mastercard

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

CONTACTLESS PAYMENTS

Making it Safe, Secure and Easy for a Billion Indians

FOREWORD

Digitization has changed the world. In India, it lets citizens tap services on their phones, book vaccinations and get certificates, access farming information, and benefit from instant payments that bypass old, leaky welfare schemes. It transforms the way transactions are initiated and processed. It enriches and analyses them on the fly, and does amazing things with those AI-backed insights-such as offering credit without collateral or history.

The world, especially India, is witnessing rapid digitization of transaction processing. The volume of transactions is rising as financial instruments are becoming increasingly accessible to citizens. State push and interventions, regulatory enablement and innovation, are driving the pace of adoption and experimentations. The industry is now thriving with various players, ranging from payment service providers, technology providers, FinTechs, mobile device manufacturers, and even social media giants. The age of mobility, devices, IoT, data science, and AI/ML opens new opportunities. The industry is witnessing a push for opening infrastructure, applications and data, making it more participatory and attracting new players.

Contactless digital payments have emerged as a credible and innovative payment option for quite some time now. It speeds up processing and adds convenience for users. It relieves the users from cognitive burden and minimizes friction in processing transactions quite significantly. The COVID-19 pandemic, concerns of infection and fomites' role in the spread, also underlined the need for contactless payments. Cashless and digital payments, in comparison, are safer and require minimum physical contact between the seller and the buyer. Shops, e-commerce platforms, and customers have preferred them over cash. Countries are adjusting their policies to enable them, and regulatory bodies are coming to terms with reality by offering concessions and removing hurdles.

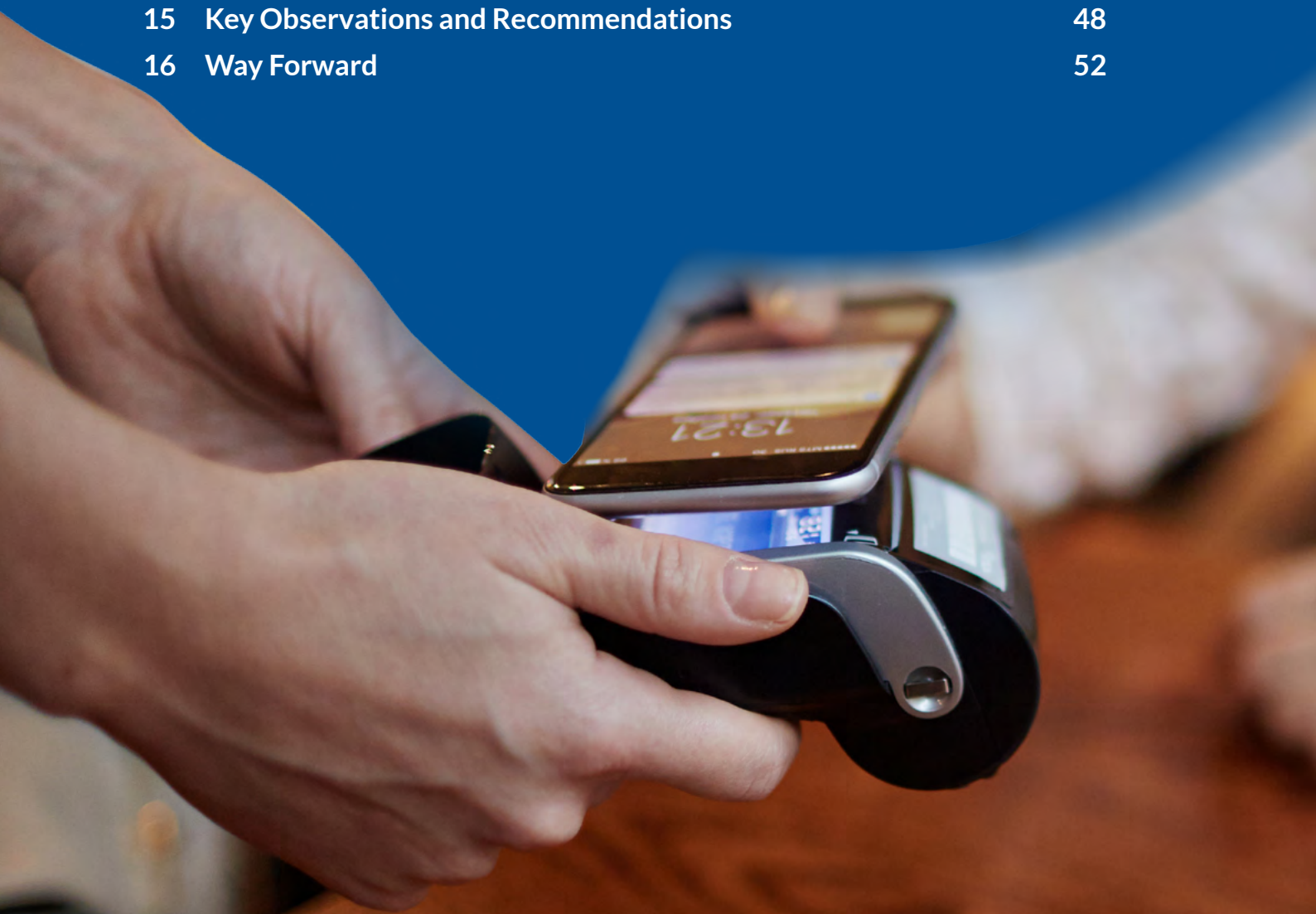
Contactless payment is becoming the new norm of society. Hence, it would be necessary to examine the nuances associated with it, evaluate the dimensions involved, and identify the bottlenecks that can hinder its progress. A critical review of elements shaping the contactless payment ecosystem would help identify issues, attention areas and policy gaps in its progress.

Data Security Council of India and Mastercard have joined hands to examine the elements and dimensions shaping India's contactless payment ecosystem. The report delves into the technologies driving contactless payments, the type of players pushing boundaries, the ecosystem shaping up to support the transition, and evolving standards for enhancing reliability and trust. It examines security issues associated with critical contactless technologies and evaluates the possibilities of frauds and remedies against them. It further assesses the privacy issues related to contactless payments. The report compiles the observations to derive the way forward to create a conducive ecosystem for nurturing the country's growth of contactless payments.

Rama Vedashree,
Chief Executive Officer,
DSCI

Ravi Aurora,
Executive Director, Global Policy Affairs & Community Relations,
Mastercard

CONTENTS



1

EXECUTIVE SUMMARY

Contactless payments have been emerging as a credible and innovative payment option for quite some time now. With the onset of COVID-19, digitalisation has been pushed to the top gear. Globally, the concerns of infection and role of fomites in the spread, underlined the need for contactless payments. Contactless payments have been found to relieve the users from cognitive burden and minimizes friction in processing transactions quite significantly. India is witnessing a rapid adoption of cashless payments fuelled by active government push, architectural intervention like UPI, institutional arrangement for effective execution, and vibrant FinTech industry. This growing ecosystem is further offering a secure, safe, and convenient means of conducting cashless transactions.

Executive Summary

- **Key factors driving contactless payment adoption:** Government intervention, ecosystem entities, innovation & enabling technologies are playing a crucial role in shaping and growing the digital payments ecosystem. FinTechs are reshaping the industry through technology adoption, process innovation and next-generation solutions. In India, the share of contactless payments increased to 12% in October 2020, from 2% in early 2019. Further, development of passive and risk-based authentication, advancement in UI/UX models, modern cryptography and most importantly "Privacy by Design" practices are serving as catalysts to drive higher adoption.

- **Trends emerging with the digital ecosystem growth:** In 2020, India saw 100 million digital transactions per day, about a five-fold jump from 2016. RBI expects this to further grow to 1.5 billion transactions a day. Significant uptake in contactless payment by smart cities, transportation, hyperlocal electronic commerce, and smart parking will significantly contribute towards the contactless ecosystem. Wide scale adoption along with the benefits of contactless payments, such as speed, convenience, scale, and productivity are estimated to grow the demand in the new reality. Transaction processing methods are parallelly evolving on the back of technological advancements to become more secure, frictionless and provide no-touch experiences which reduce cognitive burden on the user.

- **Ecosystem growth, a conducive environment to enable contactless payments:** Development of standards and policy interventions are further propelling digital payments towards contactless models. Allocation of INR 1500 crore in the union budget for 2021-22 will strengthen digital payment and enhance reliability. Furthermore, the Reserve Bank of India's (RBI) decision to waive off the need for two-factor authentication for transactions less than INR 5,000 through cards is estimated to boost adoption of contactless payments. It has also proposed to allow a pilot scheme for small value payments in offline mode. Accelerated adoption of digital payments is estimated to clock 167 billion transactions processed digitally by 2024-25, and NETC digital transaction volume is likely to grow 12x to reach 15.5 billion by 2025.

- **Risk and accountability around contactless payment:** The contactless methods are marred by some key misconceptions about security, fraud, and misuse. However, the regulatory ecosystem has made payments secure and helps establish accountability. Financial institutions have advanced security measures for protection, transactions are monitored in real-time for fraud and attack detection solutions. Mainly, the frauds in contactless payment are due to low user awareness.

- **Way forward and Recommendations:** Contactless payment has the potential to digitize all possible physical transactions and has helped in realizing crucial goals of national programs. There is a need to have concerted strategies to keep the momentum growing. While moving forward emphasis on the following models will enable a frictionless, interoperable, convenient, and secure contactless payment ecosystem:

  - Contactless by Design: Adopting this principle offers enhanced security, offers tremendous flexibility, and supports rising scale.
  - Emphasis on Interoperability: This function removes friction, offers flexibility, relieves consumer burden, and supports larger designs as it is free from closed-loop design clutches.
  - Investment in Technology Infrastructure and Network: Banks and other entities in the chain should invest in upgrading their infrastructure and network to cater to the rising volume. Insistence on zero MDR (Merchant Discount Rate) on certain payment types removes incentives for the investment.

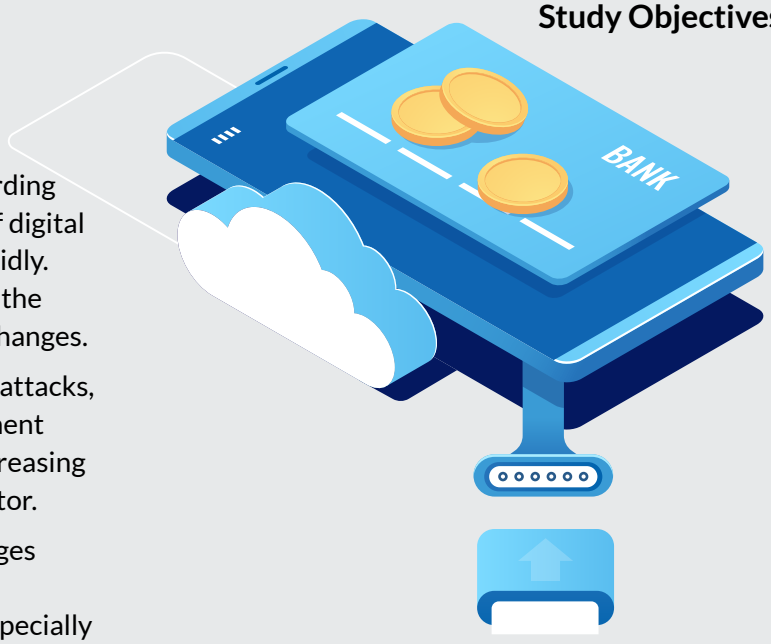
- Standard-based approach to Technology: The standard-based approach provides a better, predictable, and scalable answer to address these challenges.
- Open Framework & Specification for Use Cases & Larger Programs: A cautious approach of making ecosystems open and specification driven will create a multiplier ecosystem.
- Local financial ecosystem to support hyper local commerce boom: Allowing small and regional banks to offer financial instruments will add weight to the hyperlocal commerce momentum.
- Promoting Innovation and Experimentation: This can transform many offline and digital transactions being performed by contactless mediums.
- Security Research: As technologies adopt, the scale and success of more extensive programs hinge on them. Careful attention is required towards security preparedness and its strength against the evolving attack systems.
- Conducive Policies: Contactless technology until now has met with conservative policies but it has begun to change since the pandemic as many countries have raised limits and lifted prohibitive rules. Policymakers should see the potential contactless technologies offer and their upcoming role. These technologies deserve proactive and conducive policy support.
- Security Awareness Campaigns: The policymakers and players in the ecosystem should develop concerted awareness campaigns to dispel safety and security myths around contactless payments.

2

STUDY OBJECTIVES

Against the backdrop of rapid digitization and push for digital payments amidst the current context of COVID-19, this study pertains to the following objectives:

- Study the ongoing evolution of risk-based and frictionless transaction processing across the globe, including India.
- Examine ways and means of leveraging technology for reducing the cognitive pressure and burden on users from the viewpoint of Security and Privacy.



- Because of the speed, friction, onboarding of multiple players, the entire chain of digital transaction processing is evolving rapidly. It therefore becomes critical to study the innovations that are affecting these changes.
- Evaluate the payment related frauds, attacks, observed patterns basis various payment instruments that are becoming an increasing cause of concern for the payment sector.
- Map the Security and Privacy challenges pertaining to the various aspects and elements of the payments industry especially with respect to contactless payment systems.
- Assess the various technical standards that are getting built and enabling financial transaction processing.
- Examine how the underlying development in technology, standardization, security innovation, and fraud management practices can remove bottlenecks.
- Assess the role of the ecosystem components to ensure safety and security.
- Evaluate the policy and regulatory initiatives to further boost the contactless payment momentum.

To achieve the above objectives, we posed some critical questions that this report delves into, revealing facts, insights and ideas to help shape India's contactless payment ecosystem.

Standards: What standards are powering and should power, our rapidly evolving, exploding payment landscape?

How can standards and technologies help India create a payment landscape and systems that will help a billion Indians transact safely and seamlessly? What are the new/evolving/ emerging standards?

Payment Landscape: How does the payment landscape transform in 2021, worldwide and in India? The trends were highlighted with a specific focus on existing and evolving standards from a contactless transaction perspective.

Trends: What are the emerging payment trends in the biggest sectors that would involve the major population of India?

Scale: How to scale up digital payments for safe and secure transactions for a billion Indians. What has India done in recent years, what are the challenges, and how can we address them?

Interoperability: Given the explosion of players as well as multiple evolving technologies and platforms, how important is interoperability? How do we ensure it? The burgeoning volume of transactions in 2020 led to delayed response and timeouts due to transaction processing latency. How to address this?

Frauds: What are the biggest cons and frauds in payments? What are the causes, the most affected platforms, possible solutions and measures to deter frauds?

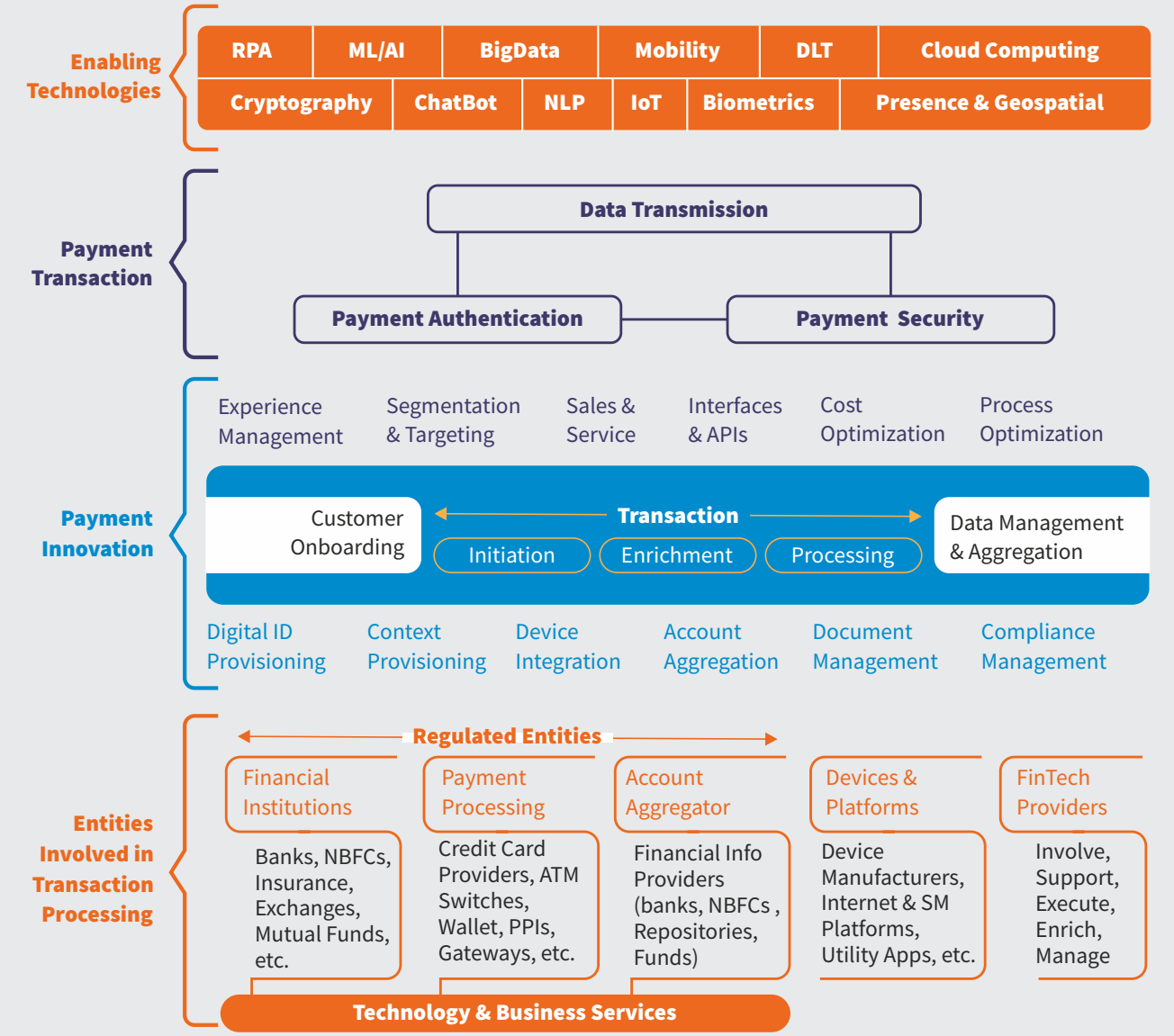
Security and Trust: What are the top challenges and concerns for contactless payments security and trust? How to win consumer trust?

3

DIGITAL PAYMENT ECOSYSTEM

Before moving to contactless payments, it would be essential to review the country's digital payment ecosystem. The following figure summarizes the ecosystem. It draws entities involved in the evolution, highlights areas witnessing innovation push, and lists the enabling technologies making it possible.

Figure 1: Digital Payment Ecosystem



Conventionally, financial institutions played a crucial role in digital payments, and they would keep doing so. Subsequently, credit card providers became an essential part of the payment ecosystem, followed by interventions like ATMs, wallets, prepaid payment instruments. Recently RBI allowed account aggregators to provide their services, primarily as financial information providers. The technology transformation, especially in mobility, digital devices and social media has opened avenues for a new set of players. They came as a credible alternative to reach end consumers at scale. Their innovation, both at hardware and software levels, promises to expand

the payment ecosystem, and solves teething problems of convenience, experience, speed and security. Conducive policies and environment are now making the transaction processing more participatory for FinTechs. Technology and business service providers will continue to support this transformation with their technologies and capabilities.

With the unbundling of transaction processing, it opened opportunities for innovation at each stage of the lifecycle of a transaction. Right from onboarding a customer, initiating transaction, providing enriching insights and information, and supporting the execution of the transaction to aggregating and managing data generated, technology players, platforms and Fintechs are adding significant value. Above figure depicts the areas where innovative ideas have helped improve the experience, enhance productivity, and create new possibilities.

Technologies like mobility, IoT, data science, AI/ML, NLP, biometrics, cryptography, and cloud computing are enabling this transformation. The environment is getting increasingly conducive to allow entities possessing these capabilities to solve payment problems and be a part of the transaction processing ecosystem.

4

CONTACTLESS PAYMENTS

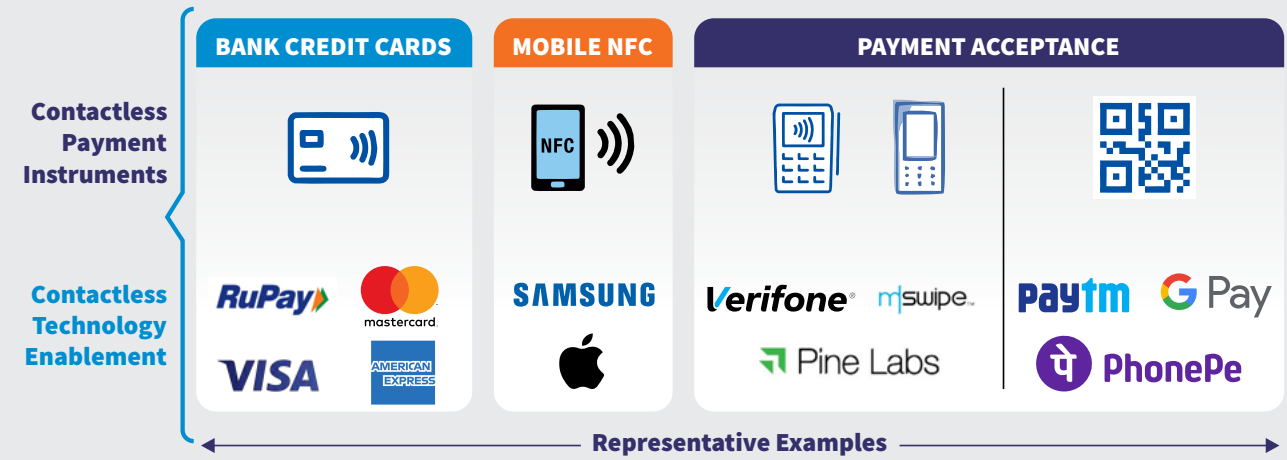
Contactless payments have been gaining traction among consumers slowly yet steadily, since payment behaviour is often marked with reluctance to change and being comfortable with familiar options. Consumers are apprehensive about the incremental changes, and this results in slow overall adoption. Safety and trust are other deciding factors hindering momentum. The COVID-19 pandemic forced consumers to change the way they see cash and contact-based payments. Increased concerns around hygiene, safety and physical distancing forced them to adjust to contactless payment methods.

As per the Mastercard global consumer study conducted in April 2020[1], nearly 8 in 10 consumers say they use contactless payments. 46% to 52% of customers swapped out their top-of-wallet card for one that offers contactless payment, the report reckons. Most consumers view contactless as a cleaner and faster way to pay, as it enables transactions up to 10 times faster than other in-person payment methods. This enables customers to get in and out of stores faster. This trend would stay even in the post-pandemic world.

As per the Mastercard global consumer study conducted in April 2020[1], nearly 8 in 10 consumers say they use contactless payments. 46% to 52% of customers swapped out their top-of-wallet card for one that offers contactless payment, the report reckons.

Being a leader charting an aggressive path for digitization, India witnessed a swift transition to contactless payments. The ecosystem flourished on the back of a transformative and inclusive architectural framework, ripe for rapid adoption, making contactless payments emerge as a favored mode for digital transacting. As per Pine Labs CEO Amrish Rau, the share of contactless payments increased to 12% in October 2020, from 2% in early 2019[2].

Figure 2: Contactless payment instruments and corresponding players



1 *https://www.mastercard.com/news/ap/en/newsroom/press-releases/en/2020/april/mastercard-study-shows-consumers-moving-to-contactless-payments-for-everyday-purchases/*

2 *https://timesofindia.indiatimes.com/business/india-business/easier-norms-for-contactless-use-may-boost-cards/articleshow/79597438.cms*

The payment players are already equipped with enabling technologies like NFC and QR code for contactless payments. Cards, mobile devices and apps are equipped with the desired technologies for authenticating users, exchanging payment messages and securing transactions. The payment acceptance infrastructure is rapidly accommodating by retrofitting the Point of Sale (POS) devices or using QR codes. One out of five POS machines, now supports contactless payment in India.

Policy interventions have contributed immensely towards bolstering and driving the contactless payment ecosystem. The RBI has enabled the ecosystem by removing the mandate of two factor authentications for payments below INR 5000. The Ministry of Urban Development released guidelines for operators willing to offer ubiquitous transit solutions across the country. It has notified contactless specifications to lay down the foundation of the National Common Mobility Card (NCMC). Many projects like Bengaluru Metropolitan Transport, Mumbai Metro, Kochi Metro and Ahmedabad Smart City went live with these guidelines. These factors are laying the foundation for a robust contactless ecosystem and is estimated to propel the value and volume of contactless payments in years to come.

Contactless payment works well in offline mode as well. RBI has also proposed to allow a pilot scheme for small value payments in offline mode. This report investigates the policy interventions for contactless payment in a separate section.

Despite all these developments, there are still concerns associated with contactless payments. They stem from security, trust, fraud, privacy and liability issues due to various incidents. Such concerns led RBI to release stricter norms around contactless payments to curb misuse. The transaction limit imposed supposedly hindered the progress of contactless payments. As digital payment transactions are rising multi-fold putting significant stress on processing infrastructure, the transaction success rate is emerging as a significant concern.

Despite all encouraging developments, there are still concerns associated with contactless payments. They stem from security, trust, fraud, privacy and liability in case of an incident.

5

EMERGING TRENDS

Contactless payment has a bright future ahead even after the world recovers from the pandemic. The benefits it offers, such as speed, convenience, scale and productivity, go beyond the current safety focus. While the contactless method will influence most retail, transfer and offline payments, it can potentially drive payments for some massive sectors quite aggressively. The figure below illustrates the current state and possible future state.

Figure 3: Frameworks and policies helping grow the digital transaction volume

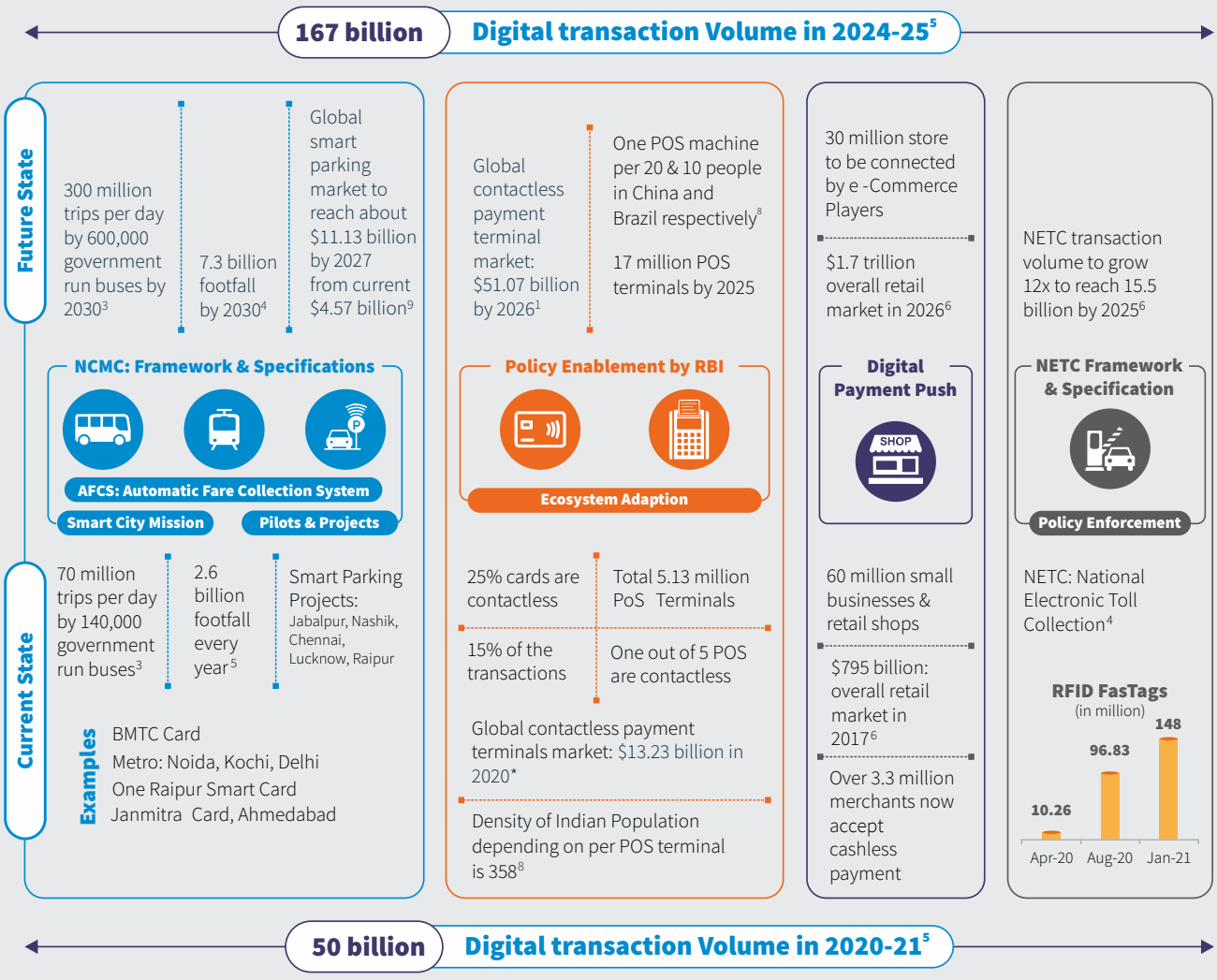


Figure References

1 *ResearchandMarkets Report,Global Contactless Payment Terminals Industry (2020 to 2025)*
2 *A report of the Ministry of Road Transport and Highways*
3 *Knight Frank Report*
4 *NETC FASTag, NPCI*
5 *PWC Report, Indian Payments Handbook*
6 *Invest India on Retail & E-commerce*
7 *Report of Grand View Research*
8 *https://www.deccanherald.com/national/digital-drawback-only-one-pos-terminal-in-india-for-every-358-people-808112.html*
9 *https://www.globenewswire.com/en/news-release/2021/01/12/2157269/0/en/Smart-Parking-Market-to-Portray-11-13-Billion-by-2027-Says-Allied-Market-Research.html*

Acceleration of Digital Payments

Active government push in the form of proposed Digital Payment Security Controls Directions to make India a less cash society in a safer way (Cashless India Initiative) is propelling change. The Indian government also allocated INR 1,500 crore[3] to help drive the adoption of digital payments in the country. The Digital India mission is another continuous initiative aimed to improve online infrastructure and facilitate digital services to citizens. Other initiatives include processing Direct Benefit Transfer (DBT) subsidies online; G2C services such as Certificates - Birth, Caste, Income, Marriage, Character etc which can be applied and paid online, and enabling citizens to pay for utility bills, property taxes, etc online. Such initiatives, coupled with architectural intervention to create a participatory payment ecosystem like UPI, institutional arrangement for effective execution, and a vibrant FinTech industry, transformed India's payment landscape. In the year 2020-21, it was estimated that the country would witness approx. 71 billion transactions processed digitally, which will be further accelerated to reach 167 billion by 2024-25. The share of contactless payments will keep increasing in the coming five years.[4]

Growth of Contactless Card Volume and Usage

Although UPI has emerged as a prominent platform, Cards continue to be a dominant and ubiquitous payment instrument. The adoption of debit/credit card payments are still on the rise in the country marked by first time account holders, rise of salaried individuals and urbanisation of small cities & towns. However, the density of Indian population per POS device still stands at 358 individuals, as against 20 and 10 individuals in China and Brazil respectively[5]. It hints at the tremendous growth opportunity in the installation of POS devices in the country. Currently, only 25% of cards issued possess contactless technology, and they account for 15% of total transactions. We will be witnessing accelerated growth in the deployment of contactless payment terminals. Market projection of contactless payment terminals globally, as depicted in the above figure, hints at the future dominance of contactless methods in card payments.

Smart City, Transportation and Parking

India was 31% urbanized in 2011 which is expected to increase to 40% by the year 2031[6]. Smart city missions and projects are focusing on making urban mobility contactless through automated fares and smart parking features.

As per a Ministry of Road Transport and Highways report, in the year 2017, about 70 million trips were catered by 140,000 government buses. By 2030, the country would be adding another 460,000 buses for urban transport. They will be catering to a total of 300 million trips a day, which means 109.5 billion trips per year. The success of the early projects such as Janmitra Card, Ahmedabad and One Raipur Smart Card hints that contactless cards can cater to these trips. These projects are based on the National Common Mobility Card (NCMC) framework and specifications notified by the Ministry of Housing and Urban Affairs. On similar lines, Delhi Metro which is expected to witness a footfall of 7.3 billion by 2030, piloted the use of NCMC cards making payments contactless.

The smart city initiative also pushes for smart parking which is already on the rise globally and India is also witnessing a significant acceleration in this area. Further, many smart city projects are

3 https://www.livemint.com/news/india/iit-madras-mpfi-collaborate-to-boost-digital-money-transactions-in-india-11620645814146.html

4 https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/the-indian-payments-handbook-2020-2025.pdf

5 https://www.deccanherald.com/national/digital-drawback-only-one-pos-terminal-in-india-for-every-358-people-808112.html

6 https://www.inae.in/storage/2020/01/Urban-Transportation.pdf

looking for Automated Fare Collection Systems (AFCS) to automate payment collection from citizens.

All these factors create unprecedented growth opportunities for contactless payments to further increase its footprint in the coming years.

Hyperlocal Commerce

With 60 million-plus small businesses and shops, India's retail segment attracts innovative start-ups and larger local and global players. The market is very competitive and is now amenable to technology innovation, thanks to the digital payment push. During the turbulent pandemic, the local stores kept their supply chain intact, swiftly transitioned to home delivery, and adopted safe contactless payment methods. Digital commerce companies are finding innovative ways to help consumers buy from local shops.

Khatabook, a start-up based out of Bengaluru, has seen 10 million downloads of its accounting app within the merchant network. Dunzo, a food and grocery delivery start-up, now serves 300 plus neighbourhoods and delivers items in less than 30 minutes. Dukaan, yet another start-up that enables local stores to become digital, has seen 4.3 million downloads in just six months. On the other hand, Reliance Jio is planning to integrate 30 million stores digitally. The pandemic made these deliveries contactless, and also the payment. Hyperlocal commerce provides immense opportunities for innovative contactless payment ecosystem.

National Electronic Toll Collection

NETC program is yet another flagship initiative that will help drive contactless payments. FASTag devices unveiled by it employ Radio Frequency Identification (RFID) technology to make toll payments directly while the vehicle is in motion. By mandating FASTag use at all highway toll plazas last year, FASTag devices have seen a significant uptake taking the total transaction carried out to 148 million in Jan 2021 from just 10.62 million in April 2020. NETC transaction volume is likely to grow 12x to reach 15.5 billion by 2025, as per the PwC Indian Payments Handbook report.

6

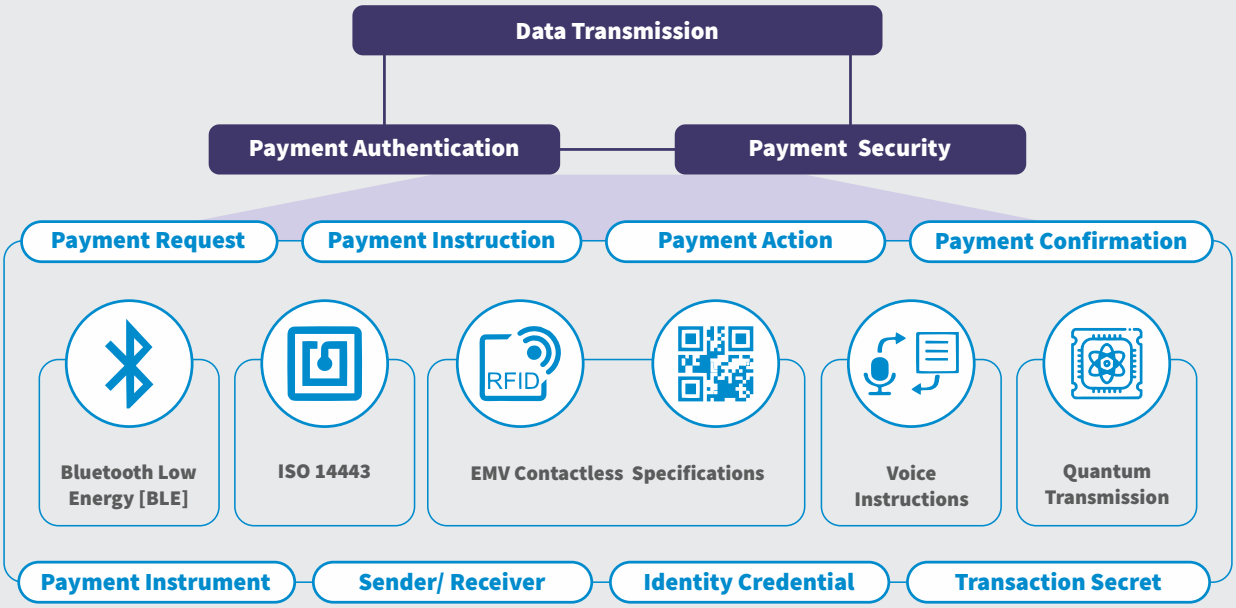
CONTACTLESS PAYMENT TRANSACTION

Three key components that make contactless transactions a reality are:

- Transmission of data that exchanges payment information
- Authentication of users (and sometimes devices)
- Security of data and communication

The figure below depicts the elements required to make a successful transaction.

Figure 4: Contactless Payment Transaction Process



For a transaction to be successful in any payment instrument, managing the sender's identity credentials and dealing with the receiver is essential. The transaction may have a secret code that needs to be exchanged between the cards/ apps and the merchant's payment acceptance device. The payment transaction can be triggered upon the request of the merchant or payee. Payment actions like quick taps (tap and go), QR code scanning, and transferring amount to phone numbers have evolved to take care of contactless transactions. The payment confirmation message is delivered in various ways like the use of tone, flashing receipts, sending SMS, and even confirming via audio message.

No-touch Experience Technologies

Many technical alternatives have emerged in the recent past to realize no-touch experience. They range from gesture recognition, expression recognition, face recognition, laser proximity, ultrasound proximity, eye tracking, and noncontact biometrics to speech commands, QR codes, RFID/NFC, and Bluetooth beacons. Remote haptics and videos can also be used for the same. Their effectiveness for contactless payment transactions will depend on how effectively they will be able to complete all stages of a payment transaction. The ability to help identify and authenticate users, ease to

7 https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/the-indian-payments-handbook-2020-2025.pdf

enter transaction data, and delivery of payment information are the critical parameters for transaction processing. Alternates like remote video, non-contact biometrics, and augmented reality are good in addressing a few of these parameters. However, RFID, NFC, QR Codes, Bluetooth, voice instructions, and non-contact biometrics are the most favoured payment service providers' options. Further the mobile revolution made them more accessible, configurable, and experimental. Commoditization of voice recognition technology due to Amazon Alexa or Google Voice Assistant is also lending itself to the use of voice instruction to initiate payment requests. Quantum computing and communication technologies are currently in very early stages of adoption, but it is promising to offer ultra-secure contactless payments at a later stage.

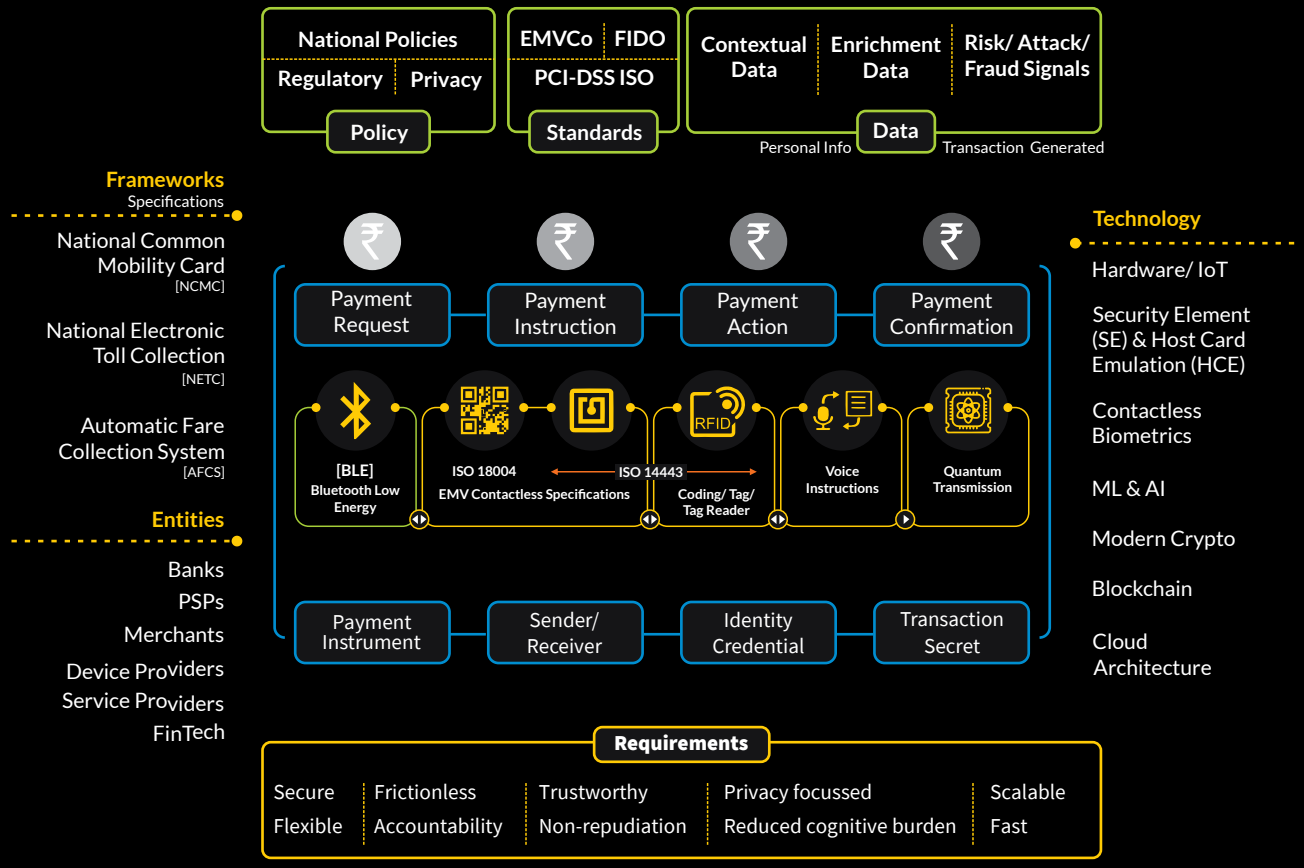
The ability to help identify and authenticate users, ease to enter transaction data, and delivery of payment information are the critical parameters for transaction processing.

7

ECOSYSTEM READINESS

The ecosystem was already in place for contactless payments to a great extent, which made it possible to cater to the sudden jump in consumer demand for convenient payment choices during the pandemic. The figure below depicts the different factors shaping the evolution of contactless payments.

Figure 5: Factors shaping the evolution of contactless payments



Key Requirements

Any contactless digital payment method must satisfy critical requirements for its success, as depicted in the figure. It must provide an excellent user experience, leverage underlying processes and user interactions to reduce friction during transactions. Further, as consumer reliance on digital and contactless methods are rising, the expectation around transaction speed is also growing.

As per P Vasudevan, Chief General Manager for the Department of Payment and Settlement Systems at RBI , India saw 100 million digital transactions per day in July 2020, about a five-fold jump from 2016. RBI expects this to further grow to 1.5 billion transactions a day. As the share of contactless payment is rising multi-fold, it should factor in the scalability requirements. Contactless payment should also show flexibility in fulfilling the payment requests as consumers prefer the contactless option for various new transactions.

As per RBI, India saw 100 million digital transactions per day in July 2020, about a five-fold jump from 2016. RBI expects this to further grow to 1.5 billion transactions a day.

Consumers remain apprehensive about the safety of using contactless cards. The pace of transaction processing and lack of user awareness provides avenues to fraudulent players for malpractices. The ecosystem should provision ways to enhance consumer trust. Along with better fraud management practices, it should ensure fixing accountability for any incident of fraud or security compromise. Furthermore, the personal data exchanges in the lifecycle of a contactless payment system would attract the attention of rising privacy expectations and obligations. Security, privacy, and trust add a cognitive burden, as systems tend to rely more on the user's action. Freeing up the user from it would go a long way in the growth of contactless payments.

Supporting Technologies

Hardware innovation has enabled embedding NFC/RFID capabilities in various form factors used for diverse applications. Google included an NFC stack in an Android release in 2011. In the same year, Mastercard and Visa integrated NFC payment in phones. In 2012, Mastercard introduced contactless RFID cards. Apple incorporated it into iPhone 6 in 2014, which triggered the NFC momentum. The real transformation began when the mobile OS, enabled card emulation for NFC services in a tamper-resistant chip inside a mobile device. It is referred to as Secure Element (SE). It is integrated either in a SIM, MicroSD, or embedded chips. It offers a secure place to store payment credentials and perform cryptographic operations. It was still constraining development, as SE is not scalable. Host card emulation (HCE) emerged as an alternative that enables software-based card emulation for NFC. This innovation enabled service providers to provision NFC services directly to their customers without partnering with a mobile carrier.

The real transformation began when the mobile OS, enabled card emulation for NFC services in a tamper-resistant chip inside a mobile device. It is referred to as Secure Element (SE). It is integrated either in a SIM, MicroSD, or embedded chips. It offers a secure place to store payment credentials and perform cryptographic operations.

Non-contact biometrics such as touch free fingerprints, and retina scans can serve the purpose of authenticating the user without needing to touch a sensor. Experimentations are on to use face recognition, respiration rate, and gait analysis for payment transactions.

The contactless card works on proximity technology; it gets powered-up nearing the card reader/POS. It begins to transmit its fixed binary code number. An attacker might get an opportunity to penetrate if this exchange is not secure, which comes by taking care of authentication, protecting data integrity, and ensuring non-repudiation in the transaction. Deployment of cryptographic module on the card solves this problem. The cryptographic function must withstand threats such as impersonation, relay, man-in-the-middle, clandestine scanning (electronic pickpocket) attacks, and denial of service attacks. On the

other hand, it deals with small form factor, low energy and limited processing power. Modern cryptography offers solutions to these challenges.

In digital payments, machine learning and AI adds critical value to all lifecycle stages of transaction processing. As entities deploy biometrics methods such as face recognition, gait analysis and remote video, technologies deploying machine learning and AI play an essential role in contactless payments as well. Secondly, the ML/AI stack is a central element of risk-based authentication. Lastly, it plays a crucial role in fraud prevention and analysis.

Experimentations of leveraging blockchain technologies for contactless payment are also on going. As all merchants and customers' transaction history is updated on the blockchain, both parties can look out for past fraudulent activities and proceed with caution. Apart from ensuring price-scoring, duplicate spending, and online fraud, blockchain can authorize, authenticate, and audit the transactions.

Simplification of EMV and contactless payment integration is crucial to cater to the speed, scale, and flexibility of transaction processing. Secondly, it must seamlessly integrate with verticals such as healthcare, retail and more. The use of SDKs and device drivers on individual machines remain cumbersome for developers and time-consuming for IT teams and small businesses. Cloud computing modernizes the development to make merchants remain competitive. Cloud delivered platform-agnostic APIs make them ready for the requirements of scale, speed, and flexibility and simplifies compliance with strict regulations. It allows them to integrate with independent software vendors (ISVs) and independent sales organizations (ISOs) to deliver a range of secure and in-person payment options.

Simplification of EMV and contactless payments integration is crucial to align to the speed, scale, and flexibility of transaction processing. The development of POS devices would get modernized by cloud delivered APIs to make them ready for the rising scale, speed, flexibility, and simplifying compliance.

Data

Payment systems consume data and generate data out of processing the transactions. Besides meta-information, contactless tends to capture more personal information as it deploys mechanisms like biometrics for authentication. Secondly, the data is transmitted over open-air, raising concerns about security, which is discussed in the subsequent sections. As with other payments, it would also get contextual and enriching data to enhance the consumer's experience. It might consume signals received from different sources highlighting risks and patterns of frauds.

Besides meta-information, contactless tends to capture more personal information as it deploys mechanisms like biometrics for authentication.

Enabling Standards

Standard development efforts are catching up with the movement of digital payment towards contactless. They target different levels such as technical specification level, the level where solutions are accepted, and the level where assurance is demonstrated by payment service providers. The following summarizes the 'Standards' development in this space.

- **The EMV® Contactless Specifications:** EMV defined Secure Protocol and Core Function specifications ensure digital payment transaction security. The same also focuses on performance and user experience. It has come up with EMV Contactless Specifications for Payment Systems enabling secure standardized and globally agreed-upon benchmarks for helping a contactless payment ecosystem.
  - NFC Payment: refers to transactions using proximity NFC payment devices/ Cards. They support cryptographic functions for secure transactions.
  - QR Code Payment: EMVCo provides specifications pertaining to the use of QR codes for payment purposes. It focuses on Consumer-presented QR Codes and Merchant-presented QR Codes.
  - Mobile EMV: Contactless Payment Terminals may need to support the possibility of multiple contactless mobile payment applications across multiple Secure Elements being active simultaneously. The mobile EMV standards enable secure transmission of data between the users and the merchant devices.
- **RFID Standards:** RFID standards define how information is coded. It gives standards for tagging data and defines tag reader linkage standards.
- **PCI-DSS Standards:** In 2019, PCI SSC released new standards to secure contactless payments. Data security standard for solutions that enable merchants to accept contactless payments using a commercial off-the-shelf (COTS) mobile device (e.g., smartphone or tablet) with near-field communication (NFC). Using the PCI Contactless Payments on COTS (CPoC™) Standard and supporting validation program, vendors can provide merchants with contactless acceptance solutions that have been developed and lab-tested to protect payment data. The PCI CPoC Standard includes security requirements for vendors on how to protect payment data in CPoC Solutions and test requirements for laboratories (labs) to evaluate these solutions through the supporting validation program. The primary elements of a CPoC Solution include:

- COTS device with an embedded NFC interface to read the payment card or payment device.
- Validated payment acceptance software application that runs on the merchant COTS device initiating a contactless transaction.
- Back-end systems independent of the COTS device and support monitoring, integrity checks, and payment processing.

- FIDO Authentication standards: Fast Identity Online (FIDO) Alliance, an open industry association focused on developing authentication standards to reduce reliance on passwords, notified FIDO U2F use for mobile authentication over NFC. FIDO standards offer strong two-factor authentication using public key crypto that protects against phishing, session hijacking, man-in-the-middle and malware attacks. As it allows users to choose, own, and control their online identity, they opt to have multiple identities, including anonymous, with no personal information associated with the identity.
- ISO 1443 Standards: It specifies the requirements for proximity cards used for identification purposes. It specifies a way to put together the card physically. It also defines characteristics of the fields used to provide power and bidirectional communication between proximity coupling devices (PCDs) and proximity cards or objects (PICCs). Lastly, it defines how the communication process begins, proceeds, and ends.

Policy Interventions

Governments have been recognizing the need to move to contactless payments, asking banks to issue contactless credit and debit cards. However, most countries migrated to EMVCo 3D secure and Chip and PIN regime, requiring the user's input in each card transaction. This proved to be a major hurdle due to which contactless payments could not take off. Subsequently, regulators allowed PIN-less transaction processing to respond to the contactless trend, although with a limit. These limits were low in value, hindering the widespread adoption of contactless payments, especially in the case of card-present transactions. The COVID-19 pandemic pushed many governments/regulators to lift these limits for contactless payments. As per the World Economic Forum, 31 countries have raised contactless payment limits in 2020 to support social distancing measures. Still, apprehensions around the safety and security of contactless payments persist. In some countries, the regulators restricted operation of the contactless feature on cards at the time of issuance requiring the same to be manually activated post issuance.

As per the World Economic Forum, 31 countries have raised contactless payment limits in 2020 to support social distancing measures.

Programs and Specifications

The national mission to accelerate digital payments through the Digital India Program-Cashless India gave rise to many ambitious and nationwide programs which promise a significant boost to contactless payments. NETC created an interoperable ecosystem where multiple issuers and acquirers are involved in issuing FASTag devices and completing the toll payment transactions.

Transport operators experimented with various solutions, largely with closed-loop cards that work only in the closed establishment. Many smart city

projects such as Surat relied on an Automated Fare Collection System (AFCS). Although AFCS has helped digitize the fare collection to a large extent, it wasn't interoperable. It denies the consumer the flexibility of using the same instrument for other modes of transport. These cards are also not enabled for retail transactions.

Although AFCS has helped digitize the fare collection to a large extent, it wasn't interoperable. It denies the consumer the flexibility of using the same card for other modes of transport. These cards are also not enabled for retail transactions.

To overcome this, the Ministry of Housing & Urban Affairs (MoHUA) took the initiative of creating standards for a complete ecosystem for the National Common Mobility Card (NCMC). The NCMC program is aimed not just at being accepted at Metro terminals but also for other low-value payments for transport, parking, and other merchant payments. Apart from payment, it supports applications such as monthly passes and seasoned tickets. Such use cases would transform smart cities, transportation projects, and fare collection programs into contactless payment hubs.

Entities Shaping Contactless Payments

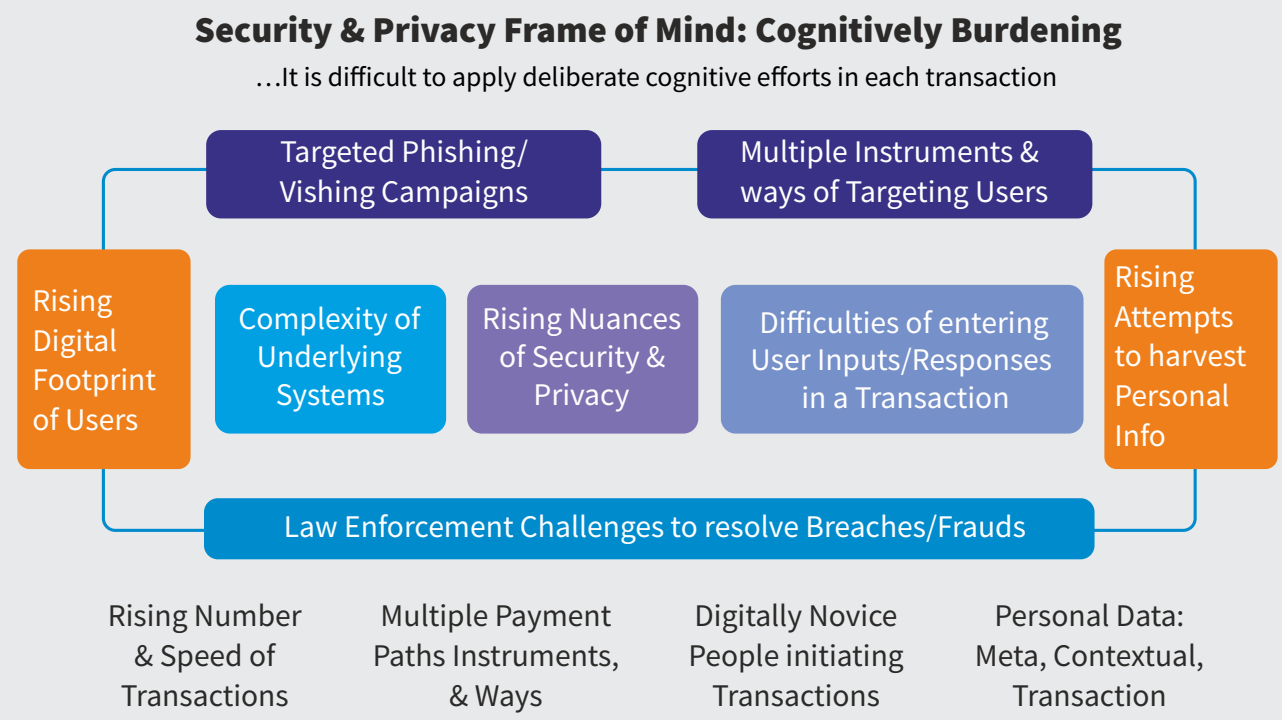
Driven by the technology offered by card providers, banks first started issuing contactless cards in 2015. For example, India has seen an increase of 19% in contactless cards issued in Q1 2020. This move by card providers and banks brought focus on contactless mediums and led other payment service providers to also join the league. In a Mastercard poll, 54% of the respondents revealed they know how to use a contactless card on a POS machine. Card providers and banks are running special campaigns for spreading awareness about the safety and security of contactless payments. Some of them even started a location search for contactless shopping. Contactless payment improves the prospects of the merchants and reduces their efforts in the handling of cash. Merchants became a real agent for spreading awareness and instilling confidence about contactless payment in the users' minds. Some ideas like audio notification of payment confirmation, worked very well in favour of contactless payments. FinTech start-ups joined this momentum by offering innovative and cost-effective solutions supporting contactless payments. Device providers and payment platform providers also upped their game. Mobile OS players added Bluetooth payment support.

Merchants became the real agents for spreading awareness and instilling confidence about contactless payment in the users' minds. Some ideas like audio notification of payment confirmation worked very well in favour of contactless payments.

8 REDUCING COGNITIVE BURDEN

Unlike earlier days, users now transact digitally much more frequently and deal with multiple payment instruments, paths, and ways. During the transaction process, their data and context are captured to serve the purpose of digitization. The digital inclusion drive brought many more digitally novice people into the formal financial transaction ecosystem. They may not be aware of their privacy rights. The current ecosystem significantly relies on the consumer's action for ensuring security and privacy, adding cognitive burden on the users. The figure below explains it.

Figure 6: Cognitive burden related to payment transactions- security and privacy concerns



The underlying systems are increasingly getting complex. Also, the subject and intricacies of security and privacy are rising for a user to comprehend. In a fast-moving transaction, it is difficult to enter the required information to initiate a transaction. More difficult is to capture the out-of-band second factor and enter securely. Phishing and vishing campaigns target consumers to get hold of this message. Users have been increasing their digital footprint and thus the attempts to harvest personal information are rising quite significantly. Moreover, if a user encounters any issue or breach, the resolution is not easy due to lack of knowledge of grievance processes. Thus, over reliance on the user action or input for security and privacy should be avoided.

By eliminating or reducing user action, the contactless payment ecosystem gives an opportunity to experiment with ways to solve security and privacy issues without putting the burden on the user.

Passive and Risk based Authentication

The use of legacy tools such as knowledge-based verification, CAPTCHA, or one-time passwords (OTP) or PIN frequently results in customer frustration and adds burden. The system set up by out-of-band authentication to capture the sent OTP is often exposed to phishing attempts. The pop-up windows or script-based frameworks used to enter them mostly lack access to security verification. Rising call centre frauds targeted to get hold of OTP, testifies the same. People of all ages, and even educated and digitally literate, fall prey to such fraud mechanisms. These frauds show how difficult it is to maintain the security and privacy frame of mind while transacting. The explicit process of authentication not only introduces friction but also makes it vulnerable.

Risk-based authentication is emerging as a solution to it. The ability to collect data, bring it together and analyse it for the intended purpose has been significantly improved in the recent past. Location data, device identity, device feeds, user behaviour, third-party credentials, past transaction history, etc., are available to take authentication decisions. The security and fraud management ecosystem is now able to identify risk signals, deliver threat intelligence, provide reputational and whitelisting feeds, and generate trust scoring. Risk-based passive authentication can also address many concerns associated with contactless authentication. It can allow carrying high-value transactions at the stores, as POS devices are becoming more intelligent and connected. Advanced POS devices can perform risk-based authentication tasks.

The explicit process of authentication not only introduces friction but also makes it vulnerable. Risk-based authentication is emerging as a solution to it.

User Experience

The success of payment digitization process critically hinges on the comfort, convenience, and confidence of the consumer. The process of payment transactions should be a low effort task for the consumer. The interface should be simple, easily understood, and convenient to act. It should reduce unnecessary customer effort for a more frictionless experience. Streamlined and straightforward processes with minimal distractions and payment check-out process enhances customer satisfaction and increases their trust. User intimation is vital for gaining confidence, especially confirmation of the payment. Notifying payment confirmation with audio messages at a shop is an example of a good user experience.

Streamlined and straightforward processes with minimal distractions in payment check-out process enhance customer satisfaction and increase trust.

Modern Cryptography

Contactless payments are enabled by NFC, RFID, Bluetooth and QR code. Security and privacy protection efforts must consider the miniatured form factor, limited power supply, and constrained processing power. Modern cryptography comes to aid not only for solving the security and privacy problems but also enabling innovations in the following ways:

- Encryption of communication between contactless card and POS terminal, authentication of card and POS terminal, and random number generation for transactions.
- Lightweight cryptography to perform cryptographic functions in a constrained environment.
- Encoding of all payment information through QR codes or smart card codes, so that digitally novice users can transact securely as the information is exchanged with terminals automatically.
- Cryptographic encoding of identity information/identity attribute such as face for offline authentication.
- Quantum cryptography for quantum enabled contactless cards.

Modern cryptography comes to aid not only for solving the security and privacy problems but also enabling innovations.

9

MYTHS AND REALITIES

Many safety and security concerns are marred with misconceptions. The figure below lists popular myths around contactless payments and the reality behind them.

Myth	Reality
Myth #1 Criminals standing close to you can siphon off money from your contactless cards while making payments	**Reality** Only KYC compliant merchants are issued these contactless POS terminals. Any unauthorized or fraudulent transaction on these POS terminals can be easily traced by legal and bank authorities.
Myth #2 Criminals can easily steal and clone the contactless card information	**Reality** The financial industry uses advanced security measures to protect the contactless device and card, incorporating industry-standard encryptions, dynamic data, authentication, confidentiality, and security controls. The card information is insufficient to clone a card or transaction. To steal the information, the criminal must come within proximity (four centimeters) of the cardholder.
Myth #3 A stolen card can be used to make unlimited fraudulent purchases	**Reality** Card issuers use sophisticated fraud detection services that are highly effective in detecting card abuse, criminal use of cards, and unauthorized activities. In India, currently INR 5000 is the transaction limit for contactless payments and any higher value than it, needs to be authenticated by entering the PIN. If any card abuse is detected, the contactless payment gets blocked, and consumers also have the option to modify the transaction limit and activate/deactivate contactless payment options online.
Myth #4 Using card skimmers, criminals can steal user's account information	**Reality** Consumers just need to tap and make payments; thus, the user will always control their contactless card. These transactions are monitored with real-time attacks and fraud detection measures. Tokenization provides additional layer of security in protecting the user's personal information which replaces the sensitive account information on the contactless cards without exposing the actual account information.

10

RF VULNERABILITIES

A contactless card integrates an antenna and a chip conforming to the standards defined. It works on a standard communication frequency of 13.56 MHz. Once the contactless card is placed near a contactless POS terminal, it emits a magnetic field enough to activate the card. There are known vulnerabilities with the RF interface. The following figure illustrates them and showcases how they are handled for safe and secure contactless payments.

Figure 7: RF Vulnerabilities: Attack Patterns, Risks and Countermeasures

Vulnerability	Attack	Attack Set-up	Risks	Countermeasures
A legitimate contactless payment transaction can be captured using a clandestine antenna	Passive Eavesdropping	Spy-reader in close proximity to read data exchanges	Leakage of card account data Leakage to manufacture a fake card or a clone	Encryption of data exchange Authenticate contactless card
Contactless card responds when it detects 13.54 MHz frequency	Clandestine scanning/ Electronic Pick Pocket/ Skimming Replay Attack	Clandestine reader in proximity with the contactless card Skimming for replay attack (using predetermined challenge)	Retrieval of data for cloning Initiation of fraudulent payment order	Reader authentication Online authorization Quality Random Number
POS confused if it has authenticated remote chip instead of presented	Grandmaster Chess/ Replay/ Man-in-the-Middle Attack	Fake Card for carrying MITM attack Using skimmed original cards	Unauthorized Payment	Binding transaction time foils replay attacks as it takes extra time
Weak Crypto implementation due to limited processing power & battery	Brute Force Attack	Brute Force Tools to read data	Eavesdropping transaction for card cloning	Lightweight crypto is standardized. It takes care of this attack
Activating all cards in the proximity leading collision	Denial of Service Attack	Activating multiple cards	Disruption in transaction processing	Standardization like ISO 14443 solves collision problem

RF Vulnerabilities

Card providers, other players in the payment ecosystem, and the stakeholders such as EMVCo, European Payment Council, National Regulatory Authorities such as the RBI, payment ecosystem facilitator like NPCI, and PCI Security Standards Council, all work together to identify and resolve payment security issues. They rely on introducing controls, standardization, adopting security architectural practices, and creating an assurance ecosystem to fix accountability. These players keep close watch on real world security risks and spread awareness around emerging threats. They promote security research in areas such as cryptography, think of policy ideas to secure payment systems, and create an environment of accountability.

The ecosystem ensures security by promoting standardization, introducing controls whenever necessary, adopting security architectural practices, setting up measures to fix the accountability, promoting payment security research, and keeping close watch on security risks and threats.

11

CONTACTLESS PAYMENT FRAUDS

Frauds committed in digital payment mediums, including contactless payments happen majorly due to the lack of awareness of working of digital payment systems or fraudsters take advantage of certain human errors. As per a report by YouGov and ACI Worldwide, 47% of Indian consumers are worried about online frauds and around one third of respondents have been themselves or know someone from their immediate circle to have been the victim of digital payments or cards fraud. Among fraud sources, duplicate websites and fake apps topped the chart with 52% (as per survey respondents), followed by password/credential information fraud at 43% and spyware/malware with 39%. Few examples of prevalent social engineering and popular types of frauds through online payment channels are highlighted below:

UPI Platforms

UPI is a real time payment system developed by NPCI which is a popular medium for conducting online payments. UPI acts as the backbone for all mobile wallet transactions, helping them connect with multiple banks in a single interface and enabling the payment process. It can be used to both send and receive money provided both parties have a UPI client installed which comes in the form of various apps such as BHIM, PhonePe, Google Pay to name a few.

Modus Operandi: Criminals send UPI payment request link via SMS, WhatsApp, etc on the pretext of receiving money for online sale or cashback. Upon clicking that, the link redirects to the corresponding UPI based app installed on the phone; once the UPI PIN is entered, the amount is deducted from victim's account.

Another mechanism is deceptive UPI handles claiming to be the official handle of global pandemic relief funds, Govt. payment channels, etc.

Mitigation Strategy:

- UPI PIN is only needed to send money and not receive money
- Avoid engaging in payment transactions with strangers
- Never click on any links or accept payment requests
- Stay away from counterfeit apps

Customer Support Frauds

Fraudsters populate fake customer care numbers on social media or create counterfeit webpages displaying these numbers. They take advantage of the customer's anxiety occurring during transaction failure or a service issue and capitalize on their state of panic under the pretence of providing customer support.

Modus Operandi: When transactions are not successful and the money is not immediately refunded, users panic and reach out to customer care. When the actual customer care numbers aren't reachable, the customer searches for alternative numbers. This is where the victim falls into the first trap laid by the fraudster by reaching out through numbers on counterfeit webpages or social media. The customer eventually calls the fraudster and after having some conversation regarding the issue, the scammer asks customers to install a remote access application such as AnyDesk, TeamViewer, Quick Support and asks for access code that is displayed on the screen by means of social engineering. Scammer can then operate the customer's device remotely and make a payment as well.

Mitigation Strategy:

Consumers need to be aware to not click on unauthorized links from an unknown source and exercise great caution while recognising the UPI handles. Few steps that can be taken to avoid being defrauded are:

- Call on customer care numbers mentioned on official websites only
- Be alert of any request that asks to download any third-party app that will allow your device to be accessed remotely
- Use a second layer of security by adding biometric or numeric locks on all payments apps

Phishing

Phishing uses fraudulent email/SMS designed to impersonate a legitimate person or organization and trick the recipient into divulging sensitive information. This includes rewards, cashbacks, refunds as attractive baits to trap victims.

Modus Operandi: One example is IT return fraud – once taxpayers have filed their IT returns online; typically, after a few days they receive an email/SMS informing that they are eligible for a refund. The message format closely resembles the

Income Tax department. The mail/SMS includes a link redirecting users to a website resembling the Income Tax website and one might mistake it as the genuine site. The website asks for account related information such as credit/debit card details including number, CVV, expiry date and PIN, using which the fraudster can make fraudulent payments.

Mitigation Strategy:

- Always verify sender's address before taking any action. Phishing emails have sender email address that resembles genuine ones, e.g. incometaxefiling@gov.in, but are spoofed. The missing 'l' from 'filling' is to be noted here.
- Do not open emails or SMS quoting refund, cashback, offers, for example. issuing refund of your IT returns in this case.
- IT Department or any other financial institution never asks for personal or financial information over SMS, email, phone or on websites.
- Report to the concerned authorised body in case you receive such phishing emails or SMS.

e-Wallets

e-Wallets/mobile wallets are being increasingly used for contactless payments during the pandemic. With the growing use of e-Wallets, the Reserve Bank of India has made KYC mandatory for all e-Wallets users. Criminals use this as an entry point to exploit users.

Modus Operandi: The victims receive a message to update their KYC to continue wallet services. Fraudsters pose as support executives and extend help. To update KYC, users are tricked to download a third-party app such as TeamViewer or AnyDesk (screen mirroring software). Fraudsters ask to check the status of their e-Wallet by sending a token amount (Rs.1) and when the victim enters the wallet PIN to login, the sensitive information is captured. The criminal keeps the victim engaged on call and meanwhile debit money from the victim's e-Wallet.

Mitigation Strategy:

- Payment service providers never ask you to install third party apps (screen mirroring tool) for KYC completion.
- Do not attend inbound KYC based calls. Always initiate calls from your end after verifying the customer care number from official website.
- Never share an OTP or any code over call to anyone, even with customer care representatives.

QR Code

Quick response code (QR code) is another digital payment mode used by consumers to send/receive payments in a contactless manner. All e-wallets allow scanning QR codes and make contactless payments.

Modus operandi: Under the pretext of receiving money, fraudsters mislead victims to scan QR codes to receive payment, whereas a QR code is only scanned to send payment. QR codes can be sent through WhatsApp or other messengers from a trusted source to mislead victims into sending money to the fraudsters.

Mitigation Strategy:

Consumers need to be aware of the fact that a QR code is scanned to make payments only. Steps should be taken to make consumers aware and updated on the modus operandi. Consumers should always check and verify the beneficiary and check for confirmation messages/notifications.

12

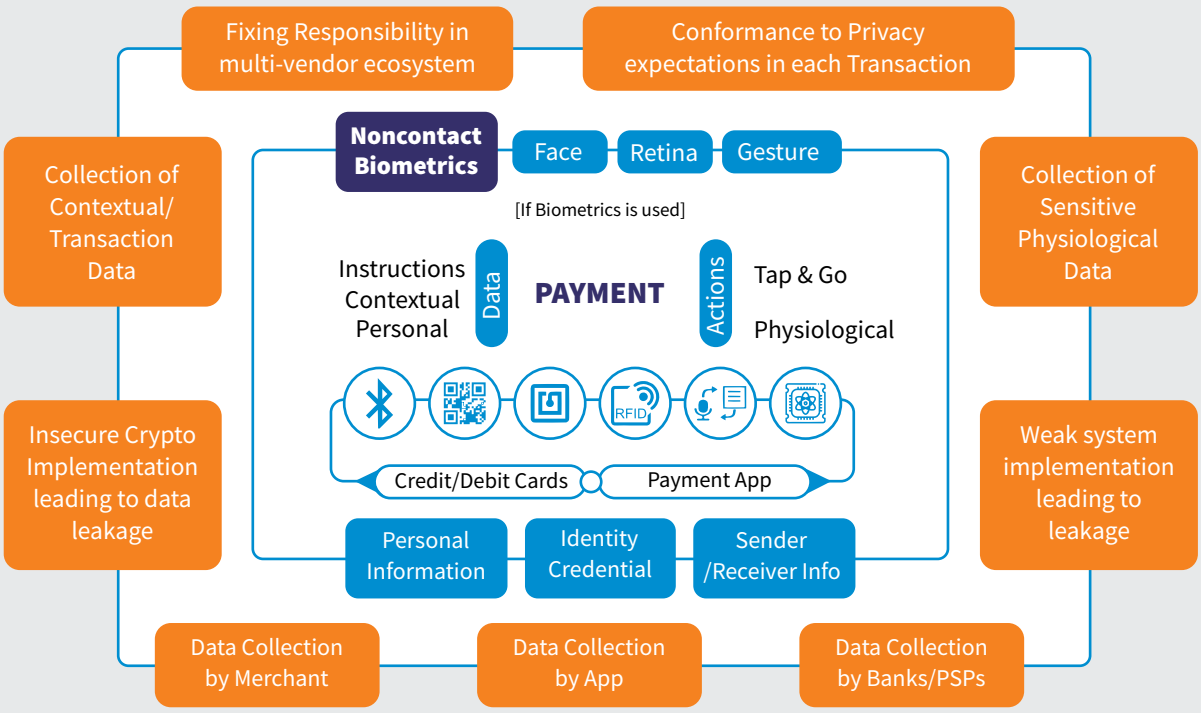
DATA PRIVACY

Privacy concerns deliberated in the context of digital payments are as follows:

- Excessive data collection, processing without consent, use for unintended purposes,
- Opacity in data handling practices
- Undermining data subject's rights over his or her data,
- Performing analysis without de-identification,
- Carrying out activities that are potentially harmful for the data subject

Financial information is treated as sensitive information in some geographies and has been proposed as such in India's Personal Data Protection Bill. Hence, all entities need to handle such information with much more caution. For the purpose of this report, it's essential to examine the privacy elements associated with contactless payments. The figure below highlights privacy issues related to contactless payments.

Figure 8: Privacy related sources of concern in contactless payments



The growth of contactless payment should focus on all layers that could potentially lead to privacy ramifications.

- Research standard driven attention to assess privacy challenges at data exchanges by NFC, RFID, QR Code, Bluetooth and Biometrics
- Embedding privacy in designing and engineering payment instruments
- Data protection practices of all players involved in the lifecycle
- Processes for involvement of consumers in the decision making

13

TRANSACTION FAILURES

Digital payment has witnessed phenomenal growth in India. The volume of transactions is rising month after month, with UPI recording 2.7 billion transactions worth INR 5 trillion in March 2021[11]. As per a Razorpay report[12], a payment gateway solution company, online transactions grew 80% in 2020. Tier-II and III cities contributed to 54% of digital transactions in 2020, demonstrating a 92% growth in just one year, the report reckons. During the pandemic, digital payment indeed reached remote areas and many new people joined this movement for hygiene, safety and convenience.

However, surging digital payments are now testing the digital infrastructure. Top banks using UPI network recorded failure rate of over 3% in September 2020, as per an NPCI report[13]. The high rate of transaction failure and the resulting piling up of credit reversal triggered worry over digital payments. As UPI transaction hits the core banking system, the rising volume puts a strain on them. In a survey conducted by ACI Worldwide, 44% respondents said that failed transactions are a top concern when it comes to digital payments. For consumer confidence in growing digital payment

11 *https://www.npci.org.in/what-we-do/upi/product-statistics*

12 *https://www.outlookindia.com/outlookmoney/apps/online-transactions-grew-80-in-2020-razorpay-5834*

13 *https://inc42.com/buzz/top-10-banks-record-3-failed-upi-transactions-some-could-have-upto-40/*

volumes, the operation needs to be stable and support high-capacity transactions to match the surge in payment requests.

The waiving off the merchant discount rate (MDR) on UPI now curbs revenue and limits resources for the entities involved to upgrade their infrastructure. In 2016 the Watal Committee on digital payments, set up by the Ministry of Finance, observed that MDR incentivizes digital payment processing players. The committee recommended that MDR be market-driven, and capping MDR hinders the digital payments industry's growth. Without incentivisation, investment in digital payment would be lower, which might lead to failure in transactions.

The high rate of transaction failure and the resulting piling up of credit reversal triggered worry over digital payments.

Developing Trust in Digital Payments

Trust is crucial for achieving the desired pace of digitization for any payment medium. In the context of contactless payments, it is critically important as myths of its safety and security are still prevalent. This report observes that the foundational contactless technologies, RFID and NFC, are robust, thanks to continual innovation and enabling standards. Their integration with different form factors, card, and mobile, also pass critical security examinations. Payment authentication, payment message exchanges, and communication security have evolved to withstand the security attacks even at the scale at which contactless payments are operating now. However, the failure of the transaction due to technical reasons raises doubts in the consumer's mind. Apart from competent security measures, investment in reducing failure rate and friction is equally important to build consumer confidence in contactless payments. The government is taking this seriously. Allocation of INR 1500 crore in the union budget for 2021-22 for strengthening digital payment is a welcoming step towards enhancing reliability. However, allowing the incentives flow in the payment network for the necessary investment would add critical value to build trust in the consumer's mind.

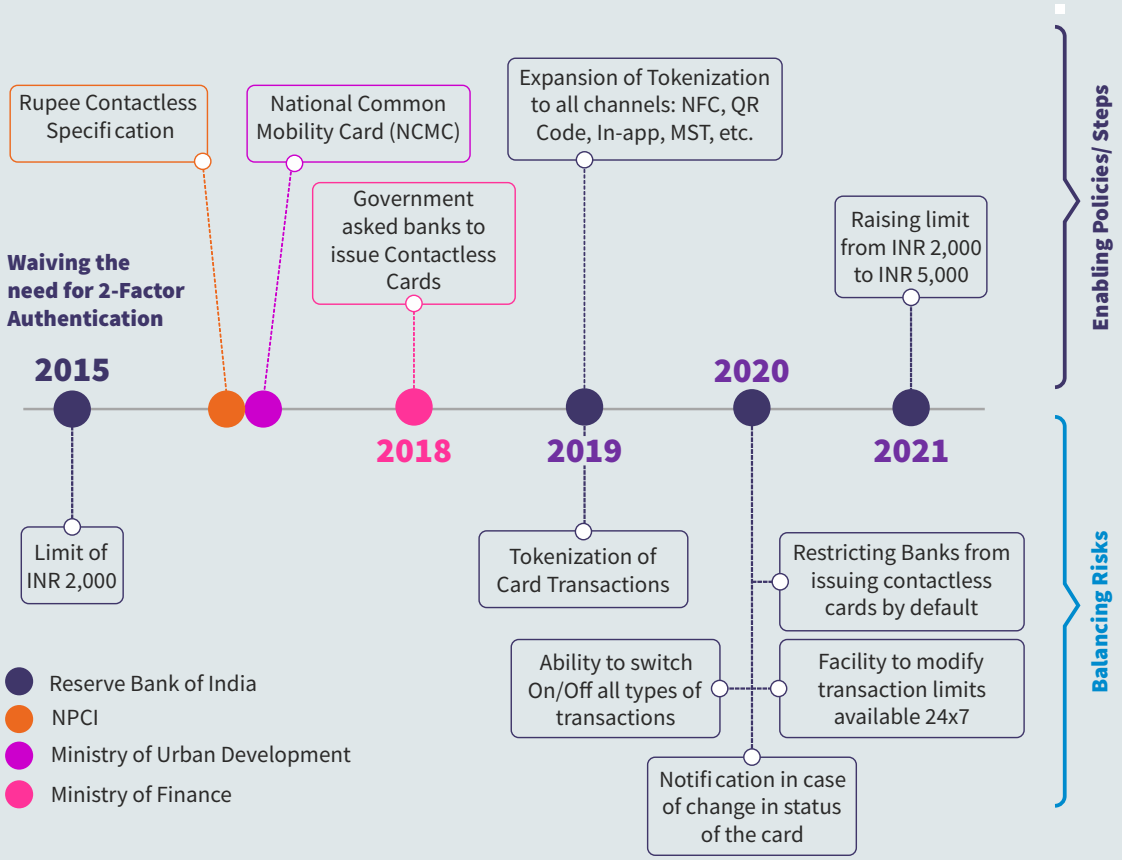
Payment authentication, payment message exchanges, and communication security in the contactless methods have evolved to withstand the security attacks even at the scale contactless payments are operating now.

Allocation of INR 1500 crore in the union budget for 2021-22 for strengthening digital payment is a welcome step towards enhancing reliability.

14 REGULATORY AND POLICY INTERVENTIONS

As technologies evolved to solve problems associated with the exchange of data securely from the consumer card to POS terminals due to the advent of NFC/RFID and then QR codes, the payment ecosystem started looking at the feasibility of enabling contactless payments. However, the earlier transition to CHIP and PIN contained a swift movement. In 2015, RBI responded by reforming the payments and settlements system to waive off the need for two-factor authentication for transactions less than INR 2,000 through cards. Since then, the policy ecosystem is evolving to shape contactless payments in India. The figure below depicts the development until now.

Figure 9: Contactless Payments - Policy level development timeline



Concerns of safety, security, privacy, and liability protection influenced the cautious approach to enable contactless payments in the country. However, the push for digitization of payment since 2016 created good interest in contactless methods. In 2018, the Ministry of Finance asked banks to issue contactless cards whenever new cards are issued or existing cards are renewed, so that the use of card payments can be extended beyond simple merchant transactions. In 2017, NPCI issued an open-loop contactless specification which are common standards devised for both online and offline transactions. The Ministry of Urban Development built on the concept of the National Common Mobility Card on these specifications.

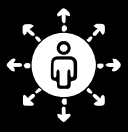
To further strengthen the payment ecosystem, the RBI in 2019 issued guidelines for card tokenization for devices. The permission extended to all channels: NFC, MST, in-app payments, and QR code payments. The RBI has now expanded Card/ Network based tokenization to extend to all web based commercial transactions irrespective of the device used. Acceptance of NFC based token through mobile devices led to a tremendous increase in NFC capable POS terminals. In 2020, the RBI took new measures to enhance security and provide more control to the consumer. It has restricted banks from issuing contactless cards by default. It has asked banks to provide activate/deactivate options to consumers for all types of card transactions including the facility of modifying transaction limits any time of the day. It has also asked them to keep consumers informed via SMS regarding any change in the status of their cards.

The COVID-19 pandemic has seen countries raising the limit of contactless transactions and the RBI has also raised the limit to INR 5000 starting, 1st January 2021.

15 KEY OBSERVATIONS AND RECOMMENDATIONS

Key Observations

Detailed investigation of elements, dimensions, and drivers shaping contactless payments show various aspects that need reflection. The following table summarizes them.

 Untapped Opportunities	No-touch experience technologies have proven their worth to make payments fast, convenient, scalable, and safe in the last few years. Early success promises many new possibilities of digitizing those offline transactions that had never been in the reach.
 Interoperability & Open Development	Payment systems should be interoperable to promote innovation and also allow flexibility and choice to the consumers. Foundations of contactless technology, associated standards, and their adoption into different form factors must support building up interoperable payment systems.
 Flourishing Hyper Local Commerce	The technology innovation ecosystem is ripe for digitizing hyperlocal commerce to bring many untouched and offline transactions in its net. However, small regional banks and financial institutions that can take the revolution to the remotest part are still not part of it.
 Smart City & National Programs	There is enough evidence of the utility of contactless technologies in automated fare collection and low-value payments like Metro and BRTs. It transformed toll collection from the in-mobile vehicle under the National NETC program. These successes can give birth to many local and national level ideas to leverage these technologies.
 Robustness of Contactless Technologies	Contactless technologies, RFID and NFC, are robust, thanks to continual innovation and enabling standards. Their integration with different form factors, card, and mobile, also passed critical security examinations. security evolved to withstand the security attacks even at the scale contactless payments are operating now.
 Security Research	Although many efforts are already on, contactless payments demand continual research to maintain the security baseline, to digitize all possible offline transactions, reduce friction, and minimize cognitive burden. In addition to focusing on threats and vulnerabilities, design and architecting solutions and leveraging benefits from the modern crypto need cautious attention.
 Transaction Failure	Transaction failures raise doubts about the trustworthiness of digital payment mediums. Without market-driven incentives, the players involved in the transaction processing chain would not invest in upgrading the network to support an exponential rise in transactions.
 Public Perception	Despite proven robustness, myths loom over public perception about contactless payments. Hence, continuous engagement is required to dispel these myths and build trust in it.

Recommendations

Contactless payments are on an upward trajectory. The overall of growth, adoption, ease of use and penetration depends on various factors. To further boost the positive momentum, the report consolidates them in the following recommendations:

Contactless by Design: The pandemic brought attention to contactless payments, but the benefits go beyond. It increases the speed of transactions by ten times and offers enhanced security, tremendous flexibility, and supports rising scale. Design efforts of new payment system should take cognizance of these offerings. They should make cautious efforts to make payments, contactless.

Emphasis on Interoperability: The payment system removes frictions, offers flexibility, relieves consumer burden, and supports larger designs if it is free from closed-loop design clutches. The early success of offerings such as transit cards for leading metros offered by leading payment networks is a great testimony of it. Interoperability should be the primary design goal of the new payment system. It should integrate well with all commonly available no-touch experiment technologies and open to combining with downstream innovations happening around them. It should also blend well with upstream developments seen in payment applications, devices, cards, and larger systems devised for scale.

Investment in Technology Infrastructure and Network: Transaction failures question the trustworthiness of the payment systems. Low value and high volume characterize the modern payment paradigm. Banks and other entities in the chain have to invest in upgrading their infrastructure and network to cater to the rising volume. Insistence on zero MDR (Merchant's Discount Rate) on certain payment types removes incentives for the investment. The market-driven incentives regime will automatically take care of it.

Standard-based approach to Technology: Standard evolved around RFID and NFC, preferred no-touch experience technologies, trigger the innovation and adoption of contactless methods. New attack vectors would challenge the current security baseline. The standard-based approach provides a better, predictable, and scalable answer to address these challenges. As discussed, the standard-based approach works at three different levels:

- Technical specification level
- The level where solutions are accepted
- The level where payment service providers demonstrate assurance

Open Framework & Specification for Use Cases & Larger Programs: Open Framework and specification in the NCMC and NETC programs could create a more participatory ecosystem. Contactless payments have the potential to transform new areas, and multiple use cases would evolve. A cautious approach of making them open and specification driven will create a multiplier ecosystem.

Local Financial Ecosystem to support Hyperlocal Commerce Boom: Hyperlocal commerce has witnessed significant momentum due to contactless payments. Though smaller issuers and regional banks may have been excluded from this boom, as they cannot issue credit cards.

Promotion of Innovation and Experimentation: Contactless technologies, within a short span of time have revolutionized digital payments. They can transform many offline and digital transactions to be performed by contactless mediums.

The recent RBI announcement for allowing offline payment and notification of the first cohort for offline technology evaluation in the sandbox underlines the area's importance. Contactless technologies can add critical value to the effort. RBI sandbox is a significant step forward and

it needs to be further nurtured to accelerate innovation and experimentations.

Security Research: Continual research, technology upgradation, and efforts of the ecosystem players have contributed to the robustness of contactless technologies. As the technologies adopted in scale, the success of more extensive programs hinges on security research; careful attention is required for security preparedness and its strength against the evolving attack systems. Apart from finding security issues and vulnerabilities, the effort should also target building up secure systems.

Modern Cryptography role in Contactless Payment: It helps to solve security and privacy problems and allows innovations in enabling contactless payments. Apart from encrypting communication, authenticating cards, modern cryptography offers lightweight solutions that can help take contactless payment to different form factors. It can even allow novice users to digitally transact securely.

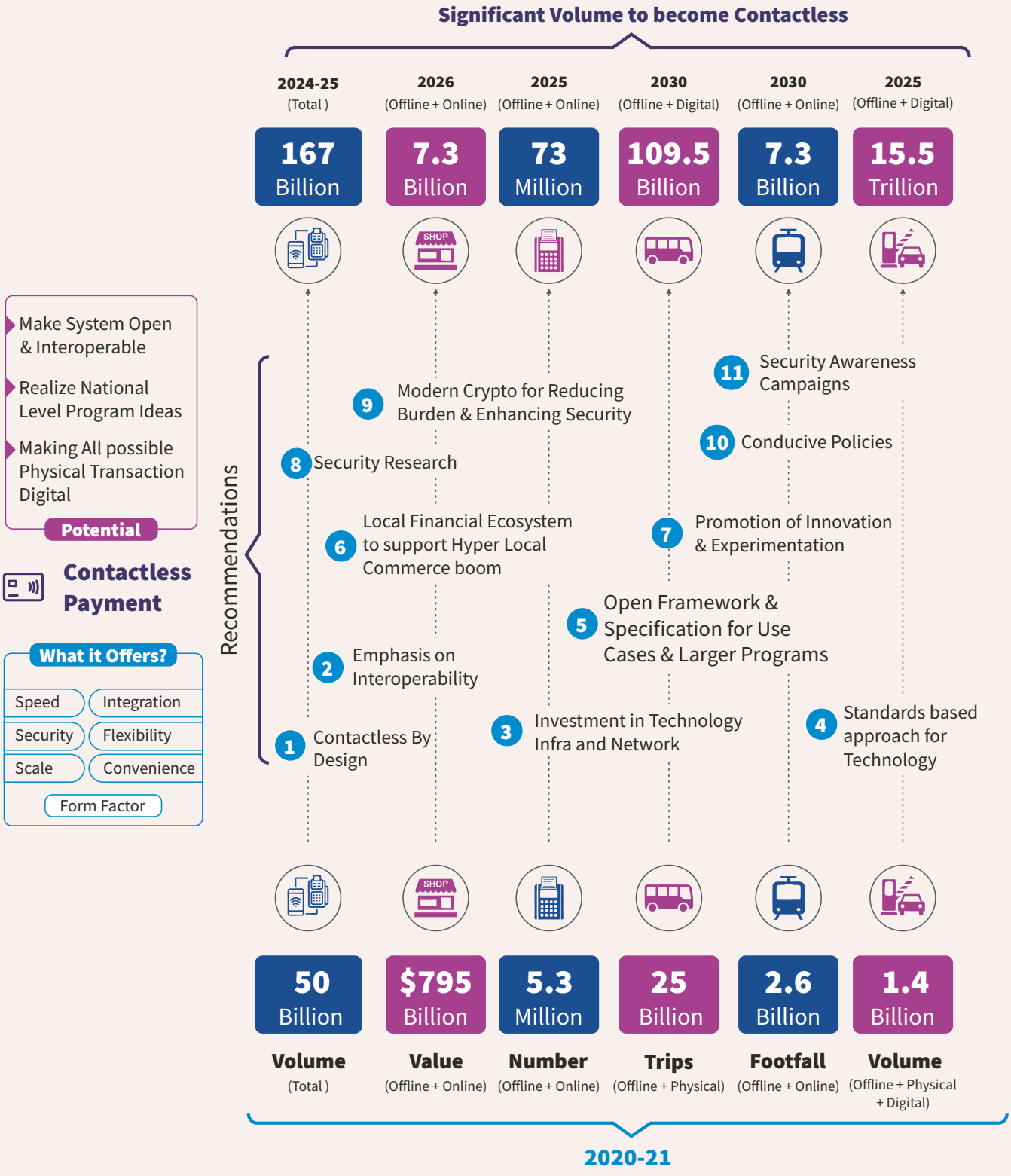
Conducive Policies: Contactless technology until now has met with conservative policies that put limitations on the transactions, inhibiting issuance of contactless cards, and prohibiting the small banks from offering payment facilities. It has begun to change due to the pandemic as many countries have raised limits and lifted prohibitive rules. However, policymakers should see the potential contactless technologies and the role they would play to add contactless transactions to the digital channel. These technologies deserve proactive and conducive policy support.

Security Awareness Campaigns: Many safety and security myths are still associated with contactless payments. The policymakers and players in the ecosystem should develop concerted awareness campaigns to dispel these notions around contactless payments. The trust of the consumer will accelerate the adoption of contactless technologies multi-fold.

16 WAY FORWARD

Contactless payment has proven its worth by offering enhanced security, supporting scalability, showcasing flexibility to possible experiments, working on various form factors, increasing transaction speed, integrating with apps and devices, and more importantly, adding to the convenience of the consumer. It has the potential to digitize all possible physical transactions. Standard-based evolution makes it possible to support open and interoperable payment systems. Contactless technologies helped realize crucial goals of national programs, as seen in the case of National Electronic Toll Collection (NETC) and National Common Mobility Card (NCMC). The figure below depicts how contactless payments can become a prime driver behind digitizing payments in India.

Figure 10: Depiction of the growth potential of Contactless Payments



Way Forward

The share of contactless payment will rise multi-folds owing to the fast growth in Digital Payments. It can prove to be the backbone of the retail boom which is expected in the coming five years. Most of the payment terminals are likely to get enabled with contactless technologies. Urban transportation, both bus and metro, would get smart by deploying contactless ticketing systems. The closed system would become open, interoperable, and consumer friendly. Cloud delivered platform-agnostic APIs will make contactless technology more open for various new use cases. The rapid rise of toll collection from FASTags has already proved how it can become a prime driver to more extensive programs.
To realize the full potential of contactless payments, we need serious reflection on the steps undertaken. We need to have concerted strategies to keep the momentum growing.

Report Team

Mastercard Team

Latika Taneja
Director, Public Policy and Government Relations, South Asia

Rohan Sirkar
Director, Public Policy, South Asia

Sujay Vasudevan
Vice President, Cyber & Intelligence Solutions (C&I), South Asia

Vikas Saraogi
Vice President, Merchant Acceptance, South Asia

DSCI Team

Aditya Bhatia
Sr. Consultant

Amit K Ghosh
Manager - Communications

Anand Raman
Assistant Manager - Research

Vinayak Godse
Vice President

FTI Consulting Team

Amrit Singh Deo
Senior Managing Director, Strategic Communications

Prasanto K Roy
Senior Director, Strategic Communications

Subhodeep Jash
Director, Strategic Communications

About DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

About Mastercard

Mastercard is a global technology company in the payments industry. Its mission is to connect and power an inclusive, digital economy that benefits everyone, everywhere by making transactions safe, simple, smart and accessible. Using secure data and networks, partnerships and passion, its innovations and solutions help individuals, financial institutions, governments and businesses realize their greatest potential. Its 'decency quotient' or DQ drives its culture and everything it does inside and outside the company. With connections across more than 210 countries and territories, Mastercard is building a sustainable world that unlocks priceless possibilities for all.

In India, Mastercard invested over a billion US dollars between 2014 and 2019 to expand fintech capabilities. In 2019, it announced an additional USD 1 billion towards developing value-added services such as fraud mitigation, authentication, tokenization, cybersecurity, intelligence solutions, and data analytics. With offices in Gurugram, Mumbai, Bangalore and Pune and Vadodara, its 4,000 employees in India make up a fifth of the company's worldwide staff and its second largest employment base in the world. India also serves as a global operations hub for Mastercard, supporting not only India but all markets where Mastercard is accepted.

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, 4th Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries, contact:

E: info@dsci.in | W: www.dsci.in

DSCI_Connect dsci.connect dsci.connect data-security-council-of-india dscivideo