

To deepen the digital payments market, users must be confident that the safety, reliability and convenience of these instruments is higher than cash. Therefore, it is imperative to understand the factors that users consider when they have to choose between cash and digital transactions. This can help identify those aspects of digital payments that should be improved. Most survey respondents considered three factors while transacting: basic requirements to transact, privacy, and security. The survey also asked respondents if they faced situations which forced them to prioritise specific factors over others[24]. Over two-thirds reported facing such trade-offs, which means that there is scope to improve users' experiences such that they are more confident to transact digitally.

Most respondents were concerned about fulfilling the basic requirements to transact, privacy, security, and convenience. Each of these are discussed in greater detail below.

3.1 BASIC REQUIREMENTS TO TRANSACT

A transaction between two parties is possible only if both use the same medium. The lack of these can dissuade consumers and be a serious impediment to a smooth user experience. 16.77 percent of respondents reported that they had decided not to buy something because they could not pay for it using their preferred mode of payment.

For cash transactions, both parties must have currency of the required denomination. Due to the high level of cash circulation in the Indian economy, it is usually straightforward to fulfil this requirement. For transacting digitally, it is important that both parties use the same payment system, and have the necessary digital infrastructure, such as an internet connection, to transact. For example, users can only pay for groceries using UPI if the

Figure 10: Factors that consumers care about when transacting (%)

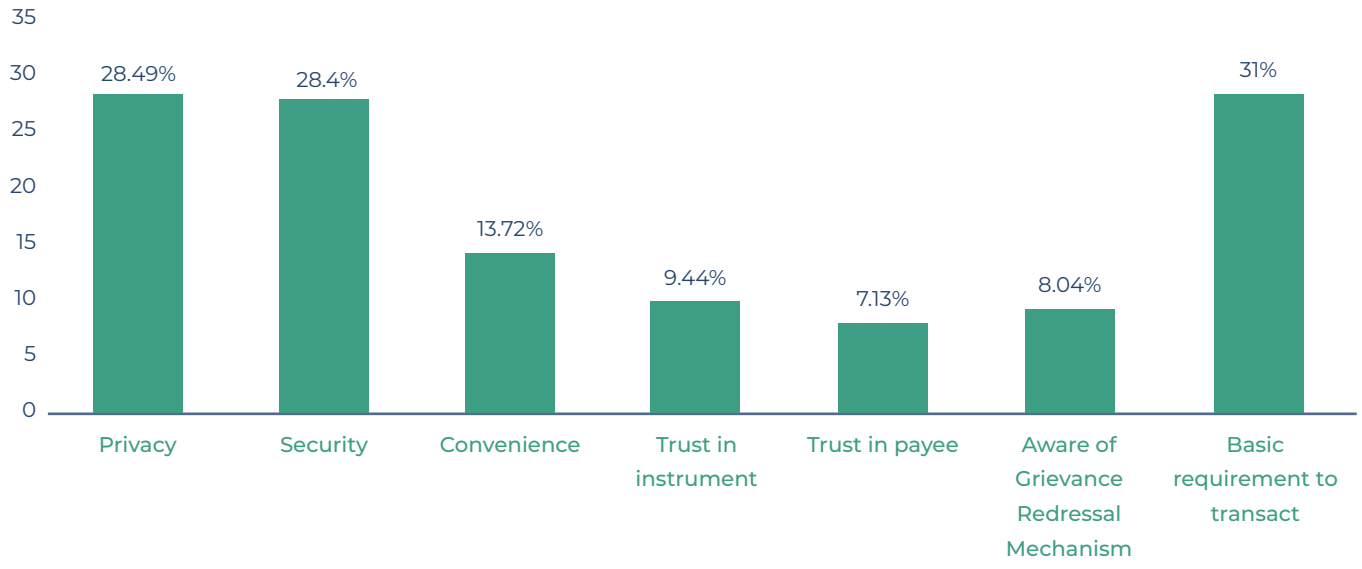


Table 3: Reasons for low acceptance of digital payments in India

STUDY	TIME PERIOD AND METHODOLOGY	REASONS IDENTIFIED
RBI's High-Level Committee on deepening digital payments[25]	Based on secondary research and stakeholder representations in 2019.	Low variety of financial services available on the acceptance side and high costs associated with it.
Centre for Effective Global Action, University of California[26]	Survey of 1,003 merchants in Jaipur conducted in August – September 2017.	Demand side factors, such as low confidence that consumers will use digital payments or fears about digital transactions increasing tax liability.
IFMR Lead[27]	Survey of 547 merchants from Jaipur, Kanpur, Indore, Nagpur and Surat in May-June 2017.	Low awareness of modern digital payments techniques such as internet banking and mobile banking relative to cards. Those who are aware of these methods do not use digital transaction platforms because they do not trust these, are unable to use them, fear having to pay higher taxes, and wish to avoid security threats.
CUTS CCIER[28]	800 merchants from Madhya Pradesh, Haryana, Karnataka, Bihar, Assam in January-March 2018.	Lower failure rates, acceptance infrastructure incentives for all stakeholders in acceptance infrastructure value chain, increased awareness and better security are required

merchant also uses UPI, and they can only pay using cards if the payee has a functional PoS terminal. 31 percent of survey respondents were concerned about whether these basic requirements will be fulfilled, which points towards low digital payments acceptance. This is corroborated by the fact that 18.01 percent of respondents used cash even when it was inconvenient to do so. Low acceptance can be a major source of friction which dissuades users from transacting digitally. Table 3 summarises findings from other sources about the reasons for low digital payments acceptance in India.

3.2 PRIVACY AND SECURITY

Privacy and security are the most important aspect to engender trust in digital transactions. It is important for users to be assured that they will not lose money while transacting, and that they are not at risk of identity or data theft. Around 28-29 percent of respondents considered privacy and security before they decided if they should transact digitally. This included access to a private internet connection, the use of cash for anonymity, and apprehensions about losing money.

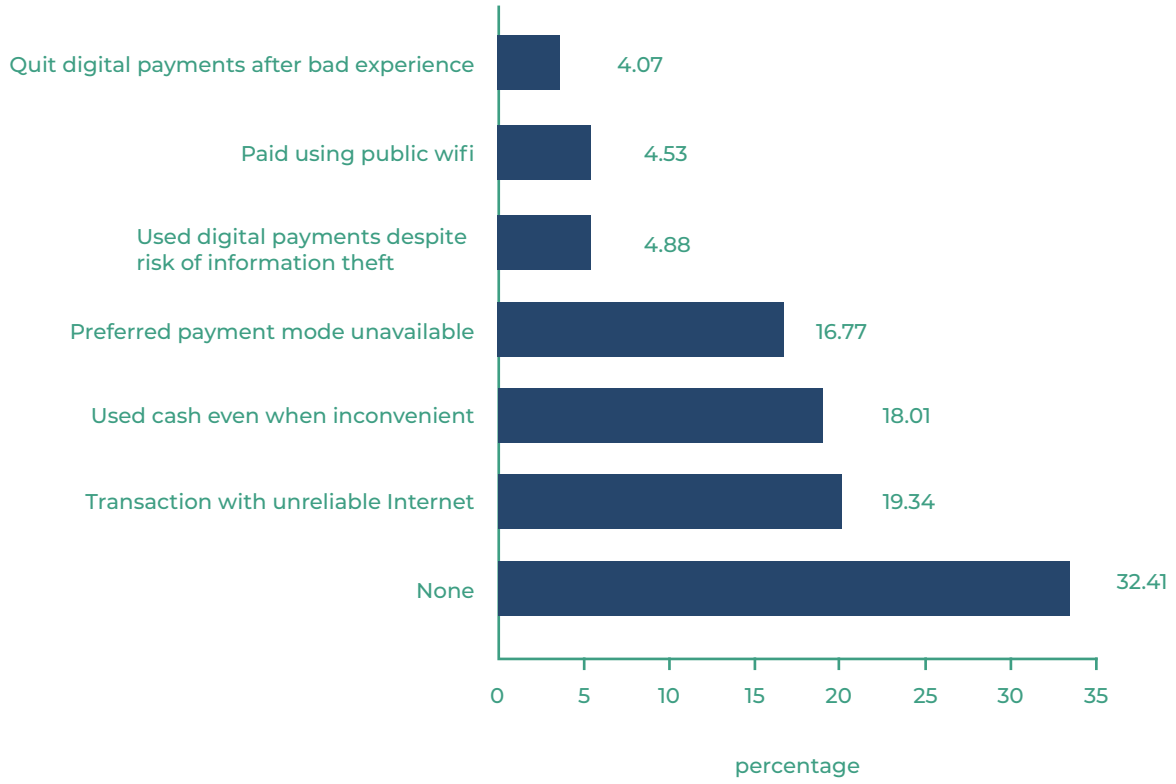
Less than 5 percent of respondents reported transacting digitally when there was a risk of information theft or making payments over public wi-fi. In fact, over 12 percent of respondents reported using cash when they did not trust the digital payment instruments that the payee accepts, or when the terms of using digital payments were not clear.

An increase in consumer awareness, to clarify misconceptions and empower them with information about how they can prevent phishing and fraud, can help engender trust. Terms and conditions which are easy to understand, reliable grievance redressal and transaction reversal mechanisms can also enhance consumer confidence. If users are assured of fast and satisfactory grievance redressal, they will be more confident to transact digitally, even if it entails risks such as transaction failure.

3.3 CONVENIENCE

Once consumers are assured about their privacy and security, they consider how convenient it would be to transact digitally or in cash. This includes factors such as the difficulty of transacting in cash, or a discount for digital payments. Therefore, it is important to design a high quality experience to convince users to transact digitally. The key aspects for such design are greater digital payments acceptance, security, privacy, and convenience. 4.07 percent of consumers were dissuaded from transacting digitally because they had a bad experience. Such instances can be avoided by improving user interface, making grievance redressal more accessible and ensuring timely fund reversal.

Figure 11: Trade offs faced



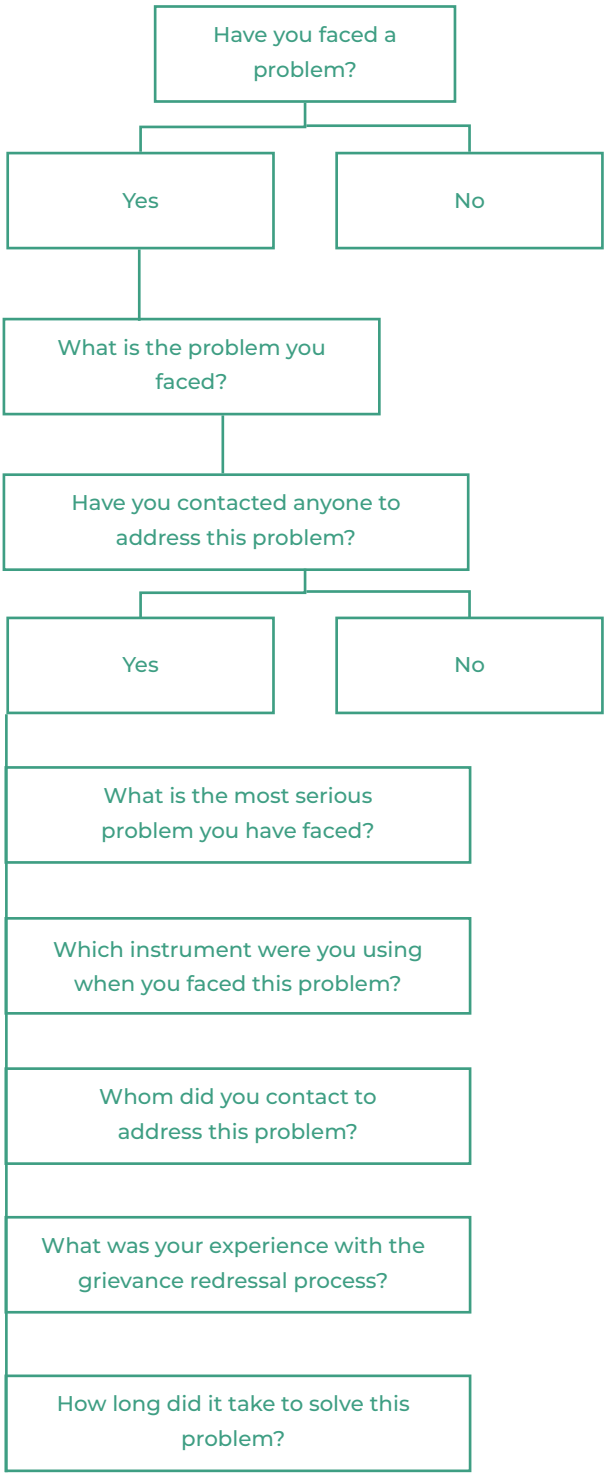
CHAPTER 4: QUALITY OF SERVICE CHALLENGES

The RBI's Ombudsman Scheme for Digital Payments, introduced in January 2019, records complaints related to digital payments to help provide recourse to consumers if they face difficulties while transacting digitally. In 2018-19, the number of complaints received on account of digital transactions increased by 41 percent over the previous year[29]. To address problems that users face when transacting digitally, entails understanding their nature, frequency, and severity.

The survey asked a more limited set of respondents if they had faced problems while using digital payments and what these were. 2,531 respondents answered these questions, of which approximately 40 percent reported facing problems while using digital payments in the last three months. Subsequently, the survey asked respondents about the most serious payments-related problem they have faced and for which they required grievance redressal. 496 respondents answered these questions related to their grievance redressal experience. Another survey, on a larger sample size, may be conducted based on these responses, with refinements to the questionnaire.

The following sections detail survey responses about the problems that users faced while using digital payments and their experiences with the grievance redressal process.

Figure 12: Questions asked about experience using digital payments

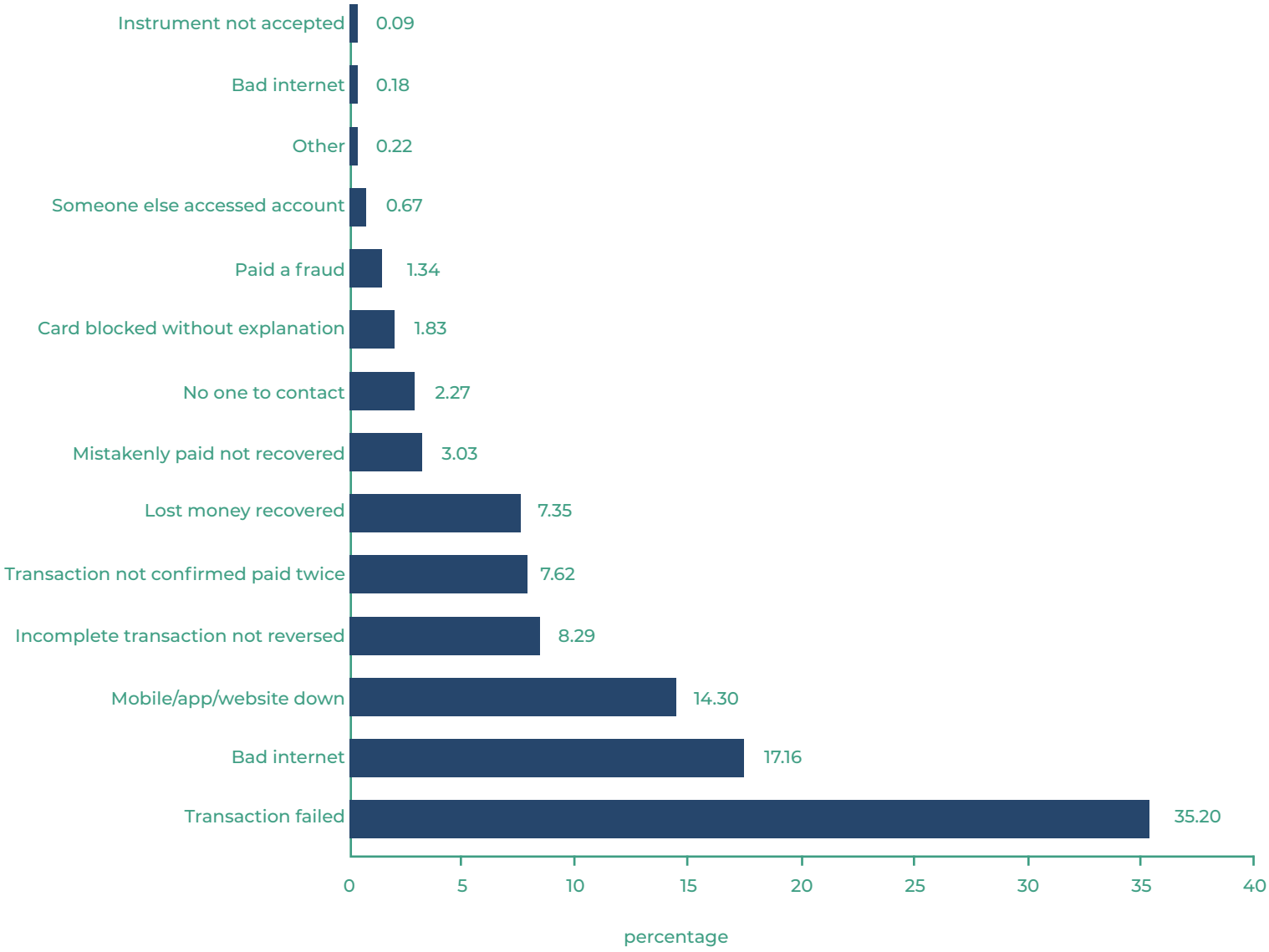


4.1 LAPSES IN RELIABILITY AND REVERSIBILITY IMPEDE USER TRUST

Reliability: Transaction failure and network-related problems emerged as the most common problems faced while transacting digitally. These make consumers uncertain about whether to transact digitally. A few related findings were:

Figure 13: Problems faced in using digital payments

(% of respondents) (N = 2244)



- 45.47 percent of respondents, who contacted someone to address their complaints, said transaction failure was the most serious problem they had faced;
- This problem was most common among mobile banking users (54.17 percent of total such users), digital wallet users (48.59 percent) and UPI users (49.1 percent);
- Of respondents who reported using cash even when inconvenient, 62.65 percent also reported facing transaction failures and network related problems.

Reversibility: At least 27.36 percent of respondents lost money while trying to transact digitally. This diminishes user trust, especially for groups who lost considerable amounts of money. UPI saw the highest share of respondents who incurred losses while transacting, followed by digital wallets and debit cards.

Table 4: Share of users who lost money while transacting (%)

Instrument	Share of users who lost money while transacting (percent)
UPI	28.20
Digital Wallet	26.16
Debit Card	26.08
Mobile Banking	25.00
Internet banking	19.99
Credit Card	9.52

4.1.1 DIGITAL PAYMENTS FOR CASH WITHDRAWAL

Our survey did not evaluate user experiences while using digital payments for cash withdrawal, such as using ATMs or Aadhar-enabled Payment Systems (AePS). However, other reports suggest that transactions using these modes are fraught with the same problems, especially transaction failure.

AePS:

The number of transactions on AePS have increased manifold since April 2020. This can be attributed to transfers to over 33 crore beneficiaries under the PM Gareeb Kalyan Yojana and disruptions to other modes of cash supply during the lockdown. Reports by Dvara Research and Indian School of Business recognise that transaction failure on AePS occurs most commonly due to biometric mismatch or other technological difficulties[30]. A report by Advait Rao Palepu also suggests that, although wrongful debits are required to be reversed within two days, paucity of staff at bank branches has extended the time required for transaction reversal to 15-20 days[31].

ATMs:

Complaints related to debit cards and ATMs accounted for the second highest number of complaints received under the RBI's Banking Ombudsman Scheme. The following table shows that most complaints received about ATMs/Debit Cards were related to cash withdrawals.

Table 5: Complaints related to ATM/Debit Cards received by the RBI Ombudsman

	No of Complaints	
Sub Category	**2017-18**	**2018-19**
Non-Payment of Cash / Account Debited but Cash not Dispensed by ATMs*	14,691 (8.98%)	19,366 (9.89%)
Use of Stolen / Cloned Cards	2117 (1.29%)	4,961 (2.53%)
*Debit in account without use of the card or details of the card	2,356 (1.4%)	4,481 (2.3%)
*Account Debited More than Once for One Withdrawal in ATMs or for POS Transaction	965 (0.59%)	1,288 (0.66%)
Short Payment of Cash / *Less or Excess amount of Cash Dispensed by ATMs	1,166 (0.71%)	1,186 (0.61%)
Others	3,377 (2.06%)	5,257 (2.68%)
Sub-Total	**24,672 (15.08%)**	**36,539 (18.65%)**
Total No. of Complaints Received	**1,63,590**	**1,95,901**

4.2 GRIEVANCE REDRESSAL PROCESS

Consumers' aversion to use digital payments may be exacerbated by a cumbersome or unsatisfactory grievance redressal experience. This is especially true when respondents lose money trying to transact online and are unable to recover it. According to the Report of the RBI's High Level Committee on Deepening Digital Payments, a reliable grievance redressal mechanism complements low error rates in increasing consumer confidence. Our survey results suggest that there is scope for improvement in the grievance redressal process for many instruments. They point towards the need for uniformity in the redressal experience across authorities that users may contact for grievance redressal, such as the bank, police, or the payee:

4.2.1 GRIEVANCE REDRESSAL IS USUALLY TIMELY BUT NOT SATISFACTORY

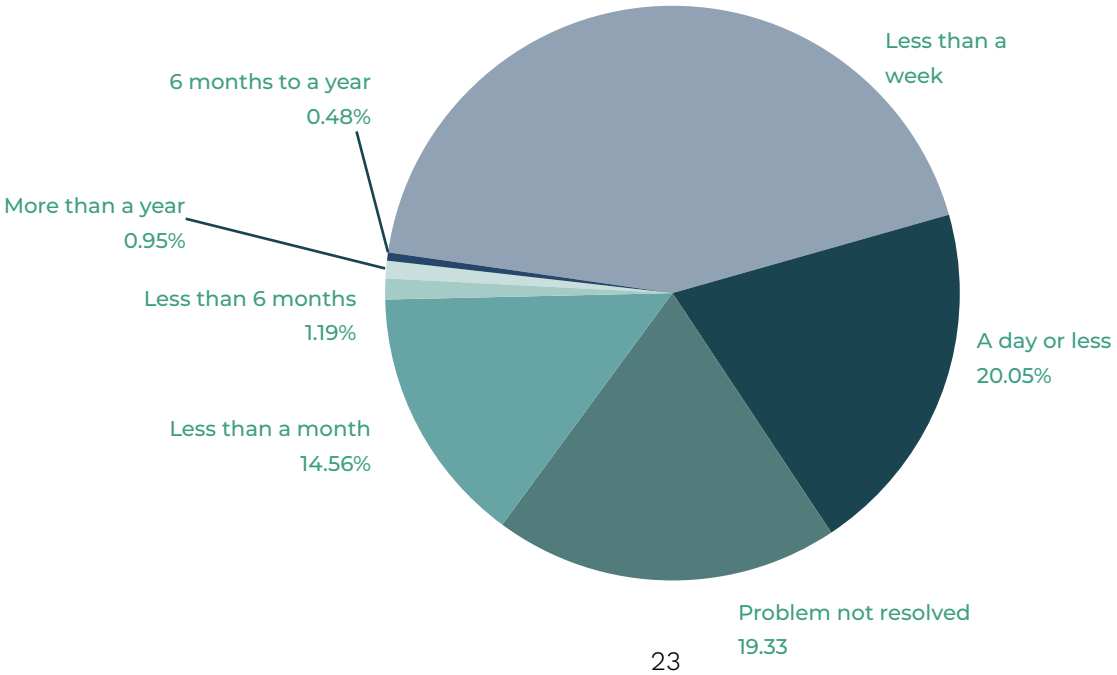
- Approximately 48 percent respondents had a negative experience in the grievance redressal process;
- The most common negative experiences were receiving inadequate explanations (21.7 percent), money not returned (21.1 percent), process too cumbersome (19.94 percent), unsatisfactory resolution (19.65 percent);
- 63.65 percent of the issues were resolved within a week irrespective of the problem instrument.

4.2.2 USERS ARE NOT SATISFIED WITH THE GRIEVANCE REDRESSAL PROCESS FOR THE MOST USED INSTRUMENTS

- Among those who had a negative grievance redressal experience, the majority used UPI (45.16 percent) and Digital Wallets (24.34 percent);
- Digital Wallets had the highest share (21.51 percent) of respondents who faced problems that were not resolved, followed by Internet Banking (20 percent) and UPI (19.15 percent);
- Internet banking had the highest share of respondents (14.8 percent) who found the grievance redressal process to be too cumbersome, followed by mobile banking and UPI users.

Figure 14: Time taken for grievance redressal process

(% of respondents) (N = 419)



4.2.3 THERE IS GREAT VARIANCE IN THE QUALITY OF GRIEVANCE REDRESSAL ACROSS PARTIES CONTACTED

- In context of the most serious payments-related problem that they had faced in the last three months, 41.28 percent of respondents contacted the payment service provider, 24.16 percent contacted the concerned e-commerce platform, and 22.88 percent contacted a bank;
- In case of transaction failure, the most common problem respondents faced, the majority (54.11 percent) contacted the payment service provider;
- None of the respondents who contacted the Police, the RBI or trusted lawyers/ CAs were able to recover money they had lost. Less than one percent of respondents contacted either the RBI or trusted lawyers/CAs, whereas 2.08 percent contacted the police.
- E-commerce platforms had the lowest share of complainants who thought the process was too cumbersome, whereas the Police had the highest share of such complainants (Table 4)
- Of respondents whose problems had not been resolved yet, 41.38 percent contacted payment service providers, 20.69 percent contacted banks, and 19.83 percent contacted e-commerce platforms. However, the share of problems that were not resolved is quite low for these parties, which probably indicates that unresolved complaints constitute those that have been raised recently. Out of the complaints that these parties received, only 19.35 percent were not resolved for payment service providers, 15.65 percent for e-commerce platforms and 17.78 percent for banks.

Figure 15: Party contacted for grievance redressal

(% of respondents) (N = 625)

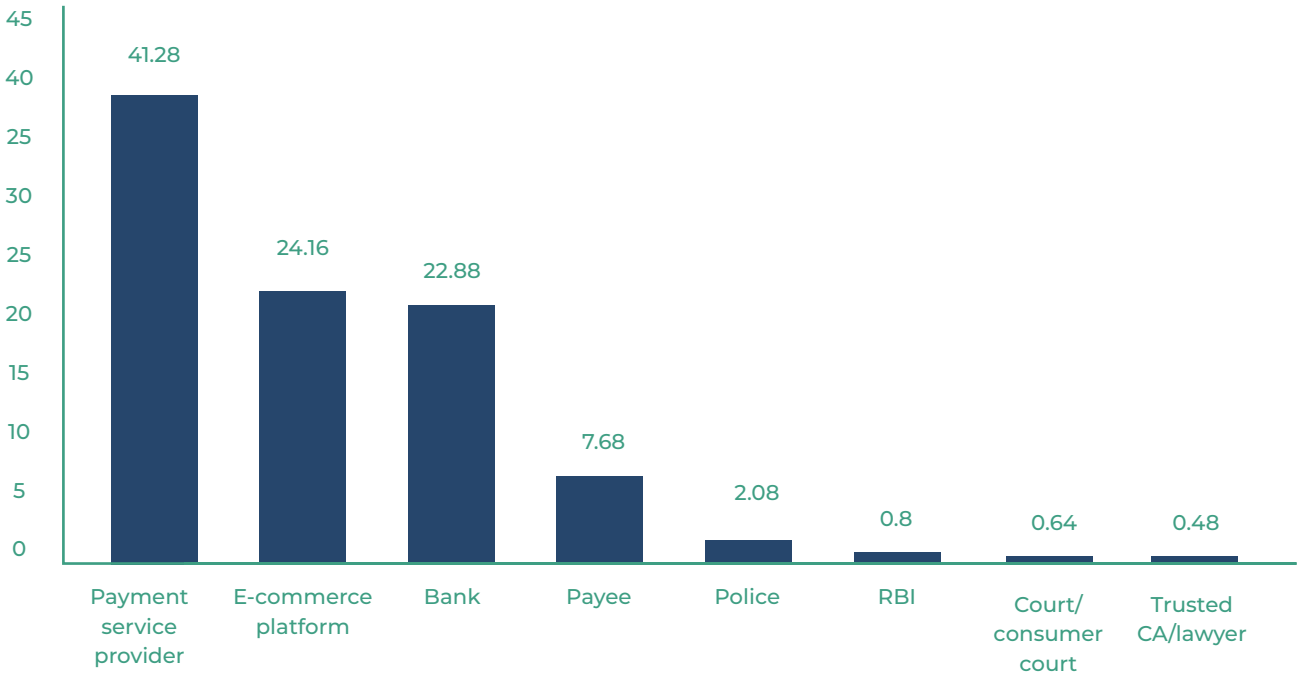


Table 6: Grievance Redressal Experience as share of Party Contacted for Grievance Redressal (percent)

Experience with grievance redressal process	Bank	Court/ Consumer Court	E-com-merce Platform	Payee	Payment Service Provider	Police	RBI	Trusted CA/ Lawyer	Total
Money returned	37.96	50.00	53.19	25.81	39.91	0.00	0.00	0.00	**41.54**
Satisfactory resolution	25.93	0.00	12.06	19.35	20.18	0.00	0.00	0.00	**18.65**
Money not returned	8.33	0.00	14.18	9.68	15.35	12.50	0.00	0.00	**13.08**
Inadequate explanation	11.11	0.00	9.22	6.45	10.09	12.50	0.00	0.00	**9.81**
Unsatisfactory resolution	6.48	0.00	2.84	12.90	7.89	12.50	0.00	0.00	**6.54**
Too cumbersome	5.56	0.00	2.84	12.90	4.39	62.50	0.00	0.00	**5.58**
Deemed resolved without adequate resolution	0.93	50.00	3.55	6.45	1.32	0.00	100	100.00	**2.69**
Told to contact correct party	1.85	0.00	1.42	0.00	0.88	0.00	0.00	0.00	**1.15**
Complaint escalated	0.93	0.00	0.71	6.45	0.00	0.00	0.00	0.00	**0.77**
Adequate explanation	0.93	0.00	0.00	0.00	0.00	0.00	0.00	0.00	**0.19**
Total	**100**	**100**	**100**	**100**	**100**	**100**	**100**	**100**	**100**

4.3 FACTORS TO ENCOURAGE DIGITAL PAYMENTS USAGE

Evidently, consumers look for a safe and reliable experience while transacting digitally. When asked about the changes that would encourage respondents to use digital payments more often, 36.93 percent requested a trustworthy reversal process and more reliable grievance redressal mechanism. This indicates that users are willing to tolerate problems while transacting digitally, if they can be assured of timely and satisfactory redressal. Hence, the reversal and redressal process emerge as key pillars to strengthen user trust.

These priorities are shared by both, users and non-users of digital payments. Of respondents who had not used digital payments in the three months preceding the survey, 20.28 percent opined that a trustworthy reversal process would encourage them to use digital payments more often. Approximately 17 percent of respondents requested each of the following: easier terms and conditions and procedure to use digital payments, a reliable grievance redressal mechanism and a better internet connection. Respondents who quit the use of digital payments after a bad experience, said that they would be encouraged to resume if they were easier to use and the transaction reversal process was trustworthy.

CHAPTER 5: SUMMARY AND RECOMMENDATIONS

Digital payments adoption is growing in India and a wide variety of digital financial services are available for use. Events such as demonetisation and the COVID 19 pandemic have persuaded many users to experiment with these instruments. However, to ensure that digital adoption translates into consistent usage and a deeper market, it is important to design a high quality user experience. Users must be confident that they will be able to reliably complete a transaction, and that they have speedy and trustworthy recourse available if they face problems.

Our survey results indicate that users harbour apprehensions about prospective transaction experiences. Before deciding whether to transact in cash or digitally, they check if they meet the basic requirements necessary to do so (such as having an internet connection). Afterwards, they consider concerns about privacy, and security. There is considerable variation in the quality of consumer experience across instruments and the parties that they contact for grievance redressal. Current users and non-users agreed that trustworthy grievance redressal and transaction reversal mechanisms would encourage them to use digital payments more often. Regulatory interventions can help remedy lapses in service quality to ensure that users are confident about having a safe and trustworthy transaction experience.

Table 7: Problems digital payments users face and recommended remedies

THEME	PROBLEM	RECOMMENDATIONS
Reliability	Transaction failure and network related issues	Improve communication infrastructure, enhance user awareness, track and reduce technical declines
Reversal	People lose money while transacting digitally	Ensure effective implementation of TAT regulations, educate users about how to make and escalate complaints
Grievance redressal	Variation across instruments used and parties contacted for grievance redressal	Make grievance redressal mechanisms more accessible, analyse complaints to ombudsman to guide service providers to improve grievance redressal mechanisms
Security	Fraud and security risks	Institutional reform, incentivise reporting and disclosures

5.1 RELIABILITY

Survey results show that transaction failures and network-related problems are the hurdles that users face most often. The Report by the RBI High-Level Committee on Deepening Digital Payments notes that transaction failures cause poor consumer experiences, which sets back the adoption of digital payments.

Transaction failures may be attributed to technical or business declines. Business declines often occur at the consumer's end through errors such as maintaining an insufficient account balance. Better user awareness and easily navigable user interfaces could reduce the rate of business declines. For example, showing users a mini statement before they transact can be useful[32]. In addition, localised consumer engagement initiatives through consumer groups are important to understand users' problems and empower a network of local agents to educate users. The RBI's envisaged network of Centres for Financial Literacy in every block in the country can be leveraged for such engagement[33].

Technical declines refer to transaction failures that stem from issues in the payment system. These may be caused by poor internet and telecom infrastructure or issues with the payment system itself. Here, the High-level Committee proposed that participants in the digital payments ecosystem should develop a roadmap to reduce technical declines by 25% each year. The RBI has started to measure declines as part of the Digital Payments Index, but it has not set milestones for reducing these[34].

Transaction success rate and timely completion of transactions are a function of deploying correct technical standards. The International Telecommunications Union (ITU) lays down and defines technical standards for transaction success and completion rates for digital financial services[35]. Regulations can supplement this by prescribing a maximum time-limit for service providers to process transactions. This practice is recent and only implemented in two countries. In the UK, service providers are mandated to declare a time limit when onboarding customers[36] and Ghana has proposed a time limit for processing transactions in their draft Quality of Service Regulations.[37]

The Indian telecom industry provides an example of how such standards may be implemented. The country has a well-equipped feedback mechanism for the quality of voice calls and call drop rates. The Telecom Regulatory Authority of India (TRAI) prescribes Quality of Service standards and enforces them through a reporting and oversight mechanism. [38]

In addition, the improvement of communications infrastructure in the country is important to ensure that network coverage is stable for users to undertake OTP based transactions. It is also important to ensure that telecom infrastructure can withstand natural disasters and other emergency situations, where access to digital payments can be extremely useful. This is aligned with one of the three missions of the National Digital Communications Policy, 2018: to create robust digital communications infrastructure.

5.2 REVERSIBILITY

The impact of transaction failures on consumer trust may be mitigated if consumers are confident about transaction reversal. In the survey, at least 27 percent of respondents reported losing money while transacting digitally, which can be avoided if there are reliable reversal mechanisms that users can access. It is imperative to create a standardised and predictable reversal procedure to retain user trust.

The RBI has taken a positive step in this direction by publishing the 'Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems'. [39] Among other things, the TAT framework defines a 'failed transaction' and lays down a framework for auto-reversal and compensation. If Authorized Payment System Operators do not address grievances as prescribed under TAT, a user

may approach the Banking Ombudsman of the Reserve Bank of India. The framework is due to be implemented by December 31, 2020. It is important to ensure that it is effectively implemented and that all service providers comply with it. Large scale consumer education, to ensure that users complain if their transactions are not reversed in the stipulated time, is essential.

5.3 GRIEVANCE REDRESSAL

The survey also reveals that close to half of the respondents had a disappointing experience with the grievance redressal process. The most common were receiving an inadequate explanation, money not returned, finding the process too cumbersome, and unsatisfactory resolution. Additionally, the survey results also highlight the lack of standardization in the grievance redressal mechanism.

Grievance redressal mechanisms provide a feedback loop for both service providers and the regulatory authority. For better enforcement, it is important to provide a statutory basis for any obligation to maintain a grievance redressal mechanism. Countries achieve this by legally mandating operators to create their own procedures and rules for setting up a grievance redressal mechanism. The RBI has mandated various payment systems to have grievance redressal mechanisms[40]. It has also mandated Payment Service Operators to institute an Online Dispute Resolution mechanism for failed transactions. In some countries including India, this is supplemented by an ombudsman. A few countries also mandate a maximum time limit for addressing grievances.

In India, grievance redressal mechanisms should be simplified to make them more accessible to all users, especially for new ones. Overcoming language and digital literacy barriers are also important to ensure participation from a wider audience. In addition, the regulator may ask service providers to publish data on the complaints they received and their responses to them. This can engender transparency, facilitate sharing of best practices, and catalyse greater competition among service providers. India has also set up the Digital Payments Ombudsman to address customer grievances that have not been satisfactorily resolved by service providers. Complaints to the Ombudsman should be analysed to identify common and serious lapses in the service providers' grievance redressal processes. They should then be guided to implement necessary reforms or meet specified standards.

For complaints to reflect user experiences accurately and for the scheme's effective implementation, it is important that users from every demographic group are made aware of its provisions and how they can complain to the Ombudsman. For instance, only 24% of the complaints to the Banking Ombudsman in 2018-19 were from rural and semi-urban areas[41].The RBI has started measuring 'consumer awareness and education in the Digital Payments Index. It should also use this data to evaluate the success of its interventions in this regard[42].

5.4 SECURITY

Our survey shows that consumer trust depends on platform and transaction security to a large extent. The role of fraud prevention in improving consumer trust is also highlighted in the Report of the High Level Committee. There is a high incidence of cyber attacks in India, aggravating this relationship between consumer trust and fraud. The country sees more data breaches than the global average, according to the Thales Data Threats Report[43]. Indian financial systems are particularly vulnerable to cyber attacks[44]. To solve this, India needs a robust mechanism for threat detection and risk mitigation. The government has taken positive measures such as the Frauds – Classification and Reporting Framework under the RBI and the National Cyber Crime Reporting Portal under the Ministry of Home Affairs. The MHA Portal provides an avenue for victims/complainants of financial fraud register a criminal complaint. The RBI has also proposed to set common minimum security standards for different digital payments systems. However, other novel measures, such as the

establishment of a specialised emergency response team for financial systems, remain in the pipeline. The Information Technology Act, 2000 created the Computer Emergency Response Team (CERT-In), India's nodal agency for cyber incident response[45]. CERT-In's functions include anticipating cybersecurity risks, alerting the concerned authorities and preparing risk-mitigation strategies. For this, they issue advisories, whitepapers, guidelines, annual reports etc[46]. In 2017, a government report outlined the need for a specialised CERT for the financial sector (CERT-Fin). The body will have sub-sectoral CERTs under each financial regulator, according to the Report by the Working Group on CERT-Fin. The CERT-Fin under the RBI would coordinate with CERT-In, the National Critical Information Infrastructure Protection Centre and a proposed CERT for telecom to secure the digital payments ecosystem. India must set-up CERT-Fin and a sub-sector CERT for digital payments in an expedient manner. This will help coordinate mitigation efforts in the face of a security threat. In the US, the Department of Homeland Security works closely with local governments and has formal information sharing arrangements between some states[47]. Further, incentives such as liability reduction when incidents are reported and other related information should also be offered to stakeholders. In other countries such as the US[48] and China, the government/regulator maintains centralised information sharing platforms so that incidents can be reported anonymously. The 2015 US Cyber-Security and Information-Sharing framework provides incentives including liability protection for voluntary disclosure by service providers, which other stakeholders can monitor to improve awareness about risks. China and Singapore also conduct emergency response drills to enhance awareness among digital payments providers. [49]

The following table provides a snapshot of best international practices against the principles highlighted above. A detailed table is annexed to this report. India can learn from these practices and adapt them to improve quality of service in the digital payments market.

Table 8: Principles and Best Practices in QoS Regulation[50]

PRINCIPLE	PRACTICE
Reliability	Ghana has proposed a maximum duration of less than 5 seconds in processing transactions in its QoS Regulations, 2019 published by the National Communications Authority (NCA).
Reversibility	In the United Kingdom, digital payment service providers are mandated to declare a maximum time-limit taken for a transaction at the time of onboarding customers. The UK law also allows consumers to apply for a refund within 8 weeks of a transaction, and the service provider is to either refund or provide reasons for refusal within 10 days. In the United States of America, service providers are mandated to ensure that system architecture enables recording information for post-transaction evaluation. The system should also enable a reversal mechanism if there is unauthorized access.

PRINCIPLE	PRACTICE
Grievance Redressal	In the USA[51], there is a mandate to develop and maintain written policies and procedures that are designed to ensure compliance with the error resolution requirements. The law also defines a maximum time for redressal as 10 business days under normal circumstances and 45 in case investigation is required. The Revised Directive on Payment Services (PSD2) obliges EU Member States to designate competent authorities to handle complaints from payment service users and other interested parties, such as consumer associations. Payment service providers should put in place a complaints procedure for consumers and prescribes an unconditional refund within 15 days.
Security	In the US and China, the government/regulator maintains centralised information sharing platforms for anonymous reporting of incidents and provides limited liability protection for incident reporting. PSD2 in the European Union obliges payment service providers to apply "strong customer authentication" (SCA). SCA is an authentication process that indicates whether the use of a payment instrument is authorised. Some EU countries have made it mandatory while some are prescribing it as voluntary. Many countries require a robust authentication mechanism for transactions. With respect to authentication standards, Europe, India, China, and Russia have country-specific standards while industry-supported standards (3D Secure 2.0, EMVCo) are the norm in other countries. In Japan, there is periodic inspection and vetting to prevent the inappropriate usage and leakage of consumer data.

ANNEXURE 1: SURVEY QUESTIONNAIRE

DEMOGRAPHIC CHARACTERISTICS

1. City (Drop down list)

2. Occupation:
- A. Self-employed
- B. Homemaker
- C. Jobseeker
- D. Student
- E. Full time worker
- F. Part time worker
- G. Freelancer
- H. Other _____

3. Household size (No. of members eating from the same kitchen for the last six months): (Drop down selection up to 10)

4. Monthly Household Income:
- A. Below 20,000
- B. 20,000-50,000
- C. 50,000-75,000
- D. 75,000- 1 lakh
- E. 1-1.5lakh
- F. 1.5-2 lakh
- G. Above 2 lakhs

5. Gender:
- A. Male
- B. Female
- C. Non-binary
- D. Prefer not to specify

6. Age:
- A. 18-21
- B. 21-24
- C. 25-30
- D. 31-35
- E. 36-40
- F. 41-50
- G. 51-60
- H. 60+

DIGITAL PAYMENTS USAGE

7. Have you used digital payments in the last three months?
- I. Yes
- J. No (jump to question 24)

8. Which of the following have you used in the last three months? (Tick all that apply)
- A. Debit card
- B. Credit card
- C. Internet Banking
- D. Mobile Banking
- E. Digital Wallet for eg. Paytm, OlaMoney, Amazon Pay
- F. UPI for eg. Google Pay, BHIM

9. Which of the following best describes your ability to use digital payments?
- A. I am able to use digital payments without any assistance
- B. I am able to use digital payments if assisted by someone
- C. I am unable to use digital payments (jump to question 24)

10. Which of the following services have you used the most frequently in the last three months? (Choose only one)
- A. Mastercard
- B. Visa
- C. RuPay
- D. American Express
- E. My bank's UPI service
- F. Google Pay
- G. BHIM UPI
- H. PayTM
- I. Amazon Pay
- J. PhonePe
- K. Mobikwik

L. Razorpay
M. Ola Money
N. Paypal
O. Airtel Payments Bank
P. Jio Money
Q. My bank's online banking service
R. My bank's mobile banking service
S. Other____

11. Other than the service chosen above, which services have you used in the last three months? (Choose up to two options)

A. Mastercard
B. Visa
C. RuPay
D. American Express
E. My bank's UPI service
F. Google Pay
G. BHIM UPI
H. PayTM
I. Amazon Pay
J. PhonePe
K. Mobikwik
L. Razorpay
M. Ola Money
N. Paypal
O. Airtel Payments Bank
P. Jio Money
Q. My bank's online banking service
R. My bank's mobile banking service
S. Other____

12. For what purpose have you used digital payments in the last three months? (Tick all that apply)

A. I have not used digital payments in the last three months
B. Paying friends, family, domestic helpers, technicians etc.
C. Paying for things I have purchased online, e.g metro recharge, cabs, movie tickets, goods purchased on e-commerce websites
D. Paying at physical establishments such as at grocery shops, restaurants, or malls
E. Paying for subscriptions eg magazines, video on demand platforms etc
F. Paying for utilities such as electricity bill, phone bill, gas bill
G. Paying for financial services such as EMIs, Mutual Fund, SIP, etc.
H. Paying fines e.g driving challan
I. Paying exam fees and other such compulsory fees
J. Others

PREFERRED METHOD OF PAYMENT

13. I prefer to use digital payments when: (Tick all that apply)

A. I am connected to a private wi-fi connection (ie a wifi connection that is shared amongst a selected group of individuals such as at home, office, etc.)
B. I am connected to any wi-fi connection (all wifi connections including those at public places eg cafés, airports, etc.)
C. I have access to a stable internet connection with adequate speed to complete a transaction
D. There is a discount/cashback for using digital payments
E. The business/person I am paying is well-known to me or is a reliable brand
F. I know that I will not lose any money if I use digital payments
G. I know that there is low risk of my privacy being compromised
H. I know that there is low risk of the transaction failing

I. I know whom to contact if there are any problems in processing the transaction or if I make a mistake
J. I can complain to the concerned platform
K. The merchant accepts a digital payment instrument that I trust
L. There is no other method of payment available
M. The transaction is recurring
N. The amount is cumbersome to pay in cash (eg. Rs. 374)

14. I prefer to use cash when: (Tick all that apply)

A. I do not have access to the internet/PoS machine cannot connect
B. I do not have access to a private internet connection (ie a wifi connection that is shared amongst a selected group of individuals such as at home, office, etc.)
C. I do not trust the business/ person I am paying
D. I do not want to have a transaction recorded
E. There is no other method of payment available
F. I suspect that my privacy may be compromised
G. I suspect that a digital transaction might fail
H. I don't know what to do in case digital transaction is not successful
I. I suspect that I might lose money
J. The terms for using other payment methods are not clear
K. I do not use the digital payment instruments that the merchant accepts

15. Which of the following have you experienced in the last three months? (Tick all that apply)

A. I tried to make a payment although I knew my internet connection was not reliable (unstable or too slow to complete transaction)
B. I tried to make a payment although I was using a public internet connection (e.g at an airport or at a café)
C. I used digital payments although I knew that my information might get stolen
D. I used cash even though digital payments would have been more convenient
E. I have decided to not buy something because I could not use my preferred mode of payment
F. I have decided to not use digital payments because of a previous bad experience
G. None of the above

GRIEVANCE REDRESSAL

16. Have you faced a problem while using digital payments in the last three months?

A. Yes
B. No (Jump to question 24)

17. Which of the following problems have you experienced in the last three months? (Tick all that apply)

A. I did not receive an OTP to complete my transaction
B. My card/account was blocked without any explanation
C. The transaction failed
D. The mobile app/website/ card machine necessary to complete the transaction was not working
E. I initiated a digital transaction and did not receive my money back even though the transaction was not completed
F. I did not receive transaction confirmation and paid money more than once

G. I paid money by mistake (unintended recipient and/ or unintended amount) and was not able to recover it
H. I paid a fraudulent person/ establishment thinking that it was a legitimate one
I. Someone else gained access to my account/card
J. I could not contact anyone to address a problem I encountered
K. I lost money but recovered it later
L. Other____

18. Have you contacted anyone to resolve a digital payments-related problem that you faced in the last three months?

A. Yes
B. No (jump to question 24)

19. What is the most serious payments related problem that you experienced in the last three months that you contacted someone about? (Choose only one)

A. My card/account was blocked without any explanation
B. The transaction failed
C. The mobile app/website/ card machine necessary to complete the transaction was not working
D. I initiated a digital transaction and did not receive my money back even though the transaction was not completed
E. I did not receive transaction confirmation and paid money more than once
F. I paid money by mistake (unintended recipient and/ or unintended amount) and was not able to recover it
G. I paid a fraudulent person/ establishment thinking that it was a legitimate one
H. Someone else gained access to my account/card
I. I could not contact anyone to address a problem I encountered
J. I lost money but recovered it later

Note: Please answer the questions 20-23 with respect to the problem you have chosen in Q19

20. Which instrument were you using when you faced the most serious payments related problem you have faced in the last three months?

A. Debit card
B. Credit card
C. Internet Banking
D. Mobile Banking
E. Digital Wallet for eg. Paytm, OlaMoney, Amazon Pay
F. UPI for eg. Google Pay, BHIM

21. Which of the following did you contact in the case of the most serious payments related problem you faced in the last three months (Tick all that apply)?

A. E-Commerce Platform e.g Zomato, Uber
B. Payment Service Provider eg Mastercard, Visa, PayTM, Google Pay, Amazon Pay
C. Bank
D. Trusted CA/Lawyer
E. Institution/Individual that received money e.g shop owner, taxi driver, restaurant
F. Police
G. RBI
H. Court/Consumer Court
I. Other

22. What happened when you contacted these parties in the case of the most serious payments related problem you faced in the last three months? (Tick all that apply)

A. My money was not returned
B. My money was returned
C. I did not receive an adequate explanation
D. I received an adequate explanation

E. My problem was resolved in a satisfactory manner
F. My problem was not resolved in a satisfactory manner
G. I had to spend an excessive amount of time and perform multiple steps
H. I contacted the wrong party and was directed to pursue the matter with the correct one
I. The party that I contacted directed me to contact a higher-ranking party
J. The matter was deemed to be resolved by the concerned party without satisfactory resolution
K. Other____

23. How long did it take to resolve the most serious payments related problem you have encountered in the last three months?

A. My problem has not been resolved
B. 24 hours or less
C. Less than a week
D. Less than a month
E. Less than 6 months
F. More than 6 months but less than a year
G. More than a year

24. Which of the following changes would encourage you to use digital payments more often? (Tick all that apply)

A. Easy to understand terms and conditions/terms of service of using digital payments (e.g. short summaries of terms and conditions, these being available in different languages)
B. Easy to understand statement of privacy policy (e.g. short summaries of privacy policies, these being available in different languages)
C. Easier procedure to use digital payments (e.g. reducing steps required to register for a service)
D. More trustworthy mechanisms to reverse problematic transactions (e.g. reducing steps required to reverse transaction)
E. More reliable grievance redressal mechanism
F. Faster grievance redressal
G. More reliable internet connection (make connection more stable and improve speed)

ANNEXURE 2: SAMPLE CHARACTERISTICS

Figure 16: Gender (% of respondents) (N = 4727)

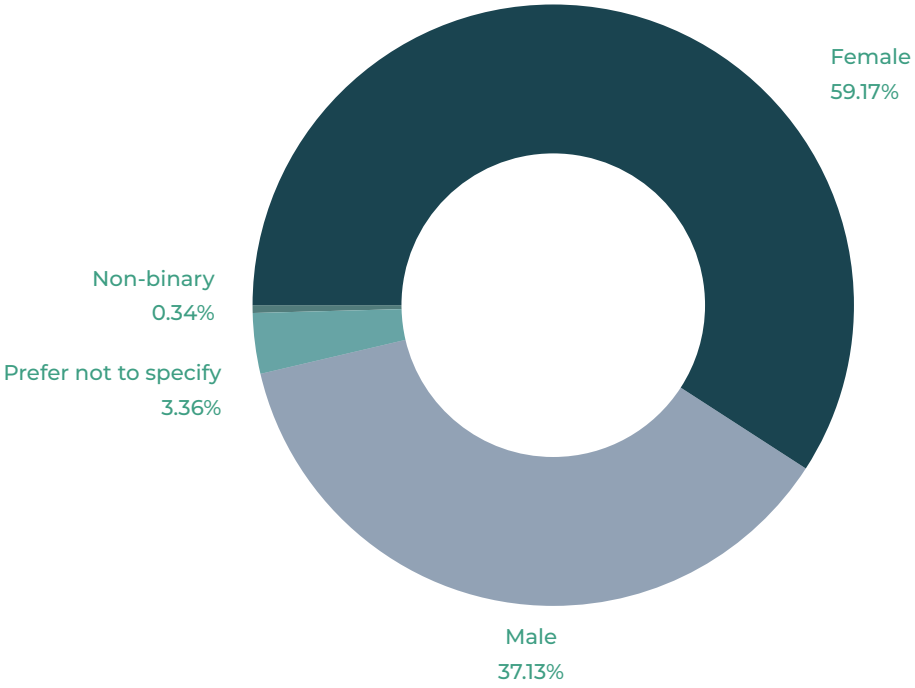
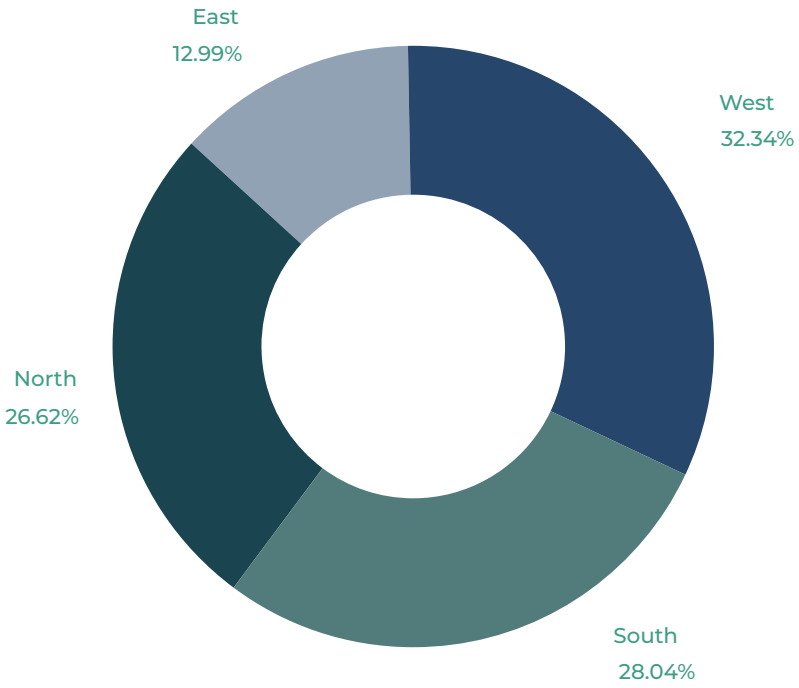


Figure 17: Geographical Region (% of respondents) (N = 4725)



ANNEXURE 3: SURVEY LIMITATIONS

1. Self reporting bias: Our survey relies on respondents to report their experiences with transacting digitally, whether they are able to transact digitally or not, and factual characteristics such as household income. This may result in inaccuracies as people are known to under-report incomes and seek to conform to socially acceptable norms when they report their experiences and opinions.[52]
2. Representative of urban, online only: Our survey includes responses only from urban consumers located in Tier X, Y and Z cities according to the 7th Pay Commission classification. Further, this is an online survey, which means that these responses pertain to users who are well informed and well connected via the internet. Therefore, our survey does not include voices from rural India and from digital payments users who do not have internet connections.

ANNEXURE 4: PRINCIPLES AND BEST PRACTICES IN QOS REGULATION[53]

PRINCIPLE	COUNTRY	PRACTICE
Transaction Efficiency	United Kingdom	Digital payment service providers are mandated to declare a maximum time-limit taken for a transaction at the time of onboarding customers.
	Ghana	Ghana has proposed a maximum duration of less than 5 seconds in processing transactions in its QoS Regulations, 2019 published by the National Communications Authority (NCA). Ghana has also proposed a near 100 percent money transfer success rate for Digital Financial Services. The NCA is empowered to sanction service providers for falling short of QoS Standards. The NCA may review QoS measurements at any time and publish monthly district-wise data of QoS parameters.
Authentication and Fraud Prevention	United States of America	Service providers are required to provide clarity about when, how, and under what terms consumers have authorized a payment. Their systems should also enable customers to limit the period, amount and payee for which authorization is valid. The US law also mandates a mechanism to revoke authorization. Service providers are mandated to ensure that system architecture enables recording information for post-transaction evaluation. The system should also enable a reversal mechanism if there is unauthorized access.
	European Union	The Revised Directive on Payment Services (PSD2) prescribes a threshold exceeding which service providers should maintain a strong risk-based authentication mechanism. PSD2 obliges payment service providers to apply “strong customer authentication” (SCA). SCA is an authentication process that indicates whether the use of a payment instrument is authorised. Some EU countries have made it mandatory while some are prescribing it as voluntary.

PRINCIPLE	COUNTRY	PRACTICE
	United Kingdom	The law provides standards for authorization and execution and attributes liability to the service provider. The country also prescribes a format for incident reporting.
	Other countries: Japan South Korea China Russia Brazil	These countries directly regulate aggregators and/or gateways. These include prescriptions on: licensing / authorisation; requirements for operation; and security of online payments. Many countries require a robust authentication mechanism for transactions. With respect to authentication standards, Europe, India, China, and Russia have country-specific standards while industry-supported standards are the norm in other countries.
	Worldwide industry standards	3D Secure and 3D Secure 2.0 are two examples of worldwide standards. 3D Secure 2.0 uses 'rich data' (which includes payer and device information) to facilitate risk-based authentication by the issuer. Information is collected, encrypted, and sent to the card scheme's directory server. This is subsequently validated. The issuer cross-references this information against rich data to understand if the authorized person has authenticated the transaction. The EMVCo, which is a consortium of American Express, Discover, JCB, Mastercard, UnionPay and Visa, facilitates this process. It also maintains the EMV technical standard for card payments.
Transparency	United States	Record-keeping is mandated in the US for 2 years. In the US, service providers should provide real-time access to information about the status of transactions, including confirmations of payment and receipt of funds. Consumers also receive timely disclosure of the costs, risks, funds availability, and security of payments and upfront disclosures when signing on.
	European Union	The Central Electronic Register at the European Banking Authority (EBA) contains all information relating to the payment institutions associated with each national-level register. EBA, makes the data available to the public on its website and national authorities are required to notify information registered in their respective national registers immediately. The respective National Authorities guarantee the accuracy of the information.

PRINCIPLE	COUNTRY	PRACTICE
	Brazil	In Brazil, payment aggregators are included in the scope of consumer protection laws. These cover transparency, data security, and returns.
Privacy and Consent	United States	In the US, financial institutions are required to provide consumers with certain notices regarding the privacy of non-public personal information and allow them to opt out of information sharing. The GLBA data security provisions give guidance on the appropriate safeguarding of customer information.
	European Union	EU Regulation (Regulation (EU) 2018/389) specifies the requirements for common and secure standards of communication between banks and FinTech companies. Customers have to give their consent to the access, use and processing of their data. Third-party providers will not be able to access any other data from the payment account beyond those explicitly authorised by the customer. In accordance with data protection rules under both PSD2 and the General Data Protection Regulation, account holders can exercise control over the transmission of their personal data under both PSD2 and no data processing can take place without the express agreement of the consumer.
	United Kingdom	The UK law lays down standards for consent and withdrawal of consent for collection, storage, and processing of data similar to the EU's GDPR Regulations.
	Japan	In Japan, there is periodic inspection and vetting to prevent the inappropriate usage and leakage of consumer data.
	Other countries: Brazil Singapore South Korea	In Brazil, Singapore and South Korea, general laws on privacy and protection of consumer data also apply to digital payments. Third-party providers or payment aggregators are mandated to comply

PRINCIPLE	COUNTRY	PRACTICE
Grievance Redressal	United States	In the US, there is a mandate to develop and maintain written policies and procedures that are designed to ensure compliance with the error resolution requirements. In the US, maximum time for redressal is 10 business days under normal circumstances in the US and 45 in case investigation is required. Service providers should provide a conditional refund during investigation in the US.
	European Union	PSD2 obliges EU Member States to designate competent authorities to handle complaints from payment service users and other interested parties, such as consumer associations. Payment service providers should put in place a complaints procedure for consumers which can be used before seeking out-of-court redress or before launching court proceedings, according to the PSD2. The PSD2 prescribes an unconditional refund within 15 days.
	United Kingdom	In the UK, service providers should create procedures and a mechanism to address complaints. They should be made accessible on the website/app; branch of the service provider and access to the procedure must also be included within terms of service between the consumer and service provider. Maximum time for redressal in the UK is 15 days under normal circumstances and 35 in exceptional circumstances. In the UK, consumers may apply for a refund within 8 weeks of a transaction, and the service provider is to either refund or provide reasons for refusal within 10 days.
	Japan	Japan also mandates third-party providers to institutionalise adequate policies, procedure and infrastructural capacity to address complaints, claims and disputes between merchants and consumers.
	Other countries: Singapore South Korea Australia	In Singapore, the Consumer Protection Fair Trading Act and the Commercial Act in South Korea extends the general consumer protection regime to digital payments users as well. In most jurisdictions, there is no separate ombudsman for transactions through digital modes. Australia is an exception and has an ombudsman that covers digital payment transactions as well.

PRINCIPLE	COUNTRY	PRACTICE
Audit and Enforcement	United States	In the US, operators have the option to club disclosures specific to the digital payments' framework with disclosures required under other laws. Record keeping for enforcement purposes is mandated for 2 years. The law further prescribes that systems should have automated monitoring capabilities. Further, providers are incentivised to report any fraud and the enforcement procedure for this is disclosed transparently.
	United Kingdom	In the UK, Dispute Resolution Rules (DISP) mandate reporting of all complaints to the FCA. Enforcement capacity lies with the Financial Conduct Authority and the FCA also has a consumer portal for complaints.
	Other countries: Australia South Africa Brazil Singapore Germany Sweden Japan	Most countries explicitly empower their Central Banks to monitor digital payments through regulation. This is the case in Australia, South Africa, Brazil, and Singapore. In other countries such as Germany, Sweden, and Japan, the recognition is implicit as Central Banks perform the broad role of ensuring adequate and safe functioning of payments in the country without an explicit reference to digital payments. The Central Banks in all the mentioned countries produce and publish statistics on payments.

REFERENCES

1. RBI (2020), Assessment of the progress of digitisation from cash to electronic
2. Ibid
3. Central Board of Direct Taxes (2019), Income-tax (16th Amendment) Rules, 2019.
4. Central Board of Direct Taxes (2019), Circular number 32/2019 dated 30th December 2019.
5. RBI (2020). RBI announces creation of Payments Infrastructure Development Fund.
6. RBI (2019). RBI's Payments Vision 2021.
   RBI (2020). Report of the Committee on the Analysis of QR Code.
7. RBI (2019). Notification dated 20 September, 2019, Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems.
8. RBI (2019). Notification dated 31 January, 2019. Ombudsman Scheme for Digital Transactions, 2019.
9. RBI (2020). Notification dated 22 June 2020, Increasing Instances of Payment Frauds – Enhancing Public Awareness Campaigns Through Multiple Channels.
   RBI (2020). Statement on Developmental and Regulatory Policies dated December 4, 2020.
10. RBI (2020). Notification dated 15 January 2020, Enhancing Security of Card Transactions.
11. RBI (2019). Statement on Developmental and Regulatory Policies dated August 7, 2019.
12. RBI (2019). Notification dated 8 January 2019, Tokenisation – Card transactions.
13. Supra note 1
14. RBI (2019). RBI Bulletin December 2019.
15. RBI Annual Report, various editions.
16. IFMR LEAD, CUTS, Dvara Research, Report of the RBI's High Level Committee on deepening digital payments
17. Sean Creehan (2018), India's Digital Payments: Growing Consumer Trust, but Merchants Needed.
18. Reserve Bank of India (2020), Report of the Committee on Analysis of Quick Response Codes
19. Razorpay
20. As on 30th April 2020. TRAI performance Indicator Reports.
21. As per a KPMG report, 58 percent of Indian language internet users cited the limited availability of local language content as a reason restricting them from using digital payments.
22. Reserve Bank of India (2019), Annual report for The Banking Ombudsman Scheme, 2006 & The Ombudsman Scheme for Non-Banking Financial Companies, 2018 (July 2018-June 2019).
23. Reserve Bank of India, Reserve Bank of India Bulletin dated 13 August 2020.
24. All calculations in this chapter are based on responses to questions "I prefer to use cash when:", "I prefer to use digital payments when:", and "Which of the following have you experienced?". To ascertain the factors that users care about, responses from the first two questions have been clubbed into the themes listed in Figure .
25. Reserve Bank of India (2019), Report of the High Level Committee on Deepening Digital Payments
26. Ligan et al. (2019), What explains low adoption of digital payment technologies? Evidence from small-scale merchants in Jaipur, India
27. IFMR LEAD (2017), The Evolving Financial Ecosystem for Micro and Small Merchants in India

28. CUTS CCIER (2020), Users' Perspectives On Digital Payments: Presentation for High-Level Committee on Deepening of Digital Payments
29. Annual Report of the RBI Ombudsman, 2018-19
30. Dvara Research (2020), Transaction failure rates in the Aadhaar enabled Payment System.
31. Advait Rao Palepu, "Glitches In Aadhaar Enabled Payment System Amplified As Transactions Surge", Bloomberg Quint, May 6, 2020, https://www.bloombergquint.com/business/glitches-in-aadhaar-enabled-payment-system-amplified-as-transactions-surge.
32. DVARA Research (May 2020). Transaction failure rates in the Aadhaar enabled Payment System.
33. RBI (2020). Statement on Developmental and Regulatory Policies dated December 4, 2020.
34. RBI (2021). Reserve Bank of India introduces the RBI-Digital Payments Index.
35. ITU-T G.1033 10/2019, Quality of service and quality of experience aspects of digital financial services
36. Section 43(2)(b), The Payment Services Regulations 2017.
37. Draft Quality of Service Regulations, 2019 by the National Communications Authority.
38. TRAI has Regulations on Standards of Quality of Service of Basic Telephone Service (Wireline) and Cellular Mobile Telephone Service. TRAI compiles and publicises state-wise reports on performance against these parameters.
39. Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems, published on September 20, 2019.
40. Reserve Bank of India (2019), Statement on Developmental and Regulatory Policies dated April 4, 2019
41. Reserve Bank of India (2019), Annual report for The Banking Ombudsman Scheme, 2006 & The Ombudsman Scheme for Non-Banking Financial Companies, 2018 (July 2018-June 2019).
42. RBI (2021). Reserve Bank of India introduces the RBI-Digital Payments Index.
43. Thales Security (2019). 2018 Data Threat Report Global Edition.
44. Carnegie Endowment (2020). Timeline of Cyber Incidents Involving Financial Institutions.
45. Section 70B, IT Act, 2000.
46. Ibid. See also http://cert-in.org.in/s2cMainServlet?pageid=VLNLIST
47. MRSC Cybersecurity Resources for Governments.
48. Economic Report of the President of the United States of America Together with The Annual Report of the Council of Economic Advisers (February 2018).
49. Observer Research Foundation and Koan Advisory (2019), Towards a Cyber Security Roadmap for Digital Payments.
50. Compiled from Report on 'Benchmarking India's Payment Systems' by the Department of Payment and Settlement Systems, RBI and 'Red Book Statistics' by the Committee on Payments and Market Infrastructure, Bank for International Settlements.
51. Economic Report of the President of the United States of America (February 2018).
52. Brenner PS and DeLamater J, Lies, Damned Lies, and Survey Self-Reports? Identity as a Cause of Measurement Bias, 2016, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5639921/
53. Compiled from Report on 'Benchmarking India's Payment Systems' by the Department of Payment and Settlement Systems, RBI and 'Red Book Statistics' by the Committee on Payments and Market Infrastructure, Bank for International Settlements.