Vijeta'2021 On...
Digital Banking

Dear friends,

The process of promotion from Clerical to Officer cadre and from Officer cadre to higher scales has already been initiated. This has brought lot of excitement and enthusiasm among all cadres. Team MDI, therefore, has come out with latest version of Vijeta-Jan 2021 for all aspirants. This book is also helpful for those, who are not appearing for promotion but wish to update their knowledge.

In the present day scenario, it is very important to have knowledge of digital banking. As we all know, fraudsters are poring over mind boggling tricks to fool the customers as well as bankers, therefore, bankers need to have up to date knowledge in IT & adopt latest technology regarding Card products, Net banking and other digital tools.

This special edition of Vijeta on IT, ITES and ADC products will be helpful for clerks and Officers alike while preparing for their promotion test as well as upgradation of their knowledge or in their day-to-day banking operations.

In the present situation when entire world is passing through Corona virus pandemic, it has become more pertinent to adopt digital platform for safe banking without being exposed.

We fervently hope that this special edition of 'Vijeta-January 2021-IT' will succeed in adding value to the knowledge of the readers. We shall be glad to receive any suggestions from you.

With best wishes,
Stay safe.

Vivek Prabhu
Deputy General Manager & Principal

Digital Banking

Digital Payments – Changing scenario

Earlier, when we used to talk about Digital Banking in India, the industry in India was lagging behind many developing nations. It was due to the increased use of legacy systems, huge costs of running branches, and outdated technology that could not be upgraded. Since then, India witnessed gradual yet dynamic growth in Digital banking.

Digital banking means the digitalization of the traditional banking activities and services that were earlier only available when customers visited the bank branch in person. Banking is done through digital platforms. The banking services can be accessed through smartphones, laptops, etc.

The need for computerization of the banking sector was felt in the late 1980s. Therefore the Reserve Bank set up a committee in this regard in 1988 headed by Dr. C. Rangarajan.

Banks started using information technology initially with the introduction of standalone Personal Computers and migrated to Local Area Network connectivity. Then with further evolution, banks adopted the core banking platform. It was when branch banking was changed to bank banking.

Core banking solution allowed banks to raise the comfort aspect to the customers, and it was hailed as a promising step towards improving customer convenience through the so-called “Anywhere and Anytime Banking”. Now it is known or termed as FPC Banking (Faceless, Paperless and Cashless Banking).

Thereafter the process of computerization kicked up with the opening of the economy in the early 90s. A major propeller for this transformation was due to the rising competition from private and foreign banks. Many commercial banks started adopting digital customer services to stay competitive.

The Indian digital payment space has seen extraordinary growth in the last few years, with the volume of transactions increasing at an average compound annual growth rate (CAGR) of 23%.1 The launch of new and innovative payment products like Unified Payments Interface (UPI), National Electronic Toll Collection (NETC) and Bharat Bill Pay Service (BBPS) have firmly placed the digital payment industry on an upward growth trajectory.

With new payment technologies and use cases across sectors emerging, this growth momentum is expected to continue. COVID-19 will be a minor blip in the growth story and then prove to be an inflection point as transactions saw a minor drop in the early months of FY 2020–21 and have now begun to go back to pre COVID-19 levels. We have seen a V-shaped recovery post the pandemic, as the outbreak accelerated the shift to digital platforms. Businesses are now looking to integrate both online and offline channels in order to provide an Omni channel experience to their customers. UPI recorded the highest number of transactions ever in September and volumes have already gone back to pre-lockdown levels. We've also seen a similar recovery in NETC transactions.

Growth in digital payments in India has been driven by multiple factors such as the launch of new and innovative payment products, increasing smartphone adoption, a growing need for faster payment modes, and a strong push from the Government and regulators towards adoption of digital channels. Prior to 2010, digital transactions saw single-digit growth. From 2010–2016, this figure rose to 28% owing to the launch of faster payment modes in the country and jumped to 56% in 2016–17 following demonetization. COVID-19 has further accelerated the shift to digital payment modes. Together, these factors are likely to create a revenue pool of INR 2,937 billion by 2024–25 for payment players – a figure that stood at INR 1,982 billion in 2019–20.

Since its launch in 2016, UPI, has seen an exponential CAGR of 414% until FY19–20 and has become the most preferred payment product in terms of volumes. Person-to-merchant (P2M) payment, which accounts for approximately 40% of the total number of UPI transactions, has become the preferred mode of payment for both online and offline merchants. We expect the volume of UPI transactions to grow by seven times by 2025.

Apart from UPI, BBPS and NETC have also grown at a similar pace. Both BBPS and NETC are growing at a CAGR of 500% and 123% respectively since 2018, with the help of a government and regulatory push.

Banks and non-banking financial companies are now more focused on providing integrated solutions. Digital payments have evolved from being viewed as a cost centre for banks to a revenue centre and a key lever for customer acquisition. Financial companies have stepped up their efforts to strengthen their payment infrastructure and have started offering other adjacent services such as lending, wealth management, micro insurance, and use of data analytics to offer for more customized solutions for customers

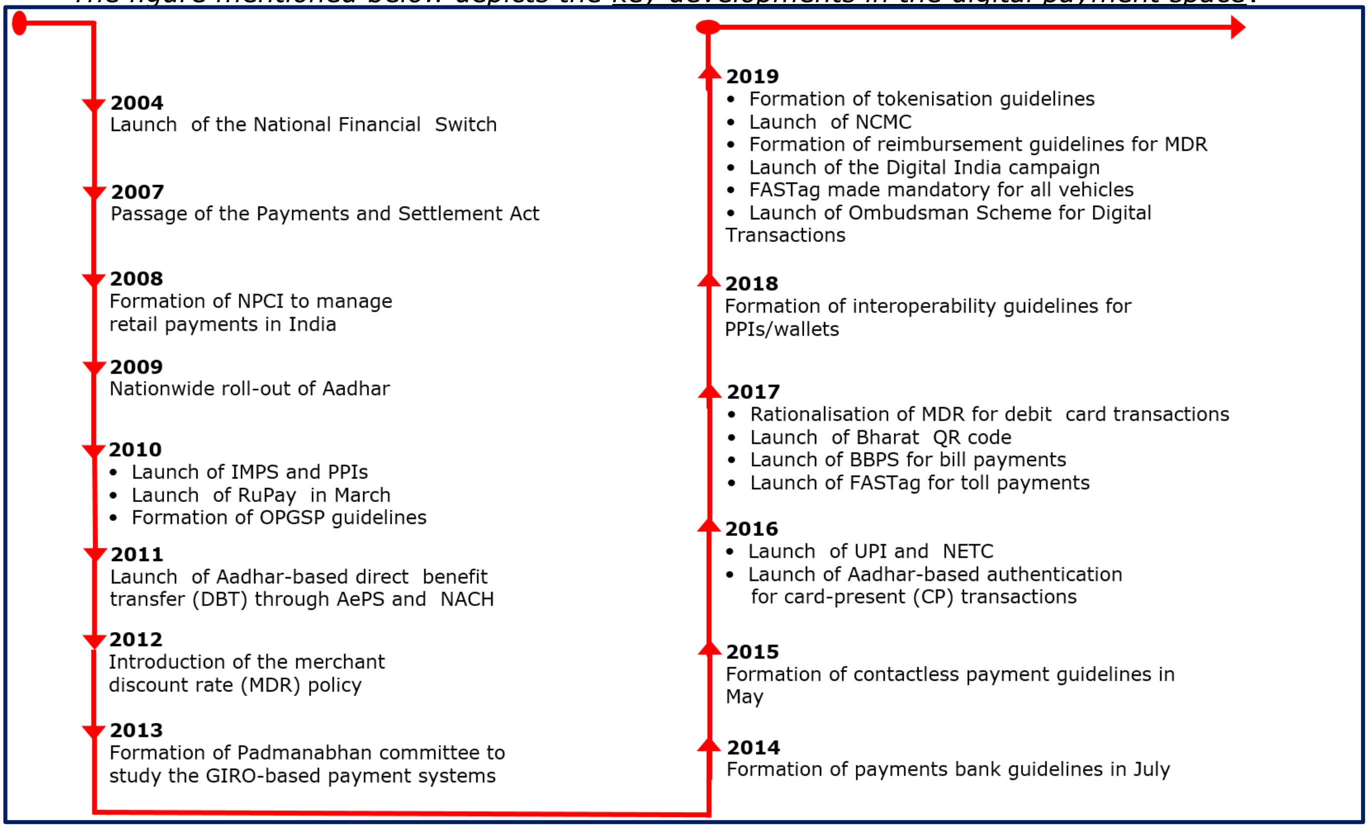
The digital payments industry is poised for a transformation that will enable it to improve the customer experience while making payments online. We believe the digital payment ecosystem will flourish with continuous efforts from the Government, regulators and payment companies to increase awareness and trust. We believe that the future success of digital payments will be driven mainly by the factors below:

- Overlay services will help businesses in creating value for their customers and improve profitability
- Contextual payments will help in leveraging data analytics and AI to understand customer behavior
- Offline payments will provide the next big push to digital transactions as the focus is shifting to this mode and the Reserve Bank of India (RBI) has started encouraging companies to develop an offline payment mode for using cards, wallets and mobile phones to conduct banking transactions
- Invisible payments have also gained traction owing to the pandemic and have the potential to drive the course of digital payments in India.

The last few years have witnessed tremendous growth in digital payments in the country. Digital modes like electronic fund transfer have seen greater adoption, along with increased use of cards backed by customer propositions around loyalty and privilege programmes, exclusivity, etc., and an increase in the merchant base aided by a proliferation of e-commerce sites and apps.

Over the years, successive governments and the RBI have issued enabling guidelines that have been instrumental in driving the growth of digital payments in India.

The figure mentioned below depicts the key developments in the digital payment space:-



2004
Launch of the National Financial Switch

2007
Passage of the Payments and Settlement Act

2008
Formation of NPCI to manage retail payments in India

2009
Nationwide roll-out of Aadhar

2010
- Launch of IMPS and PPIs
- Launch of RuPay in March
- Formation of OPGSP guidelines

2011
Launch of Aadhar-based direct benefit transfer (DBT) through AePS and NACH

2012
Introduction of the merchant discount rate (MDR) policy

2013
Formation of Padmanabhan committee to study the GIRO-based payment systems

2014
Formation of payments bank guidelines in July

2015
Formation of contactless payment guidelines in May

2016
- Launch of UPI and NETC
- Launch of Aadhar-based authentication for card-present (CP) transactions

2017
- Rationalisation of MDR for debit card transactions
- Launch of Bharat QR code
- Launch of BBPS for bill payments
- Launch of FASTag for toll payments

2018
Formation of interoperability guidelines for PPIs/wallets

2019
- Formation of tokenisation guidelines
- Launch of NCMC
- Formation of reimbursement guidelines for MDR
- Launch of the Digital India campaign
- FASTag made mandatory for all vehicles
- Launch of Ombudsman Scheme for Digital Transactions

To boost digital transactions and enhance security as well as customer convenience, the RBI has taken numerous steps such as the adoption of the National Common Mobility Card (NCMC), licenses to White Label ATM operators, issuance of Europay, MasterCard and Visa (EMV) and Near Field Communication (NFC) based cards and customer grievance redressal. The Government played an active role in popularizing digital payment instruments by organising Digi-Dhan Melas across the country and incentivizing customers and merchants through the Lucky Grahak Yojana and Digi-Dhan Vyapari Yojana and cashback offers at fuel stations on payments through digital modes.

The growth and potential of digital payments have allowed numerous FinTechs and payment companies to flourish in recent years. Payment companies have leveraged investor funding to diversify their existing product portfolio and become full-stack financial service providers, with a lot of them venturing into lending, wealth management and insurance aggregator platforms. Customers are now offered a one-stop solution for all their financial needs, and this has significantly boosted the customer experience.

Future of top payment modes

From cash as the primary mode of payment and usage of debit cards being limited to cash withdrawals at the beginning of the century, the Indian payment landscape has evolved to widespread adoption of multiple payment products and systems like prepaid payment instruments (PPIs), Immediate Payment Service (IMPS), UPI, NETC, BBPS and Aadhar- enabled Payment Service (AePS). Use cases of cards for e-commerce transactions have expanded and form factors have changed through tokenisation. IMPS and UPI have provided faster mobile-based payment options to customers. Low- value transactions are increasingly being made through these modes, and prepaid wallets and cards are also emerging as other preferred options.

These instruments have helped acquirers (banks) deepen their merchant base.

BBPS has provided an organized platform for bill payments. Similarly, NETC and NCMC have allowed digitization of payments at toll gates on highways and public transport respectively. In addition, players are offering remittance services to the migrant population.

The COVID-19 pandemic, which brought the global economy to a standstill, triggered a transformation in payments, and customers are expected to increasingly opt for contactless, QR and mobile-/wearable-based digital payment modes.

In addition, wallet providers received an impetus after the RBI announced a new PPI category, and wallets are likely to see greater adoption in the near future.

Payment and Settlement Systems in India: Vision – 2019-2021

PAYMENT AND SETTLEMENT SYSTEMS IN INDIA: VISION – 2019-2021

Empowering Exceptional (E)payment Experience

1. FOREWORD

1.1 Payment and settlement systems are the backbone of any economy. The last decade has witnessed substantial developments in this area of activity across the country. The Reserve Bank of India (RBI), under powers from the Payment and Settlement Systems Act, 2007, has endeavored to ensure that India has 'state-of-the-art' payment and settlement systems that are not just safe and secure, but are also efficient, fast and affordable. Efforts in this direction has yielded handsome results. The planned development of the payment systems has been guided by RBI's vision document for the payment and settlement systems in India which is being put out in the public domain since the year 2002; the last in this series was the Payment Systems Vision 2018. The current Vision document outlines the road map for the three-year period spanning from 2019 to 2021.

1.2 Some of the positive outcomes of the developments during the period 2015-2018 include ushering introduction of new and innovative systems, distinctive shift from paper to electronic payment modes, sizeable increase in transaction turnover, customer centric initiatives, international recognition, etc. Growth in electronic payments has been substantial with retail payments reflecting large growth in volume terms, while the Systemically Important Financial Market Infrastructures (SIFMIs), such as the Real Time Gross Settlement (RTGS) system and Financial Markets Clearing through Clearing Corporation of India Ltd. (CCIL), dominate in value terms.

1.3 New challenges have arisen requiring new strategies and planned efforts to address them. While building on the constructs and achievements of the previous Vision, the Payment Systems Vision 2021 recognizes the need for continued emphasis on innovation, cyber security, financial inclusion, customer protection and competition.

2. REVIEW OF ACHIEVEMENTS OF THE VISION – 2018

2.1 The Payment Systems Vision 2018 of the Reserve Bank envisaged building of 'best-in-class' payment and settlement systems for a 'less-cash' India through the four strategic pillars of responsive regulation, robust infrastructure, effective supervision and customer centricity. The Vision 2018 has facilitated (a) continued decrease in the share of paper-based clearing instruments; (b) consistent growth in individual segments of retail electronic payment systems such as the National Electronic Funds Transfer (NEFT), Immediate Payment Service (IMPS) and card transactions; (c) increase in registered customer base for mobile banking; (d) launch of new products like Unified Payments Interface (UPI) and Bharat QR (BQR); (e) significant growth in acceptance infrastructure; and (f) accelerated use of Aadhaar in payment systems.

2.2 An assessment of the achievements during the three years covered by Vision 2018 reveals that the goal posts indicated above have been accomplished; in respect of the accelerated use of Aadhaar in payment systems, the matter is under review in light of the judgement of the Honorable Supreme Court regarding storage of Aadhaar data.

2.3 Quantitatively measured, digital payment transaction turnover vis-à-vis GDP (at market prices-current price) increased from 7.14 in 2016 to 7.85 in 2017 and further to 8.42 in 2018., The turnover in payment transactions (after including CCIL figures and paper) vis-à-vis GDP (at market prices-current price) increased from 14.41 in FY 2015-16 to and 14.73 in FY 2016-17 and further to 15 in 2017-18.

2.4 Debit card usage at Point of Sale (PoS) vis-à-vis ATM is 30.1% of total in terms of volume (10.4% in 2014-15).

3. PAYMENT SYSTEMS VISION – 2021

CORE THEME – EMPOWERING EXCEPTIONAL (E)PAYMENT EXPERIENCE

Vision Statement – Empower every Indian with access to a bouquet of e-payment options that is safe, secure, convenient, quick and affordable.

3.1 The Vision 2021 for payment and settlement systems in India enhances the strong foundation built over the last two decades. While the pursuit towards a 'less cash' society continues, accompanied by the ambition to have a less-card India as well, the endeavor is to also ensure increased efficiency, uninterrupted availability of safe, secure, accessible and affordable payment systems as also to serve segments of the population which are hitherto untouched by the payment systems. The decade to follow will witness a revolutionary shift in the way Indian citizens use digital payment options and will also empower them with an e-payment experience that will be exceptionally safe, secure and truly world class.

3.2 Vision 2021 concentrates on a two-pronged approach of, (a) exceptional customer experience; and (b) enabling an eco-system which will result in this customer experience. With this in view, the Vision aims towards,

- enhancing the experience of **Customers**;
- empowering payment **System Operators and Service Providers**;
- enabling the **Eco-system and Infrastructure**;
- putting in place a **Forward-looking Regulation**;
- supported by a **Risk-focussed Supervision**.

3.3 To achieve the above, the Vision envisages four goal-posts (4 Cs) – Competition, Cost, Convenience and Confidence. For enhancement of Competition in the payment systems landscape, specific thrust areas like creating regulatory sandbox, authorising new players, etc., have been incorporated; this along with the presence of multiple players in the market is expected to achieve optimal Cost for the customers; freer access with availability of multiple payment system options anytime-anywhere should cater to the requirement of

Convenience; the ‘no-compromise’ approach towards safety of payment systems should address security vulnerabilities to retain customer Confidence.

3.4 It is recognised that cash entails a significant cost to the whole economic system, including consumers. Migration to digital modes of making a payment can obviate some of these costs and can give customers a friction-free and enjoyable experience. Giving them multiple options is expected to make this experience exceptional, apart from furthering growth measurable in terms of digital payments turnover to GDP.

3.5 The savings achieved at all levels on account of digitization of payments need to be considered in pricing of these services to the end customers. Payment System Operators (PSOs) need to consider cost of accessing and managing transactions and accordingly price their services. The aim is towards progressive reduction in ‘per-transaction' cost to customers keeping in view the marginal cost advantage with increase in the number of transactions. The need to move towards marginal cost of pricing based on volume of transactions handled needs no over-emphasis.

4. EXPECTED OUTCOMES OF VISION 2021

4.1 The Payment Systems Vision 2021 covers the period up to December 2021.

4.2 Vision 2021 focuses on further enhancements / improvements in all facets of payment systems.

4.3 With concerted efforts and involvement of all stake holders, the four goal-posts of Vision 2021 with 36 specific action points over the 36-month timeframe will have the following 12 specific outcomes:
(i) Further decrease in the share of paper-based clearing as a percentage of retail payments, particularly in terms of number of paper instruments processed. Given the current trend in cheque usage and the thrust to shift to digitised transactions it is expected that the volume of cheque-based payments would be less than 2.0% of the retail electronic transactions by 2021.

(ii) Accelerated growth in individual retail electronic payment systems, both in terms of number of transactions and increased availability. Payment systems like UPI / IMPS are likely to register average annualised growth of over 100% and NEFT at 40% over the vision period. The number of digital transactions is expected to increase more than four times from 2069 crore in December 2018 to 8707 crores in December 2021.

(iii) Measurably, the digital payment transaction turnover vis-à-vis GDP (at market prices-current price) is expected to further increase to 10.37 in 2019, 12.29 in 2020 and 14.80 in 2021. Payment transaction turnover, including CCIL transactions and paper, is expected to be 22.30 times the GDP (at market prices-current price) by December 2021.

(iv) Increase in use of digital modes of payment for purchase of goods and services through increase in debit card transactions at PoS (35% increase during the vision period) and continued growth in PPI transactions.

(v) Usage of debit cards at PoS transactions is expected to be at least 44% of total debit card transactions (at PoS + ATM). In value terms it is 15.2 per cent in 2018-19 (5.2 per cent in 2014-15) which is expected to be 22% by end 2021.

(vi) Increased deployment of card acceptance infrastructure across the country including at smaller centres with a substantial portion of the infrastructure taking care of processing contactless card payments. Given the current growth trend it is expected to have 5 mn active PoS by end 2021; digital PoS (QR code) is also expected to increase substantially; and the total card acceptance infrastructure will be up scaled to six times present levels by end 2021. This is expected to support aim of cash-lite economy and also shift Cash on Delivery (CoD) transactions to digital modes for e-commerce.

(vii) While no specific target is considered for cash in circulation, the enhanced availability of PoS infrastructure is expected to reduce demand for cash and thus over time achieve reduction in Cash in Circulation (CIC) as a percentage of GDP.
(viii) Further facilitation of mobile based payment transactions as gauged on basis of the registered customer base (expected increase of 50% considering the base effect).

(ix) Enhanced usage of electronic payment systems is expected to reduce the marginal cost given the additional volume. The pricing of such services to customers should, over the vision period, show reduction of at least a 100 bps from current levels. Plus, a shift from ad valorem rates to per transaction rates is envisaged, as usage of a system is irrespective of the value of a transaction.
(x) Security of systems and customer centricity as reflected by –

a. Decrease in Technical Declines reported across various payment systems by 10% year-on-year.
b. Reduction in Business Declines reported across various payment systems by 5% year-on-year. This will be achieved through targeted hand-holding of merchants and customers with customised campaigns by partnering with system operators and system participants.
c. Improvement in Turn Around Time (TAT) for resolution of customer complaints by PSOs.

(xi) FTS [Fraud to Sales (Fraud value / Sales value) x 10000] count for payment systems is expected to be less than 10 bps for most of the payment systems.

(xii) Enhanced healthy competition in the payments space and establishment of new PSOs during the Vision period is envisaged.

4.4 The focus of the Reserve Bank through Vision 2021 is outlined in the subsequent sections. For better understanding and clarity of role, responsibilities and expectations, the identifiable stakeholders for achievement of the various objectives, are delineated in this document. The action points emphasising the four specific goal-posts are summarised in this table –

Goals-posts for Payment System Vision 2021			
COMPETITION	**COST**	**CONVENIENCE**	**CONFIDENCE**
1. Self-Regulatory Organisation for all PSOs (para 5.2.1)	1. Accessible, affordable and inclusive services (para 5.1.1)	1. Harmonizing TAT for resolution of customer complaints (para 5.1.2)	1. Increased coverage of the Cheque Truncation System (para 5.3.6)
2. Encourage and facilitate innovation in an environment of collaborative competition (para 5.2.2)	2. Review of corridors and charges for inbound cross border remittances (para 5.1.7)	2. Setting up a 24x7 helpline (para 5.1.3)	2. Increased scope and coverage of the Trade Receivables Discounting System (TReDS) (para 5.3.7)
3. Feature phone-based payment services (para 5.2.3)	3. Inter-operability and building capability to process transactions of one system in another system (para 5.3.4)	3. Enhancing awareness (para 5.1.4)	3. Geo-tagging of payment system touch points (para 5.3.8)
4. Off-line payment solutions (para 5.2.4)	4. Acceptance infrastructure to address supply-side issues (para 5.3.5)	4. Conducting customer awareness surveys (para 5.1.5)	4. Contact-less payments and tokenization (para 5.4.3)
5. USSD-based payment services (para 5.2.5)	5. System capacity and scalability (para 5.4.2)	5. Internal ombudsman for digital payments (para 5.1.6)	5. Enhanced security of mobile-based payments (para 5.4.8)
6. Global outreach of payment systems (para 5.3.2)	6. Increasing LEI usage for large value cross border payments (para 5.4.5)	6. National settlement services for card schemes (para 5.2.6)	6. Oversight for maintaining integrity of payment systems (para 5.5.1)
7. Fostering innovation in a responsible environment through regulatory sandbox (para 5.4.1)	7. Regulation of payment gateway service providers and payment aggregators (para 5.4.9)	7. Enhanced availability of retail payment systems and a wide bouquet of offerings (para 5.3.1)	7. Third party risk management and system wide security (para 5.5.2)
8. Review of membership to centralised payment systems (para 5.4.4)		8. Widen scope / use of domestic cards (para 5.3.3)	8. Framework for collection of data on frauds in payment systems (para 5.5.3)
9. Inter-regulatory and intra-regulatory co-ordination (para 5.4.10)		9. Explore adoption of newer technologies including DLT for enhancement of digital payment services (para 5.4.6)	9. Framework for testing resilience of payment systems (para 5.5.4)
10. Benchmarking India's Payment Systems (para 5.5.5)		10. E-mandates / Standing Instructions for payment transactions (para 5.4.7)	

5. SPECIFIC INITIATIVES

5.1 CUSTOMERS

5.1.1 AFFORDABLE, ACCESSIBLE AND INCLUSIVE SERVICES

The Indian payment ecosystem and its constituents are likely to respond well when processes are affordable, and accessibility is simple and wide spread. While the approach of the Reserve Bank will continue to be of minimal intervention in the pricing of charges to customers for digital payments, all efforts will be made towards facilitating the operation of payment systems which are efficient and price-attractive. To this end, service providers should set up pricing structures that are transparent, affordable and do not restrict public from accessing payment system services. The basis shall have to be that pricing is reasonable to encourage usage and also pass-on to the customer the benefit of cost saved on managing cash in the system. The Reserve Bank will require service providers to bring about transparency in pricing. Reserve Bank would consider a review of its instructions on customer charge for its Payment Systems and shift from transaction value-based pricing slabs to a fixed minimum transaction-based pricing. The approach to pricing should be towards recovery of marginal costs and to migrate to a low margin-high volume regime.

(Action – RBI, NPCI and PSOs)

5.1.2 HARMONISING TURN AROUND TIME FOR RESOLUTION OF CUSTOMER COMPLAINTS, INCLUDING FOR CARD TRANSACTIONS

There is need for harmonising the TAT of customer complaints and requisite chargebacks. Such time lines should be reasonable and also in alignment with the instructions issued in respect of customer liability for unauthorised electronic payment transactions. The Reserve Bank will be addressing the various facets in this regard, with the objective of optimal time lines expected to result in customer delight and certainty of conclusion. Recourse to technology-driven dispute redressal mechanisms that are rule-based, transparent, customer-friendly and involve minimum (or no) manual intervention will be advocated / encouraged / appreciated.

(Action – RBI, NPCI and PSOs)

5.1.3 SETTING UP A 24X7 HELPLINE

Customer experience can be enhanced with a general centralised helpline for addressing customer queries in respect of various digital payment products, security aspects, recourse mechanism, etc. This will not only build trust and confidence but also reduce expenditure (both financial and human resources) otherwise incurred on addressing complaints and grievances. The payment service industry level Self-Regulatory Organisation (SRO) proposed in this Vision can facilitate the setting up of an industry wide 24x7 helpline and the large-scale use of technology for customer assistance and complaint redressal.

(Action – RBI, NPCI and PSOs)

5.1.4 CREATING AWARENESS

To give thrust to the regulatory interventions on customer awareness, an industry level initiative needs to be taken for building awareness through generic advertisements and systematically planned customer orientation programmes. Equally important is to create customer awareness for basic cyber-security hygiene. Bankers and operators of the payments systems would have to ensure awareness at their end for strictly following defined secure operational processes. Creation of a Universal Icon / Symbol Set for basic use cases / operations in the area of retail electronic payments will also be explored during the period of this Vision document. Ensuring involvement of and co-operation from all stakeholders can help in achieving a very secure and convenient payment environment, with attendant reduction of Business Declines, and maybe, Technical Declines as well.

(Action – RBI, NPCI and PSOs)

5.1.5 CONDUCTING CUSTOMER AWARENESS SURVEYS

Customer surveys to gauge awareness and usage of various payment services, including digital payment systems amongst various stake holders and individuals would be undertaken by the Reserve Bank. The findings of such surveys will be an important component for policy formulation. Repeated surveys in a location will help assess efficacy impact of various targeted interventions.

(Action – RBI)

5.1.6 INTERNAL OMBUDSMAN BY PAYMENT SYSTEM OPERATORS (PSOS)

The terms and conditions for authorisation of various payment systems by the Reserve Bank require them to put in place a grievance redressal mechanism. The Reserve Bank has also put in place an ombudsman scheme for digital transactions. While PSOs have set up their own mechanism for addressing customer complaints, there is a need to formalise an internal ombudsman in the PSOs so that there is an avenue for swift and cost-effective complaint redressal mechanism within the organisation.

(Action – RBI, NPCI and PSOs)

5.1.7. REVIEW OF CORRIDORS AND CHARGES FOR INBOUND CROSS BORDER REMITTANCES

Remittances play a crucial role for developing economies and have significant welfare implications. While the quantum of remittances depends on a number of factors, the cost of remitting funds is increasingly becoming a key element influencing the size of remittances. High cost of remittance made through formal channels may drive customers to informal channels which are less secure and prone to misuse. The G20 has prioritised the issue of cost of remittances in its agenda and is encouraging appropriate policies at the country level. India has already taken several measures to liberalise remittance schemes to drive competition and thereby reduce costs. Some of the initiatives include facilitating the appointment of more intermediaries / money transfer agents, introducing more official channels to route cross-border remittances, receipt of foreign inward remittances directly into the bank accounts of beneficiaries under the Money Transfer Service Scheme (MTSS), etc.

In order to infuse fair competition in this sphere and bring in transparency in costs, RBI will examine the role that payment services providers (PSPs) can play to ensure friction free remittances at lower cost.

(Action – RBI)

5.2 SYSTEM OPERATORS & SERVICE PROVIDERS

5.2.1 SELF-REGULATORY ORGANISATION (SRO)

Industry self-governance is an important feature in modern economies which is also useful for industry wide smooth operations and development. With time, bodies representing interests of certain segments of PSOs have evolved and have been engaging with the regulator. There is a need for self-regulatory governance framework to foster best practices on important aspects like security, customer protection, pricing, etc. Such an organisation can be constituted to cover the entire gamut of digital PSOs, including retail products of National Payments Corporation of India (NPCI). The SRO will serve as a two-way communication channel between the players and the regulator / supervisor. The SRO will of course work towards establishing minimum benchmarks, standards and help discipline rogue behaviour.

(Action – RBI, NPCI and PSOs)

5.2.2 CREATING AN ENVIRONMENT TO ENCOURAGE AND FACILITATE INNOVATION THROUGH COLLABORATIVE COMPETITION

As announced in the second bi-monthly monetary policy statement 2018-19, that the Reserve Bank would be publishing a consultation paper on the policy to encourage more players to participate in and promote pan-India payment platforms, to give a fillip to innovation and competition. The framework finalised after such consultations and discussions would be implemented. To encourage competition in existing payment systems, a review would be undertaken to consider authorisation of new players including one / few pan-India Umbrella Organisation/s. A framework, transparently delineating minimum entry requirements for any PSO, would also be made public. Need for existing authorised PSOs to essentially have physical presence in India for operating payment systems would also be explored. Increased use of technology in all spheres of the payment system ecospace will be actively encouraged and appreciated. A review of existing policy would be undertaken to encourage / facilitate healthy competition and level playing field among banks and non-banks.

(Action – RBI)

5.2.3 FEATURE PHONE-BASED PAYMENT SERVICES

Availability of mobile telephony devices has democratised payments. As on February 28, 2019, there were 1,184 million wireless telephone subscribers and 532 million wireless broad band subscribers [as per data from Telecom Regulatory Authority of India (TRAI)]. While various reports indicate more than 350 million smartphone users in the country, a large user base of feature phones exists. General innovation in mobile payment services has focused or supported app-based access limited to smartphones and such devices. There is a need to innovate payment services for feature phones to provide the necessary thrust towards enhanced adoption of digital payments by various strata of society which will be vigorously followed for implementation.

(Action – PSOs)

5.2.4 OFF-LINE PAYMENT SOLUTIONS

Consumer behaviour has been driving growth of digital payment systems as more and more consumers are embracing mobile technology. Though mobile internet speed has risen, connectivity issues remain unresolved in large areas. Therefore, providing an option of off-line payments through mobile devices for furthering the adoption of digital payments shall be a focus area during this Vision period.

(Action – PSOs)

5.2.5 USSD BASED PAYMENT SERVICES

The available USSD based services require additional push through review of customer cost and enhanced usage through participation. The payment service providers may add features to scale up the security of the transactions, irrespective of the device security level / environment.

(Action – NPCI)

5.2.6 NATIONAL SETTLEMENT SERVICES

Banks are required to have different settlement accounts for settling card transactions with different card networks. To bring in more efficiency in the system and making the process more graceful, the Reserve Bank shall examine the feasibility of having a single national settlement account for all authorised card networks in consultation with the stakeholders.

(Action – RBI, Card Networks)

5.3. ECO-SYSTEM AND INFRASTRUCTURE

5.3.1 AVAILABILITY OF RETAIL PAYMENT SYSTEMS

Ease of use is often the reason for choosing one platform over the other by the customers looking for instantaneous transactions with confirmation. Reserve Bank would examine the need to consider uninterrupted and round-the-clock availability of various payment systems; gradual enhancement of limits, including differential day-night, holiday limits for transactions, subject to risk management and liquidity management; etc. The need for extending availability of NEFT on a 24x7 basis to facilitate beyond the banking hour fund transfer needs would be examined. Need to add more features to NEFT (faster settlements, staggered payments) will also be examined. Reserve Bank of India will also examine the possibility to extend the timings for customer transactions in RTGS based on industry preparedness and customer demand.

(Action – RBI)

5.3.2 GLOBAL OUTREACH OF PAYMENT SYTEMS

India is home to several innovative digital payment products which are available to the public at low cost anytime anywhere. Many countries have expressed interest in partnering in this growth and replicating our products based on their country specific requirements. Specific interests / requests are being received for implementing CTS, NEFT, UPI, messaging solutions, etc., by certain jurisdictions. There is scope for enhancing global outreach of our payment systems, including remittance services, through active participation and co-operation in international and regional fora by collaborating and contributing to standard setting. RBI will continue to actively participate, involve and engage in discussions in international standard-setting bodies. Leadership role towards regional co-operation in payment systems is also envisaged.

(Action – RBI and NPCI)

5.3.3 WIDEN SCOPE, USE AND REACH OF DOMESTIC CARDS

Domestic cards have stabilised well and the potential for their large-scale use is high. Efforts will be made to increase the scope, coverage and usage of domestic cards, including the RuPay card scheme which was launched in March 2012. Collaborative effort will be initiated among NPCI, banks and the Government to widen and deepen the scope / usage of RuPay cards to enhance its brand value internationally.

(Action – NPCI)

5.3.4 BUILDING CAPABILITY TO PROCESS TRANSACTIONS OF ONE SYSTEM IN ANOTHER SYSTEM

Interoperability of payment systems will be a watch word during the ensuing three-year period. Various retail payment systems will be encouraged to have this feature which provides benefits to all stake holders. The role of standardisation and the use of universally accepted standards will also be enhanced. Inter-operability in and among payment system operators / players will be vigorously pursued.

(Action – RBI and PSOs)

5.3.5 ACCEPTANCE INFRASTRUCTURE – ADDRESS SUPPLY SIDE ISSUES

Acceptance infrastructure, particularly Point of Sale (PoS) terminals / mobile PoS / asset-light terminals, as a percentage of the total number of debit / credit cards is low. There is a need to increase the penetration of acceptance infrastructure in the country. The infrastructure will be upscaled to at least six times of the present levels in the next three years' time.

i. Acquirers: Explore the option of permitting acquiring PoS infrastructure by all regulated entities, subject to regulatory clearance / no objection certificates. Increase in acquirers, like Regional Rural Banks and Non-Banking Financial Companies, to cover a large section of establishments.

(Action – RBI)

ii. Innovation-based new devices: Innovation towards low-cost acceptance devices will be encouraged with a view towards cost reduction, enhanced safety and ubiquitousness.

(Action – RBI)

iii. Acceptance Development Fund (ADF): Creation of an ADF to subsidise acquirers for deploying PoS acceptance infrastructure in tier-3 to tier-6 centers. This would help in facilitating innovation and reducing cost of such transactions.

(Action – RBI)

iv. Bharat QR (BQR): Enhanced usage of signed and encrypted BQR as proactive preventive measure for secure payments

(Action – PSOs)

5.3.6 INCREASED COVERAGE OF THE CHEQUE TRUNCATION SYSTEM (CTS)

Since cheques continue to be an important payment instrument, steps would be taken to enhance the security and efficiency of the present CTS mechanism, including bringing in uniformity and harmony in processes across the three cheque processing grids, apart from steps towards increased coverage and a single settlement. Coverage will be increased across more locations including examining improvement in processes / features and discontinuing recourse to Paper to Follow (P2F) across all State Governments.

(Action – RBI and NPCI)

5.3.7 TRADE RECEIVABLES DISCOUNTING SYSTEM (TREDS)

MSMEs face constraints in obtaining adequate finance given their inability to readily convert their trade receivables into liquid funds. TReDS was envisaged for resolving the liquidity crunch faced by MSMEs by facilitating the financing of their trade receivables from corporate and other buyers, including Government Departments and Public Sector Undertakings (PSUs), through multiple financiers. As on date, three TReDS platforms are operational. The ecosystem is at a nascent stage; thus, over the Vision period, guidelines would be reviewed to provide maximum traction to the platform for achieving the goals of MSME financing by enabling re-discounting, considering some participation of non-MSMEs, expanding financier categories, increasing the number of platforms, on boarding more buyers, etc.

(Action – RBI)

5.3.8 GEO-TAGGING OF PAYMENT SYSTEM TOUCH POINTS

In order to measure the adoption of digital payments, it is essential to have geographical location of the payment system touch points [bank branches, ATMs, PoS terminals, Business Correspondents (BCs), etc.] across the country. The Reserve Bank is examining a framework to capture the location and business details of commercial bank branches, ATMs and BCs. It is envisaged to extend a similar framework to capture and maintain information about PoS terminals and other payment system touch points as well.

(Action – RBI, NPCI and PSOs)

5.4 REGULATION

5.4.1 FOSTERING INNOVATION IN A RESPONSIBLE ENVIRONMENT THROUGH REGULATORY SANDBOX

The regulatory sandbox approach has been gaining traction in several jurisdictions. A sandbox approach to regulation would help enable innovation in digital payments while avoiding any systemic risks. The Reserve Bank's Working

Group Report on FinTech and Digital Banking recommended developing a framework for regulatory sandboxes. Given the evolving nature of payment instruments and technologies used to provide payment services, a framework for a regulatory sandbox for payment systems would be designed to provide a controlled environment, with certain regulatory exemptions, to allow experimentation of new payment system products by traditional and non-traditional players.

(Action – RBI)

5.4.2 SYSTEM CAPACITY AND SCALABILITY

The current approach to authorisation for payment systems is liberal with no prescriptions and / or assessment responsibilities on the payment service providers in terms of performance metrics like uptime, technical declines, capacity, etc. for systems operated by them. At the infant stage of development, this measure was considered necessary to enable service providers to build and enhance capabilities over time. As payment systems have since come a long way, and there is an increasing expectation that the systems should be robust and resilient, a framework for an ongoing assessment of the performance of retail payment systems would be designed. Need for prescribing explicit exit criteria of payment systems and payment system operators based on a transparent point-of-arrival metrics will also be explored.

(Action – RBI, NPCI and PSOs)

5.4.3 CONTACTLESS PAYMENTS AND TOKENISATION

Contactless payments, while decreasing the time taken for payment checkout, also ease payments for small ticket payment transactions. Tokenisation technologies often form the basis of facilitating seamless e-commerce experiences fuelled by mobile and other connected devices. The rapid growth in devices provides a significant opportunity for payments through any form factor and anywhere. For digital payments to take advantage of this opportunity, an appropriate regulatory framework built on the principles of innovation, transparency and consumer control is required. Reserve Bank has already recognized this and authorised certain players to offer mobile payment solutions driven by secure tokenisation standards. RBI would consider a broad-based framework for other payment experiences, keeping in mind customer liability issues and security of authentication mechanisms.

(Action – RBI)

5.4.4 REVIEW OF MEMBERSHIP OF CENTRALISED PAYMENT SYSTEMS

The Reserve Bank continuously receives requests and feedback for payment infrastructure access neutrality between banks and non-banks. RBI has already permitted participation of non-banks in certain payment infrastructure; RBI will initiate discussion to develop a framework for settlement risk management with increased participation of non-banks.

(Action – RBI)

5.4.5 INCREASING LEI USAGE FOR LARGE VALUE CROSS BORDER PAYMENTS

Legal Entity Identifier (LEI) system envisages identification of unique parties to financial transactions across the globe and is designed as an important component for improvement in financial data across the globe. Cross border retail payments are generally less transparent and more expensive than domestic transactions. Given the nature of cross border transactions, there is a case for exploring the option of using LEI to identify the payment service providers, their agents and distributors, in respect of cross border services, particularly for large value payments, including expanding the implementation across all the identified segments.

(Action – RBI and LEIL)

5.4.6 ENCOURAGE ADOPTION OF NEW TECHNOLOGIES INCLUDING DLT FOR ENHANCEMENT OF DIGITAL PAYMENT SERVICES

Technology has been at the centre of payment systems innovation and development. Adoption of Distributed Ledger Technology (DLT) for financial services has been a subject of interest. Various views espouse that adoption of DLT can enhance the operations of payment systems by improving the quality of data and providing additional information for payment transaction, which help automated reconciliation and reversal with high degree of precision. Adoption of DLT will be considered to facilitate industry wide adoption for areas which can benefit from this technology.

(Action – RBI, CCIL, NPCI and PSOs)

5.4.7 E-MANDATES / STANDING INSTRUCTIONS

The Reserve Bank has been receiving requests for allowing e-mandate / standing instructions-based automation of periodically recurring, non-discretionary payments. The Reserve Bank will consider implementation of e-mandates / standing instructions for retail payment systems, subject to customer protection and adequate safeguards like authenticating payment instrument registration, mandating transaction limits, segments, etc.

(Action – RBI)

5.4.8 SECURITY ASPECTS OF MOBILE PAYMENTS

The guidelines for mobile banking issued by the Reserve Bank indicate the technological and security standards which the banks may comply with while providing mobile banking services to their customers. The Reserve Bank would issue specific standards which the banks providing mobile payment services shall comply with, mandate minimum requirements, highlight best practices and initiate discussion on risks emerging from innovative payment channels through emerging technologies including Artificial Intelligence, Internet of Things devices, wearables, etc.

(Action – RBI)

5.4.9 REGULATION OF PAYMENT GATEWAY SERVICE PROVIDERS AND PAYMENT AGGREGATORS

The growth of online payment transactions has led to increasing role of payment gateway service providers. The current guidelines on payment gateway operations (monitored through banks) are indirect and address only a few specific aspects of their functioning. The Reserve Bank has initiated discussion on examining the need for separate guidelines for payments related activities of these entities which will be taken forward during the vision period.

(Action – RBI)

5.4.10 INTER-REGULATORY AND INTRA-REGULATORY CO-ORDINATION

In order to have a coordinated approach towards regulation, the Reserve Bank shall engage with the other sectoral regulators – SEBI, IRDA, TRAI, etc., to remove frictions in regulation and ease system operator / customer comfort. The endeavor will also to have a coordinated approach to regulation and supervision within Reserve Bank across the different related departments – Department of Banking Regulation, Department of Banking Supervision, Department of Non-Banking Regulation, Department of Co-operative Banking Regulation, Financial Markets Regulation Department, Financial Markets Operations Department, Foreign Exchange Department, Customer Education and Protection Department, Department of Information Technology, Department of Economic and Policy Research, Department of Statistics and Information Management, Department of Government and Bank Accounts, etc. Similar engagements with the subsidiaries of Reserve Bank – Institute for Development and Research in Banking Technology (IDRBT), Reserve Bank Information Technology Pvt. Ltd. (ReBIT), etc., will be pursued.

(Action – RBI)

5.5 RISK-FOCUSSED SUPERVISION

5.5.1 PROPORTIONATE OVERSIGHT FOR MAINTAINING INTEGRITY OF PAYMENT SYSTEMS

Security is pivotal and risk management practices should be implemented with conservativeness in approach and ruthlessness in implementation across each and every product. Cyber risks are increasing rampantly with advancement in technology, and increasing adoption of digital services, whether financial or otherwise, is bringing these issues to the forefront. This issue becomes grave given the fact that the nature of threat is dynamic and keeps changing rapidly. The interconnected systems are as safe as their weakest link. There is, therefore, a need for both security against possible cyber-attacks and resilience in the eventuality of such attacks. All payment systems should display explicit levels of safety. It would be necessary that systems not only meet the requirements of safety but are also subjected to safety audits at periodic intervals.

The Reserve Bank undertakes oversight of the payment systems through onsite supervision and off-site surveillance. There is a prescription of self-assessment by the PSOs, which are also required to subject their systems to IS audit through

CERT-In empaneled auditors. For transparency and clarity, there is a need for disclosed supervisory framework for all the stake holders to better understand their roles and responsibilities. The need for publishing oversight reports in public domain by the Reserve Bank would be considered. The feasibility of oversight of cross border entities with the help of information sharing MOUs with overseas regulators will also be examined. The oversight framework for PSOs would also include data reporting and analytics requirements for PSOs.

(Action – RBI, PSOs)

The existing penalty framework for payment system operators will be reviewed and modified, if required, to make the process more transparent and achieve the expected outcomes.

(Action – RBI)

In consultation with the CSITE Cell of the Reserve Bank, the need to subject payment system operators to the same rigour for cyber-security preparedness as the other entities in the financial sector will be looked into.
(Action – RBI)

5.5.2 THIRD PARTY RISK MANAGEMENT AND SYSTEM-WIDE SECURITY

The Reserve Bank had earlier issued guidelines on managing risks in respect of outsourcing of financial services by banks. The need for a separate regulatory framework for outsourcing arrangements by non-bank payment service providers would be examined given the current trend of outsourcing arrangements and the need for security control and clarity of roles and responsibilities of the regulated entities. Such a framework would consider the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. Such a framework would also consider overall security of the digital payments ecosystem by covering the entire payment transaction chain, including the need for establishing end point security. Adoption of PCI (Payment Card Industry) standards can be considered as a desirable best practice by all the entities in a payment transaction chain, irrespective of their status as a regulated entity or otherwise. Need to customise PCI standards to better suit / reflect Indian situations will also be explored.

(Action – RBI, NPCI and PSOs)

5.5.3 FRAMEWORK FOR COLLECTING DATA ON FRAUDS IN PAYMENT SYSTEMS

To further strengthen the confidence in the payment systems and minimise instances of frauds, there is a need to monitor the types of frauds that may be taking place in various payment systems. To this end, there is a need to share fraud related data for payment systems. Such data can be used analytically for differentiating fraudulent and legitimate transactions; oversight and supervision, and also for providing guidelines to entities for minimising risks of similar frauds. This would also help in improving resilience and trust in the system. The Reserve Bank would promote use of such analytics to proactively identify instances and aspire for prediction of frauds to help instant response and recovery actions, such as blocking irregular transactions, before the payment authorisation. The fraud data will be used to influence regulatory decisions and for reducing the incidence and level of frauds in the payments ecospace.

(Action – RBI, NPCI and PSOs)

5.5.4 DRAFTING A FRAMEWORK FOR TESTING RESILIENCE OF PAYMENT SYSTEMS

With the introduction of alternate modes of electronic payments, both for the financial markets, and for businesses and individuals, the resilience of the payment systems has gained importance. Here, resilience refers to the ability to continue to operate even if a system has failed completely by switching activity to a separate system or process or a combination of both. A framework would be drafted for the same. The framework shall also include business continuity and infrastructure redundancy preparedness.

(Action – RBI)

5.5.5 BENCHMARKING INDIA'S PAYMENT SYSTEMS

An efficient payment system reduces the cost of exchanging goods and services and is indispensable to the functioning of the intra-bank, inter-bank, money and capital markets. The past decade has been witness to a number of innovations, especially in retail payments. The Reserve Bank shall conduct an exercise which will aim at benchmarking India's payment systems and gauge India's standing against major countries across all payment systems and payment instruments. Efforts will be towards improving the performance and standing of our payment systems vis-à-vis international / cross-country best practices. The learning points will also be used to improve existing payment system features in the interest of reducing frictions and enhancing acceptance and usage levels. The endeavor shall also be to repeat the benchmarking exercise by expanding coverage and features.

(Action – RBI)

Formation of Digital Banking Department (DBD) at Head Office (BOI)

Indian payments ecosystem is innovating, expanding and evolving. Growth of digital payments continue to be robust. Driven by progressive regulatory policies of the Government and RBI and with the increased use of mobile internet, Indian payment industry has witnessed a significant growth due to the use of technology.

Government of India along with RBI have been taking effective steps to boost digital payments in the country. Incentives for consumers and merchants, robust payment infrastructure, increased digital literacy programs and appropriate grievance Redressal mechanism have led to surge in usage of digital payments.

Mobile wallets, Smart devices, Contactless /QR based payments have increased digital adoption. UPI, through interoperable feature has been witnessing significant growth over the years.

With digital payments gaining popularity, there is an increasing end-user demand for a more seamless payment experience. It is important that the Bank develops more agile, flexible, customer-centric and secure framework for deploying cost-effective and feature-rich digital payment solutions.

In order to meet the expectations and address the challenges faced by all the stake holders a new department "Digital Banking Department" is being made operational from 13-08-2020.

Objectives of Digital Banking Department (DBD)

The focus of Digital Banking Department shall be moving towards less cash economy. The following are the broad objectives of the functioning of Digital Banking Department (DBD).

- Owner of Digital Products, Digital Devices & Cards.
- Product Innovation, Market Research & Analysis of digital products.
- Introduction of Digital Products/Services.
- Improvement, enhancement & enrichment of features/functionalities/services under each digital product for better user experience.
- Ensuring all digital devices are up & functional by maintaining optimum uptime & maximizing number of hits per device.
- Issue of operational guidelines & providing MIS
- Imparting periodical training to field staffs, Call Centre/help desk personnel with the help of Training Centres on product features/functionalities/services
- Periodical review and monitoring of performance under each digital product/channel regarding on-boarding/registrations, volume/value of transactions, unavailability/disruptions of services and impact thereon, business/technical declines etc.

Products and Services under Digital Banking Department

The below mentioned products and services shall be handled by Digital Banking Department.

Acquiring service

- ATM including Mobile ATM, white label ATM
- Cash Recyclers
- National Financial Switch(NFS) & Other Products
- Point of Sale(POS), Mobile POS(MPOS),BHIM-Aadhar Pay

Issuing service

- Card issuance — Debit card, Credit card, Prepaid card, Green PIN, etc.

Delivery Channel

- Mobile Banking, Internet Banking, Star Token NG
- Unified Payment Interface(UPI)
- Immediate Payment Service(IMPS), Instant Money Transfer(IMT),
- Bharat Bill Payment System(BBPS)
- National Electronic Toll Collection(NETC)
- SMS banking
- Loyalty Rewards
- Application Programming Interface(API)-Open Banking
- Online Account Opening
- Ecommerce
- Pass book printing kiosks

Transactions Banking

- National Automated Clearing House(NACH/ACH)(including
- Aadhaar Based Payment) ,Direct Debits
- Public Finance Management System(PFMS)
- Payment Aggregator/Payment Gateway
- Cash Management Services(CMS), Channel Finance, Cheque collection, Doorstep banking for Corporates
- ASBA, Online share trade(3 in 1 A/cs)

Call Centre (Digital Banking services)

- Call Centre & Help Desk related to Digital banking products & services.

Grievances Redressal

- To facilitate branches in resolving issues pertaining to product feature, functionalities and services
- Handling of disputed/fraudulent transactions, prompt refund of failed transactions pertaining to Digital Banking Services as per TAT guidelines of regulator/network associates.

Product Sales and Marketing

For on-boarding more customers into digital banking services, sales and marketing shall be done through Marketing Department.

Apart from explaining functionalities during customer meet/handholding, customers shall be sensitised about doing digital transaction in safe manner and grievances handling mechanism shall also be explained.

Customer feedback on the products and services shall be communicated to Digital Banking Department for continuous improvement in our products and services.

Reconciliation

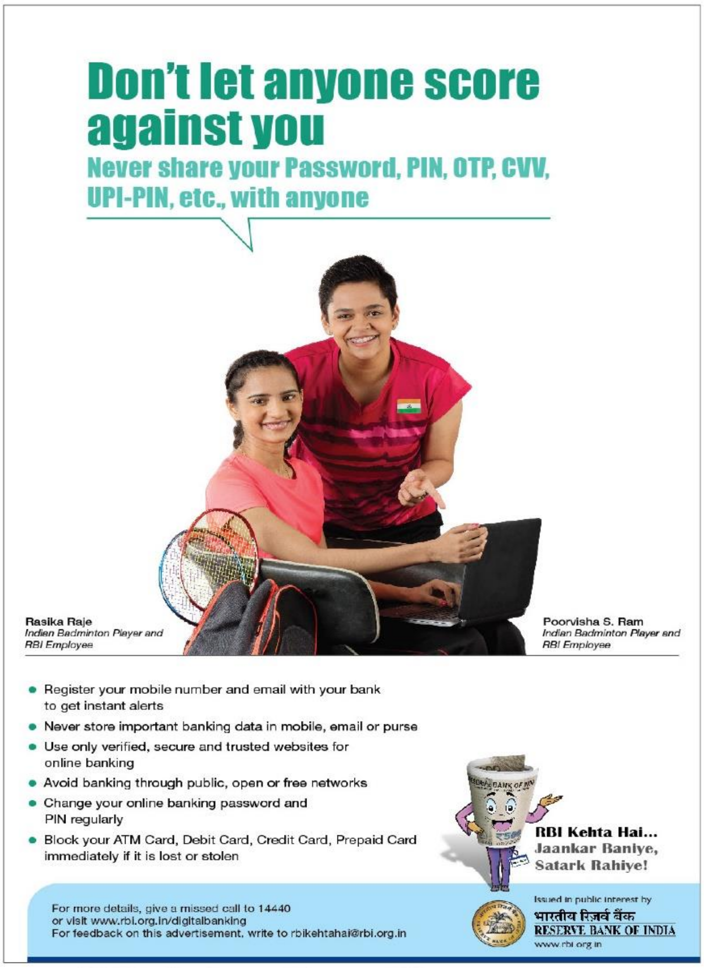
For better control and monitoring Centralised Back Office Department (CBOD) shall be the nodal department for settlement and reconciliation of all digital transactions and related office accounts.

Abolition of ADC, CPD & Transaction Banking Department

With formation of Digital Banking Department the following departments shall cease to exist.

- Alternate Delivery Channels(ADC)
- Card Products Department(CPD)
- Transaction Banking Department

SMS on Safe Digital Banking
Online Banking? Only use sites with https; avoid banking on free networks; regularly change and do not share password/PIN. For more, give missed call on 14440.
IVRS on Safe Digital Banking
Register your mobile number and email with your bank to get instant alerts. If you get an alert about a transaction that you have not initiated or authorised, you can immediately take it up with your bank. You need to take a few more precautions while banking online. For instance, do not store important banking data in your mobile, email or wallet. Use only verified, secure and trusted websites, that is, websites starting with https: for online banking. Avoid banking through public, open or free networks. Change your online banking password and PIN. Block your ATM card, Credit Card, Prepaid Card immediately, if it is lost or stolen.


Don't let anyone score against you
Never share your Password, PIN, OTP, CVV, UPI-PIN, etc., with anyone
RBI Kehta Hai...
Jaankar Baniye,
Satark Rahiye!

Rasika Raje
Indian Badminton Player and RBI Employee

Poorvisha S. Ram
Indian Badminton Player and RBI Employee

- Register your mobile number and email with your bank to get instant alerts
- Never store important banking data in mobile, email or purse
- Use only verified, secure and trusted websites for online banking
- Avoid banking through public, open or free networks
- Change your online banking password and PIN regularly
- Block your ATM Card, Debit Card, Credit Card, Prepaid Card immediately if it is lost or stolen

For more details, give a missed call to 14440
or visit www.rbi.org.in/digitalbanking
For feedback on this advertisement, write to rbikehtahai@rbi.org.in

Issued in public interest by
भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

Digital Banking Products Service Charges W.E.F 01.01.2021

S.N.	CARD/Charges	Revised Charges w.e.f. 01.01.2021
	DEBIT / ATM CARD	
1	**Debit Card Issuance Charge/ Additional Card/ Replacement**	**First Year(Issuance of Debit card):**
	Classic	**Free**
	Platinum	**Free**
	Business Debit	**Free**
	NCMC Debit	**Free**
	Contact Less	**Free**
	Prepaid	**Free**
	Travel Card	**Free**
	Visa Signature (Metal Card)	Rs.4,500/-
	Visa Signature(Plastic Card)	Rs.600/-
	RuPay Select	Rs.800/-
	Additional Card / Replacement Card Conversion of Mega strip Card into EMV Card	
	Classic	For Classic/ NCMC : Rs.150/-
	Platinum	
	Business Debit	Others : Rs.200/-
	NCMC Debit	
	Contact Less	
	Prepaid	
	Travel Card	
	Visa Signature (Metal card)	Rs.4,500/-
	Visa Signature (Plastic card)	Rs.600/-
	RuPay Select	Rs.800/-
2	**Issuance charges for : Non - personalized card (Ready Kits/ Welcome Kits)**	Free
3	**Debit Card Maintenance Charges - (Annual)**	
	Classic /NCMC	For Classis/NCMC:
	Platinum	Rs.150/-
	Business Debit	
	Contact Less	For Others: Rs.200/-
	Prepaid	
	Travel Card	
	Visa Signature (Metal Card)	Rs.4,500/-
	Visa Signature(Plastic Card)	Rs.600/-

S.N.	CARD/Charges	Revised Charges w.e.f. 01.01.2021
	RuPay Select Card shield Facility One time Per year	Rs.800/- **Free**
4	Debit Card Re-pin Charges Green PIN	Rs. 50/- Green Pin : **Free**
5	Surcharge (in case of Debit card usage) on Fuel purchasing (From Fuel station)	NIL
	Surcharge (in case of Debit card usage) on Railway ticket purchasing (From IRCTC)	NIL
	6. Debit Card in Concessional Accounts (Special Charge Code)	
a	BSBDA opened under PMJDY Scheme codes- SB181/ SB182/ SB183/ SB104/ SB105/ SB106/ SB190/ SB101 WITH CHRG_LEVEL_CODE = "NOMIN" and CHRG_COLL_FLG = "N" as per HOBC-111/39	Debit Card Issuance Charge : **Free** Annual Maintenance Charge : **Free**
b	Jai Jawan Salary Plus Account Scheme Scheme code - SB161 (commissioned officers) Scheme code SB 162 (Non-Commissioned officers)	Debit Card Issuance Charge : **Free** Annual Maintenance Charge : **Free**
c	Para Military Forces Scheme code SB 163 & Spl. Charge code 0201	Debit Card Issuance Charge : **Free** Annual Maintenance Charge : **Free**
d	Employees of central & sate govt. universities/college – Scheme code SB163 & Spl. Charge code -0202	Debit Card Issuance Charge : **Free** Annual Maintenance Charge : **Free**
e	Employees of public sector undertaking – Scheme code SB163 & Spl. Charge code 0203	Debit Card Issuance Charge : **Free** Annual Maintenance Charge : **Free**
f	Pvt. Sector employee Scheme code SB163 & Spl. Charge Code 0204	**Debit Card Issuance Charge**: First Year(Issuance of Debit card): **Free** **Annual Maintenance charge:** For Classis/NCMC: Rs.150/- For Others : Rs.200/-

S.N.	CARD/Charges	Revised Charges w.e.f. 01.01.2021
g	BOI Saral Salary account scheme Scheme code SB165 & Spl. Charge code 0202,0203,0204	**Debit Card Issuance Charge:** First Year(Issuance of Debit card): **Free** **Annual Maintenance charge:** For Classis/NCMC: Rs.150/- For Others : Rs.200/-
h	Star Gurukul Savings account - Scheme code SB163 & Spl. Charge Code- **GURU**	**Debit Card Issuance Charge:** First Year(Issuance of Debit card): **Free** **Annual Maintenance charge :** For Classis/NCMC: - Rs.150/- For Others : Rs.200/-
	CREDIT CARD	
7	Issuance & Annual Charges for - **Visa Gold /Platinum International** Credit Card- **Principal**	500.00
8	Issuance & Annual Charges for - **Visa Gold / Platinum International** Credit Card-**Add on**	300.00
9	Issuance charges for: **India Card** (Master Credit Card) - **Principal/ Add-on**	**Free**
10	Annual Maintenance Charges on completion of every year for - **India Card** (Master Credit Card) - **Principal/ Add-on**	**Free**
11	Issuance & Annual Charges for - **Master Platinum International** Credit Card- **Principal**	1000.00 (International) 500.00 (Domestic)
12	Issuance & Annual Charges for - **Master Platinum International** Credit Card - **Add on**	500.00 (International) 300.00 (Domestic)
13	Issuance & Annual Charges - **RuPay Platinum International** Credit Card – **Principal** **Add - on card**	**FREE** **FREE**
14	Annual Charges **SwaDhan Platinum International** Credit Card - **Principal & Add-on Card**	**Free**
15	**Replacement of Credit Card (any variant)**	300.00 Any variant **excluding SwaDhan** Card

S.N.	CARD/Charges	Revised Charges w.e.f. 01.01.2021
	16. Credit Card in Concessional Accounts (Special Charge Code)	
a	**Jai Jawan Salary Plus Account Scheme** Scheme code-SB161(commissioned officers) Scheme code SB 162 (Non-Commissioned officers)	**Issuance Charge:** **For Commissioned Officer :** International gold credit card : **Free** **For Non Commissioned Officers:** India card : **Free** **Annual Maintenance Charge:** Free (in above mentioned cases)
b	**Para Military Forces** Scheme code SB 163 & Spl. Charge code 0201	**Issuance Charge:** Gold Credit Card : **Free** Gold International Credit Card :**Free** **Note**: Gold international credit card to be issued to those employees whose net take home salary is Rs.25,000/- per month. **Annual Maintenance charge:** Applicable as per variant of card
c	**Employees of central & sate govt. universities/college** Scheme code SB163 & Spl. Charge code-0202	**Issuance Charge:** Gold Credit Card : **Free** Gold International Credit Card :**Free** **Note**: Gold international credit card to be issued to those employees whose net take home salary is Rs.25,000/- per month. **Annual Maintenance charge:** Applicable as per variant of card
d	**Employees of public sector undertaking** Scheme code SB163 & Spl. Charge code 0203	**Issuance Charge:** Gold Credit Card : **Free** Gold International Credit Card :Free **Note**: Gold international credit card to be issued to those employees whose net take home salary is Rs.25,000/- per month. **Annual Maintenance charge:** Applicable as per variant of card
e	**Pvt. Sector employee** Scheme code SB163 & SCC 0204	**Issuance Charge:** Gold Credit Card : **Free** Gold International Credit Card :**Free** **Note**: Gold international credit card to be issued to those employees whose net take home salary is Rs.25,000/- per month. **Annual Maintenance charge:** Applicable as per variant of card

S.N.	CARD/Charges	Revised Charges w.e.f. 01.01.2021
f	**BOI Saral Salary account scheme** Scheme code SB165 & SCC 0202,0203,0204	**Issuance Charge:** Gold Credit Card : **Free** Gold International Credit Card :**Free** **Note:** I. **Gold Credit card** to be provided to those employees whose net take home salary of last 6 months is Rs.10,000/- & above. II. **Gold international credit** card to be provided to those employees whose net take home salary of last 6 months is Rs.25,000/- and above. **Annual Maintenance charge:** Applicable as per variant of card
g	**Star Gurukul Savings account** Scheme code SB163 & Spl. Ch. Code - **GURU**	**Issuance Charge:** Gold Credit Card : **Free** Gold International Credit Card :**Free** **Note:** I. **Gold Credit card** to be provided to those employees whose net take home salary of last 6 months is Rs.10,000/- & above. II. **Gold international credit** card to be provided to those employees whose net take home salary of last 6 months is Rs.25,000/- and above. **Annual Maintenance charge :** Applicable as per variant of card
	Credit Card Related Misc. Charges	
17	**Interest free period**	**For Cash Advance/ Withdrawal against Cash advance**: Nil **For Other Transactions**: **21-51 days** (applicable only on retail purchases and if outstanding balance is paid in full on due date)
18	**Charges on Revolving Credit**	**Secured Credit (SwaDhan)-** 1.20% p.m. (15.40% p.a.) on daily balances. In case of default service charges is 1.70% p.m. (22.45 % p.a) **Unsecured Credit (Other than SwaDhan) -** 1.70% p.m. (22.45% p.a.) on daily balances. In case of default service charges is 2.50% p.m. (34.50 % p.a)

S.N.	CARD/Charges	Revised Charges w.e.f. 01.01.2021
19	**Minimum Repayment Amount**	10% of Total Outstanding, if revolving credit is opted + EMI (all EMI due) + other amount due.
20	**Cash Advance Limit /** **Loan Against Card Limit**	**For both Principal and Add-on card:** 50% of Spending Limit or available limit, whichever is lower. Cash withdrawal upto 40% of spending limit of Primary card and upto 20% on Add-on Card. Cash withdrawal per day Rs.50,000 for Platinum card and Rs.15,000 for rest variant One-time processing fees shall be charged along with first EMI.
21	**Cash Advance Charges**	**BOI ATM:** 2% (minimum Rs. 50) for each transaction. **Other ATM:** 2.5% (minimum Rs. 75) for each transaction. **Overseas ATM:** 2.5% (minimum Rs. 125) for each transaction and Currency Conversion Charges, presently 2%. **Interest on dues/overdue applicable**
22	**Star Easy Pay (EMI)**	**Processing Charges** – One-Time - % of the Purchase **Finance Charge -** 1.25 % of the Purchase In case of default service charges is 2.50% p.m. (34.50 % p.a)
23	**Balance Enquiry Charges at ATM** **Payment of charges (Cash / Cheque / Online / NEFT / RTGS)**	**BOI ATM**: Nil **Other Bank ATM in India**: Rs.20/- **Other Bank ATM Abroad**: Rs.25/- **Nil**
24	**Charges on over limit account (Purchase / Cash)**	**Secured Credit (SwaDhan)** 1.70% p.m. (22.45 % p.a) on daily balances **Unsecured Credit** (Other than SwaDhan) 2.50% p.m. (34.50 % p.a) on daily balances
25	**Usage Over Spending Limit**	Rs. 100/- per occasion

<table>
<tr><th>S.N.</th><th>CARD/Charges</th><th>Revised Charges w.e.f. 01.01.2021</th></tr>
<tr><td>26</td><td><b>Outstation Cheque Processing Charge</b></td><td>For prevailing rates please refer to our website.
Charges wef 15.12.2016 are as under:
<table>
<tr><th colspan="2">Cheque Amount (in Rs.)</th><th>Commission (in Rs.)</th></tr>
<tr><td>From</td><td>Upto</td><td></td></tr>
<tr><td colspan="2">Upto 5000</td><td>25</td></tr>
<tr><td>5001</td><td>10000</td><td>50</td></tr>
<tr><td>10001</td><td>100000</td><td>100</td></tr>
<tr><td>100001</td><td>500000</td><td>200</td></tr>
<tr><td>500001</td><td>1000000</td><td>225</td></tr>
<tr><td colspan="2">Above 1000000</td><td>250</td></tr>
</table></td></tr>
<tr><td>27</td><td><b>Payment Return Charges</b></td><td>Rs. 100/ - per instrument</td></tr>
<tr><td>28</td><td><b>PIN replacement Charges</b></td><td>Rs. 50/- (per occasion)</td></tr>
<tr><td>29</td><td><b>Duplicate Bill Charges</b></td><td>Rs. 50/- per quarter (after 12 months)</td></tr>
<tr><td>30</td><td><b>Retrieval of Charge Slip</b></td><td>Actual or Rs. 100/- whichever is higher</td></tr>
<tr><td>31</td><td><b>Balance Transfer Processing Charges</b></td><td><b>Nil</b></td></tr>
<tr><td>32</td><td><b>Fuel Transaction Surcharge</b></td><td>1.00 % of transaction amount or Actual charges claimed by the acquirer bank, whichever is higher</td></tr>
<tr><td>33</td><td><b>Railway Ticket Purchase or Cancellation Fee</b></td><td>1.00 % of transaction amount or Actual charges claimed by the acquirer bank, whichever is higher</td></tr>
<tr><td>34</td><td><b>Lounge Access</b></td><td>As charged by Card Operators.
If card is used abroad, Currency Conversion charges shall also apply</td></tr>
<tr><td>35</td><td><b>Foreign Currency Transactions</b></td><td>2% Currency Conversion Charges for all currencies, (excluding INR, being home currency).
For all types of transaction, including cash withdrawal and transactions through POS/e-commerce/online.</td></tr>
<tr><td>36</td><td><b>Goods and Services Tax (GST)</b></td><td>• Applicable on all Fees and other Charges.
• The applicable GST would be dependent on place of provision and place of supply.
• If POP and POS is in the same state then applicable GST would be CGST and SGST/UTGST else, IGST.
• GST for fee & Charges / Interest transactions Billed on statement date will reflect in next month statement.
• GST levied will not be reversed on any dispute on Fee & Charges / interest.</td></tr>
</table>

<table>
<tr><th>S.N.</th><th>CARD/Charges</th><th>Revised Charges w.e.f. 01.01.2021</th></tr>
<tr><td colspan="3">Note: Issuance & Annual Charges in respect of all Cards (Debit & Credit) are exempt for the following categories for the reasons stated their against:-

<b>Staff/Ex-Staff A/c</b> : Incentive for increased use by the Staff/Ex-staff.
<b>Senior Citizen A/c</b> : Incentive for higher no. of issuance of cards <b>and increased use by Sr. Citizen.</b></td></tr>
<tr><td>37</td><td><b>SMS Alerts</b></td><td>SMS Alerts charges are on actual usage basis from the customers registered for SMS Alerts as under:-
<b>Charges are Quarterly</b>
<table>
<tr><td><b>Upto 5 SMS Alerts</b></td><td><b>Free</b></td></tr>
<tr><td><b>From 6 to 20 SMS Alerts</b></td><td>Rs.10/- per quarter</td></tr>
<tr><td><b>Above 20 SMS Alerts</b></td><td>Rs.15/- per quarter</td></tr>
</table>
SMS Charges not applicable to A/cs of staff & Ex-Staff, A/cs opened under Prime Minister Jan Dhan Yojana (PMJDY) & BSBD Schemes, Pensioners, Senior Citizens, Salary A/cs (SB-161-165) and SB-101 with Special Charge Code “NOMIN”.</td></tr>
<tr><td>38</td><td><b>SMS International Customers</b></td><td>Actual cost of International SMS to be recovered.</td></tr>
<tr><td>39</td><td><b>IMPS Charges</b></td><td><b>Outward: (Through Branch)</b>
<table>
<tr><td><b>Upto Rs. 1000/-</b></td><td><b>Nil</b></td></tr>
<tr><td><b>Over 1000/- upto Rs. 10,000/-</b></td><td>Rs.1/- per Txn.</td></tr>
<tr><td><b>Over 10,000/-upto Rs. 1,00,000/-</b></td><td>Rs.2/- per txn.</td></tr>
<tr><td><b>Over 1,00,000/- upto Rs. 2,00,000/-</b></td><td>Rs. 3/- per txn.</td></tr>
</table>
<b>IMPS Fund Transfer charges through Internet Banking/ Mobile Banking : NIL</b></td></tr>
<tr><td>40</td><td><b>Decline of transaction on ATM or POS due to insufficient fund.</b></td><td>Rs.20/- per failed transaction due to insufficient fund (<b>when used in other banks ATM</b>)</td></tr>
<tr><td>41</td><td><b>Registration charges for mandate on NACH platform</b></td><td>
<table>
<tr><td>Mandate Registration Charges.</td><td>Rs.200.00</td></tr>
<tr><td>Total</td><td>Rs.200.00</td></tr>
</table>
<b>Note:-</b>
Registration charges & signature verification charges for mandate on NACH platform for contribution towards following schemes:-
<b>I.</b> Pradhan Mantri Kisan Maan-dhan Yojana (PM-KMY) : <b>NIL</b>
<b>II.</b> Pradhan Mantri Shram Yogi Maan-dhan (PM-SYM): <b>NIL</b>
<b>III.</b> Pradhan Mantri Laghu Vyapari Maan-dhan Yojana(PM-LVMY) : <b>NIL</b></td></tr>
</table>

S.N.	CARD/Charges	Revised Charges w.e.f. 01.01.2021
42	**Registration Charges for Direct Debit mandate**	Mandate Registration Charges | Rs.200.00 Total | Rs.200.00 **Note:-** Signature verification & Registration charges for Direct Debit mandate for contribution towards following schemes:- I. Pradhan Mantri Kisan Maan-dhan Yojana (PM-KMY) : **NIL** II. Pradhan Mantri Shram Yogi Maan-dhan (PM-SYM): **NIL** III. Pradhan Mantri Laghu Vyapari Maan-dhan Yojana(PM-LVMY): **NIL**
43	**ECS/NACH return Charges**	ECS/NACH Transaction return charges: Rs.250.00 **Note:-** ECS return charges in account of contribution towards following schemes:- I. Pradhan Mantri Kisan Maan-dhan Yojana (PM-KMY): **NIL** II. Pradhan Mantri Shram Yogi Maan-dhan (PM-SYM): **NIL** III. Pradhan Mantri Laghu Vyapari Maan-dhan Yojana (PM-LVMY): **NIL**
44	**INWARD ECS**	**NIL**
	Non-individual: Credit Clearing (Per entry/item)	No Charge
	NCC Clearing House Destination Bank	No Charge
	Sponsor Bank	Rs.5.50 Minimum Rs. 3000/-
	Debit Clearing (Per entry/item)	No Charge
	NCC Clearing House Destination Bank	No Charge
	Sponsor Bank	Rs. 4.00 Minimum Rs. 2670/-

Positive Pay System

*(Pl. refer Circular Letter 2020-21 / 71
Ref. HO/GOD/SRM/2020-21/26 Dt. 29.12.2021)*

Under the positive pay system, the issuer of the cheque will be required to submit electronically, through SMS, mobile app, internet banking or ATM certain minimum details of that cheque like date, name of the beneficiary, payee, amount to the drawee bank.

In order to check banking fraud, the Reserve Bank of India has decided to introduce from January 1, 2021, the 'positive pay system' for cheque, under which re-confirmation of key details may be needed for payments beyond Rs 50,000.

Availing of this facility would be at the discretion of the account holder. However, banks may consider making it mandatory in case of cheques for amounts of Rs 5 lakh and above.

Standard Operating Procedure (SOP) for Implementation of PPS
As per Reserve bank of India vide their Notification No. DPSS.CO.RPPD.No.309/ 04.07.005/2020-21 dated September 25, 2020.Positive Pay System for CTS clearing has been implemented in our Bank w.e.f 01st January, 2020 in order to prevent cheque related frauds by reconfirming key details of cheques.

Details Process Flow of Positive Payment System (PPS)
1. Under Positive Pay System (PPS), Customers has to provide the detail of the cheque/instruments to the bank immediately after issuance of cheques of Rs.5 Lakh and above through any of the below mentioned channel.

- Internet Banking
- Mobile App
- Home Branch

Channel available for Retail Customers: Internet Banking, Mobile App, Home Branch
Channel available for Corporate Customers: Internet Banking & Home Branch

2. Details of Cheques/instrument to be provided by customer:

- Drawers Account Number
- Cheque Number
- Cheque Date
- Amount
- Payee's Name

Note:

1. The cheques which are already paid or made stop payment shall not be available for selection.
2. Customer has to resubmit correct cheque details in case of error status received from NPCI.

3. In case of Corporate Internet Banking, the maker & checker concept and level of transaction password setup/used by corporate customers for RTGS/NEFT transactions shall be enforced for PPS data capture also.

Through Home branch (Both for Corporate & Retail Customer):

- Branch to enter the details of cheque through **Finacle menu "PPS"**.

Revision of Transactional Based Charges on ATM Transactions

RBI vide letter Ref. No. RBI/2019-20/41 dated 14.08.2019 have issued a directive regarding charges based on ATM transaction. On the basis of the same we have revised Transaction Based Charges on ATM transactions as under: -

(BC: 113/114 Dated: 12.09.2019)

<table>
<tr><th>Type of charge</th><th colspan="4">Revised Charges (Excluding GST) w.e.f 01.10.2019</th></tr>
<tr><td rowspan="6"><b>a) Transactions based charges on ATM transactions in SB a/cs.</b></td><td colspan="4"><b>a) Monthly Limit SB A/cs.: Number of Free ATM Transactions (Both financial & Non – Financial Transactions) Other</b></td></tr>
<tr><td><b>Monthly avg. Balance</b></td><td><b>Other ATM 6 Metro Centers</b></td><td><b>Other ATM Other Centers</b></td><td><b>Out ATM 6 Metro & Other Centers</b></td></tr>
<tr><td><b>Upto Rs. 1.00 Lakh</b></td><td>3</td><td>5</td><td>10</td></tr>
<tr><td><b>Charges for Financial trxns Beyond the set limit</b></td><td>Rs.20/-</td><td>Rs.20/-</td><td>Rs.10/-</td></tr>
<tr><td><b>Charges for Nonfinancial trxns beyond the set limit</b></td><td>Rs.8/-</td><td>Rs.8/-</td><td>NIL</td></tr>
<tr><td colspan="4">2. SB accounts with MAB of Rs.1.00 lac & above — No charge to be levied.
3. These charges will not be applicable to Small/No Frill Deposit Account holders. These customers will continue to get 5 free transactions, irrespective of the centre, as hitherto. <b>As also charges on nonfinancial transactions will now be free on our own ATM irrespective of number of transactions.</b></td></tr>
<tr><td rowspan="5"><b>b) Transactions ns based charges on ATM transactions in CC/OD/CD a/cs..</b></td><td colspan="4">b) For Current/Overdraft account holders following charges are applicable: -</td></tr>
<tr><td><b>Charges for</b></td><td><b>Other Bank ATM on all centres</b></td><td colspan="2"><b>Our ATM on all centres</b></td></tr>
<tr><td><b>Financial transaction</b></td><td>Rs.20/-</td><td colspan="2">Rs.20/-</td></tr>
<tr><td><b>Non-Financial transaction</b></td><td>Rs.8/-</td><td colspan="2">NIL</td></tr>
<tr><td colspan="4">The number of transaction should not be counted as valid ATM transactions on account of failed transaction due to technical reason like hardware, software, communication issues; non-availability of currency notes in the ATM; and other declines ascribable directly/wholly to the bank/service provider; invalid PIN/ validations; etc.</td></tr>
</table>

REPORT FOR DEBIT CARDS RETURNED TO BRANCHES

(BC: 113/76 Dated: 09.07.2019)

Please refer to HO BC 110/225 dated 14.01.2017 wherein we have advised introduction of CARDTRAK menu to know the status of Debit card dispatch to branches.

Subsequently, we have started sending the debit cards to the customers directly. Cards which are not delivered are re-dispatched to branches. We are sending SMS containing AWB details to customer when the card is dispatched to them /re-dispatched to branches.

When the debit cards are returned it is necessary to ascertain the reason and where the communication address has changed, re-KYC may have to be done.

We have introduced a new report in Finacle DR so that the detailed report can be generated and necessary action, including change in address, mobile number, and email-id can be done.

Procedure to generate the report is as under:
i. Go to Menu "MISRPT" in Finacle DR.
ii. Select Module name "OTHERS", Report Number "RTO" and press F4.
iii. Enter the branch code and date range for which report is to be generated, proceed to generate report.

Branches are advised to generate the report weekly/fortnightly depending upon number of cards returned and complete re-KYC wherever required.

Introduction of RuPay Credit Cards

(BC: 113/23 Dated: 30.04.2019)

RuPay Credit Cards offers various benefits to card holders with superior customer service and higher levels of acceptance. NPCI offers RuPay cards at low processing fees. RuPay Credit Card is designed for Mass-Affluent segment with host of power packed benefits /offers.

Two variants of RuPay Credit Cards:

- RuPay Platinum Credit Card
- Swadhan Platinum Credit Card(Credit Card Against TDR)

"RuPay Platinum" & "Swadhan Platinum Credit Cards" are International Credit Cards and can be used in any Merchant Establishment (POS terminals) ,on ATMs and for ecommerce transactions where RuPay Cards are accepted worldwide.

"RuPay Platinum" Credit Cards & "Swadhan Platinum" Credit Cards have the following added advantages:

- **Welcome Benefits:** Exclusive Gift Vouchers from leading merchants

- **Accidental Insurance Cover:** Insurance Cover of up to Rs. 2.00 lacs on RuPay Platinum & Swadhan Platinum Credit Card in case of loss of life or permanent disability due to accident from NPCI.

- **Concierge Services:** Avail 24X7 host of referral services from Travel assistance to Hotel reservations and Consultancy services.
- **Cash Back and Merchant Offers:** Cash back offers on Utility bill payments, at Restaurants and at Eateries and also exclusive Merchant Offers on (POS and Ecom) are being provided by NPCI from time to time. The cardholders can avail latest offers available on RuPay Credit Card by visiting the following URL. https://www.rupay.co.in/rupay-offers. Terms and Conditions as per service provider applies.

RuPay Platinum Credit Card:

Valid for usage: In India and Abroad.

Eligibility: As per credit card management policy issued by Card Products Department. Please refer Branch Circular No.113/04 dated01.04.2019.

SwaDhan RuPay Platinum: SwaDhan RuPay Platinum Credit card to be issued to against TDR.

Eligibility: As per credit card management policy issued by Card Products Department. Please refer Branch Circular No.113/04 dated01.04.2019.

Valid for usage: In India and Abroad.

Entrance Fee, Annual Membership Fees and Replacement Card Charges without GST

Card	**Type**	**Entrance Fee**	**Annual Membership Fee**		**Replacement Charges Principal/Add-on**
			Principal	**Add-on**	
RuPay Platinum	Credit	1500	1500	800	500
SwaDhan RuPay Platinum	Credit	0	0	0	0

Nil Charges for Staff / Ex-Staff / Senior Citizens

Marking of lien in Finacle: The branches while issuing credit card against TDR need to ensure that the lien is marked in ALM menu in CBS with reason code Credit Card against TDR. In case of enhancement of limit of the credit card the lien amount has to be modified accordingly.

It is the duty of the branch staff to ensure that the lien is marked. In case the customer wants to surrender the card, the branch needs to ensure that the necessary dues are recovered.

Periodicity of Billing- Billing is done on the 15th of every month. Branch billing customer's account will be debited on 5th of next month.

Issuing of Insta Pin: Insta pin to RuPay Credit Cards to be issued as per Branch Circular No 110-237 dated 23.03.17. **The pin serial number for RuPay Credit Cards will begin with "6"**

All other operational guidelines and Process flow to continue as mentioned in Master Circular on Credit Cards 111/44 dated 19.06.2017 and Branch Circular 111/114 dated 11.10.2017 and the Branch Circular Reference No.113/04 dated 01.04.2019 on the Credit Card Management Policy issued by Card Products Department.

Delegation for Sanction of Retail Credit Card shall be as under:
Delegation for Sanction shall be exercised by Branch Head as per limits applicable to respective Scale of the Chief Incumbent of the Branch.

In proposing the limits, all sanctions at Head Office shall be routed through respective Credit Committees.

ZLCC Shall be the Authority to approve Complimentary Card to be issued to Customers of the Zone.

Delegation for Sanction of Retail Credit Card shall be as under:

Delegation for Sanction of Credit Card	**(Rs. Lakhs)**
	Proposed Limit
JMG Scale-I @	0.50
JMG Scale-II @	1.00
JMG Scale-III @	4.00
SMG Scale-IV @	6.00
AMOLCC	6.00
SMG Scale-V @	10.00
SZLCC	10.00
TEG Scale-VI @	25.00
ZLCC	25.00
TEG Scale-VII @	-
NBGLCC / GMLCC	100.00
ED	-
EDLCC	150.00
MD & CEO	-
CAC	250.00
M.Corn	Full Power

@-Branch Head

General Manager, Card Products Department, shall be the Authority to approve Complimentary Credit Card to Whole Time Directors, Chief Vigilance Officer and Top Executives.

Delegation for Sanction of Credit card against Term Deposit (SwaDhan Card)

Delegation for Sanction of Credit Card	(Rs. Lakhs)
	Proposed Limit
JMG Scale-I @	2.00
JMG Scale-II @	5.00
JMG Scale-III @	7.50
SMG Scale-IV @	10.00
AMOLCC	15.00
SMG Scale-V @	30.00
SZLCC	40.00
TEG Scale-VI @	50.00
ZLCC	75.00
TEG Scale-VII @	100.00
NBGLCC / GMLCC	125.00
ED	-
EDLCC	200.00
MD & CEO	-
CAC	500.00
M.Corn	Full Power

@-Branch Head

Sanction of corporate credit card excluding SwaDhan as per the extent delegation of Power.

Other Charges for Credit Cards

Description of charges	Charges
Interest free period	**For Cash Advance:** Nil **For Other Transactions:** 21-51 days (applicable only on retail purchases and if previous month's outstanding balance is paid in full)
Charges on Revolving Credit	**Secured Credit (SwaDhan)** 1.20% p.m. (15.40% p.a.) on daily balances In case of default service charges is 1.70% p.m. (22.45 % p.a) **Unsecured Credit (Other than SwaDhan)** 1.70% p.m. (22.45% p.a.) on daily balances In case of default service charges is 2.50% p.m. (34.50 % p.a)
Minimum Repayment Amount	10% of Total Outstanding, if revolving credit is opted + EMI (all EMI due) + other amount due.
Cash Advance Limit	**For both Principal and Add-on card:** 50% of Spending Limit or available limit, whichever is lower. Cash withdrawal upto 40% of spending limit of Primary card and upto 20% on Add-on Card. Cash withdrawal per day Rs.50,000 for Platinum and Rs.15,000 for rest variant

<table>
<tr><td>Cash Advance Charges</td><td><b>BOI ATM:</b> 2% (minimum Rs. 50) for each transaction.
<b>Other ATM:</b> 2.5% (minimum Rs. 75) for each transaction.
<b>Overseas ATM:</b> 2.5% (minimum Rs. 125) for each transaction and Currency Conversion Charges, presently 2%.

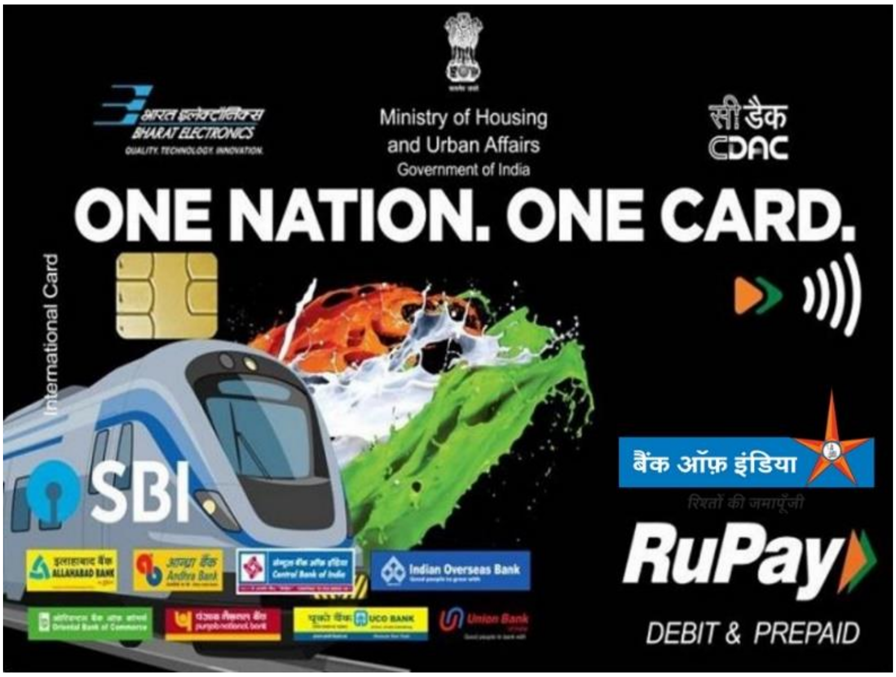
Interest on dues/overdue applicable</td></tr>
<tr><td>Star Easy Pay (EMI)</td><td><b>Processing Charges — One-Time</b>
1.00 % of the Purchase (Existing 2.20 %)
<b>Finance Charge</b>
1.25 % of the Purchase
(existing 1.50% p.m. on original amount)
In case of default service charges is 2.50% p.m. (34.50 % p.a)
Prepayment Charges - Nil</td></tr>
<tr><td>Balance Enquiry Charges at ATM</td><td>BOI ATM: Nil
Other Bank ATM in India: Rs. 20/-
Other Bank ATM Abroad: Rs. 25/-</td></tr>
<tr><td>Payment of charges (Cash/Cheque/Online/NEFT /RTGS)</td><td>Nil</td></tr>
<tr><td><b>Description of charges</b></td><td><b>Charges</b></td></tr>
<tr><td>Charges on over limit account
(Purchase / Cash)</td><td><u>Secured Credit (SwaDhan)</u>
1.70% p.m. (22.45 % p.a) on daily balances
<u>Unsecured Credit (Other than SwaDhan)</u>
2.50% p.m. (34.50 % p.a) on daily balances</td></tr>
<tr><td>Usage Over Spending Limit</td><td><u>Rs. 100/- per occasion</u></td></tr>
<tr><td>Outstation Cheque Processing charge</td><td>For prevailing rates please refer to our website. Charges wef 15.12.2016 are as under:
<table>
<tr><td>Cheque Rs.</td><td>Comm Rs.</td></tr>
<tr><td>Upto 5000</td><td>25</td></tr>
<tr><td>5001 - 10000</td><td>50</td></tr>
<tr><td>10001 — 100000</td><td>100</td></tr>
<tr><td>100001 — 500000</td><td>200</td></tr>
<tr><td>500001 — 1000000</td><td>225</td></tr>
<tr><td>Above 10,00,000</td><td>250</td></tr>
</table></td></tr>
<tr><td>Payment Return Charges</td><td>Rs. 100/ - per instrument.</td></tr>
<tr><td>PIN replacement Charges</td><td>Rs. 50/- (per occasion)</td></tr>
<tr><td>Duplicate Bill Charges</td><td>Rs. 50/- per quarter (after 12 months)</td></tr>
<tr><td>Retrieval of Charge Slip</td><td>Actual or Rs. 100/- whichever is higher</td></tr>
<tr><td>Balance Transfer Processing Charges</td><td>NIL</td></tr>
<tr><td>Fuel Transaction Surcharge</td><td>2.5% of transaction amount (minimum Rs. 10) or Actual charges claimed by the Acquirer bank, whichever is higher.</td></tr>
<tr><td>Railway Ticket Purchase or Cancellation Fee</td><td>Rs. 30/- charged by Railways + 2.5% (Min. Rs. 25/-) or Actual charges claimed by Railways / acquirer bank</td></tr>
</table>

Foreign Currency Transactions	2% Currency Conversion Charges for all currencies, (excluding INR, being home currency). For all types of transaction, including cash withdrawal and transactions through POS/ecommerce/ online.
Goods and Services Tax (GST)	• Applicable on all Fees, Interest and other Charges. • The applicable GST would be dependent on place of provision and place of supply. • If POP and POS are in the same state then applicable GST would be CGST and SGST/UTGST else, IGST. • GST for fee & Charges / Interest transactions Billed on statement date will reflect in next month statement. • GST levied will not be reversed on any dispute on Fee & Charges / interest.

Credit card against Term Deposit (SwaDhan Card)

- SwaDhan RuPay Platinum Credit card to be issued to against TDR.
- It is Chip card without Photo.
- Card valid in India, Nepal and at all foreign centres across the GLOBE, wherever RuPay logo is displayed.
- Since it is a chip card it is safer for POS transactions; it would require PIN for POS transaction
- Billing is done on the 15th of every month. Branch billing customer's account will be debited on 5th of next month.
- Welcome Benefits: Exclusive Gift Vouchers from leading merchants

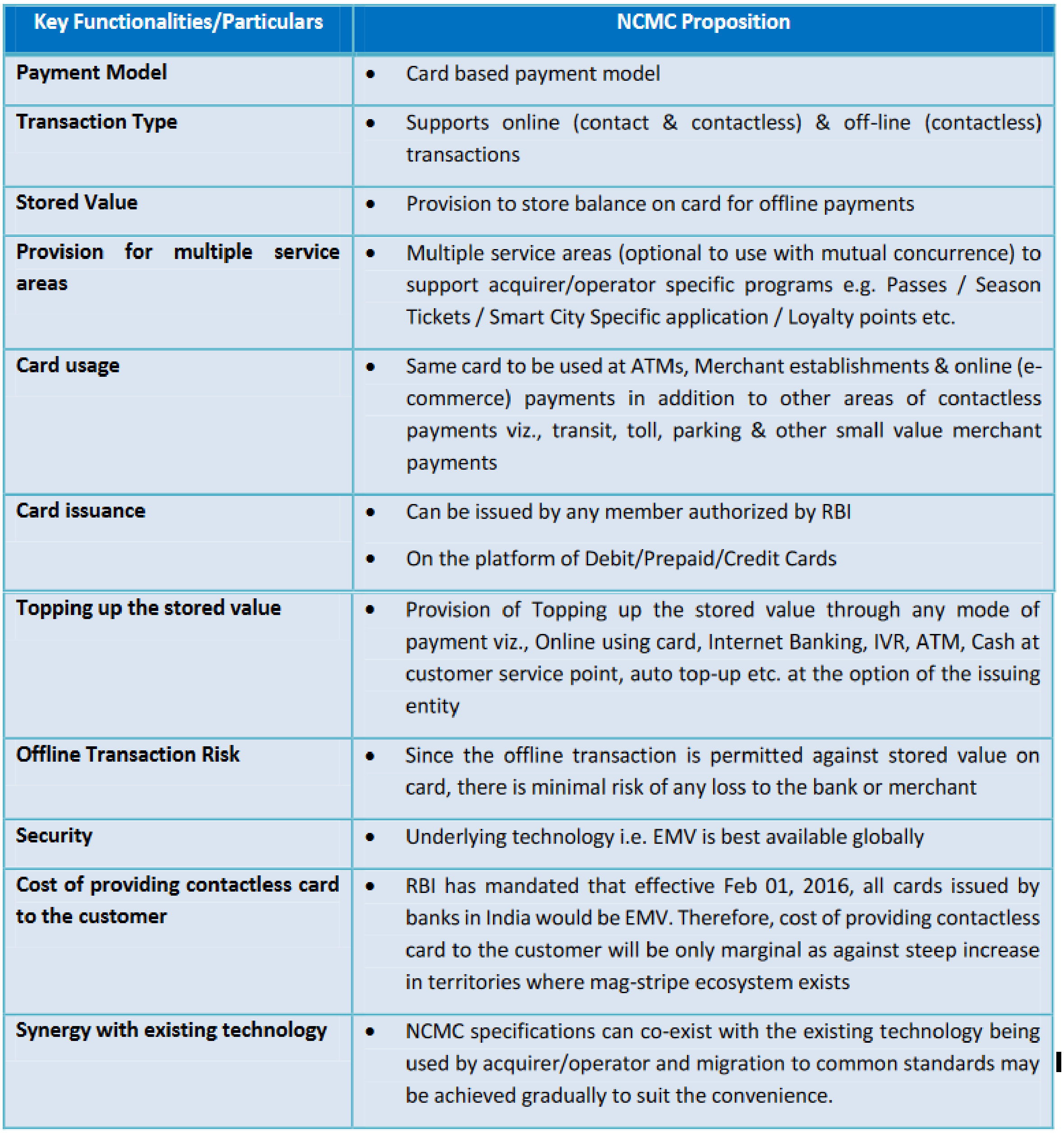
National Common Mobility Card (NCMC)



Introduction to National Common Mobility Card (NCMC)

Ministry of Urban Development (MoUD) has come out with a National Common Mobility Card (NCMC) model to enable seamless travel by different metros and other transport systems across the country besides retail shopping and purchases. A committee was formed with representatives of National Informatics Centre (NIC), Centre for Development of Advance Computing (C-DAC), Bureau of Indian Standards (BIS), National Payment Corporation of India (NPCI)and the Ministry of Finance. After extensive study of various models being followed across the world, the Committee recommended the EMV Open Loop Card with stored value-based model and the same was approved. This card meets travel needs based on stored value of money and can be used for travelling by any means of transport and also enables account-based retail applications. Accordingly, this card does away with the need of carrying separate cards for banking and transit requirements. With a vision to create One Card for all Payments system, NPCI is working with Ministry of Urban Development (MoUD), Government of India for implementation of National Common Mobility Card Program (NCMC). This specification is dual interface (contact & contactless) EMV card-based specification and is interoperable based on open standards. This is aimed at low value payments for various segments e.g. Transit, Smart cities, Toll, Parking and other low value merchant payments in addition to the normal day to day retail payments. These specifications would be capable of supporting not only payment products but also transit applications like passes& government applications such as social security, driving license, Id/access card etc. This will have increased customers convenience as it would allow customers to use the same card for variety of needs.

Key Features of NCMC:



Key Functionalities/Particulars	NCMC Proposition
Payment Model	- Card based payment model
Transaction Type	- Supports online (contact & contactless) & off-line (contactless) transactions
Stored Value	- Provision to store balance on card for offline payments
Provision for multiple service areas	- Multiple service areas (optional to use with mutual concurrence) to support acquirer/operator specific programs e.g. Passes / Season Tickets / Smart City Specific application / Loyalty points etc.
Card usage	- Same card to be used at ATMs, Merchant establishments & online (e-commerce) payments in addition to other areas of contactless payments viz., transit, toll, parking & other small value merchant payments
Card issuance	- Can be issued by any member authorized by RBI - On the platform of Debit/Prepaid/Credit Cards
Topping up the stored value	- Provision of Topping up the stored value through any mode of payment viz., Online using card, Internet Banking, IVR, ATM, Cash at customer service point, auto top-up etc. at the option of the issuing entity
Offline Transaction Risk	- Since the offline transaction is permitted against stored value on card, there is minimal risk of any loss to the bank or merchant
Security	- Underlying technology i.e. EMV is best available globally
Cost of providing contactless card to the customer	- RBI has mandated that effective Feb 01, 2016, all cards issued by banks in India would be EMV. Therefore, cost of providing contactless card to the customer will be only marginal as against steep increase in territories where mag-stripe ecosystem exists
Synergy with existing technology	- NCMC specifications can co-exist with the existing technology being used by acquirer/operator and migration to common standards may be achieved gradually to suit the convenience.

With a vision to create One Card for all Payments system, Ministry of Urban Development along with National Payments Corporation of India (NPCI) has come out with a National Common Mobility Card (NCMC).

National Common Mobility Card (NCMC) is a dual interface (contact & contactless) classic domestic EMV card which is interoperable and has an offline wallet as a default option.

The amount in the offline wallet can be utilized for making low value payments for various segments e.g. Transit, Smart cities, Toll. This will add to customer's convenience as it would allow customers to use the same card for variety of needs.

As per RBI norms, transactions upto Rs.2,000/- can be processed without a PIN. (RBI/2014-15/601-DPSS. CO. PD. No.2163/02.14.003/2014- 2015 Dtd 14th May 2015). The card will enable the customers to make electronic payments by just waving the cards near the merchant terminal in lieu of dipping or swiping them. These cards are based on the "Near Field Communication (NFC) technology", which provides customers the improved convenience of speed as these cards require significantly less time than traditional cards to complete a transaction along with enhanced security as they remain in control of the customer.

<u>Salient Features</u>

- The NCMC cards will be available in two variants Classic & Platinum. As of now Bank is launching the Classic variant of NCMC debit card.

- The contactless debit card can be used for other purposes like any other Debit Card for ATM cash withdrawal, shopping at merchant outlets (at pos), safe and secure for online shopping (Ecom) and has an offline wallet which can be used at transit, smart cities, toll.

- It is an advanced chip card with additional element (antenna) which will work as sensor, due to which card will be required only to be tapped / waved near the EDC /POS machine instead of swiping or inserting. Please note that Contactless Payment may be made on the POS machines which are enabled for RuPay Cards.

- While using this card the cardholder need not hand over the card to the merchant. He has to simply go near the NFC terminal (EDC machine) and tap / wave his card. Then the machine will capture the details of his card and process the transaction and his account will be debited immediately with the amount he has to pay and charge slip will be generated.

- As per R.B.I guidelines, **PIN** is waived for transactions upto Rupees 5000 for contactless card transactions to enable the convenience and quick transaction experience.

- At ATMs / non-NFC terminals and for transactions beyond Rs.5000/-, the contactless card will continue to function like a normal credit / debit cards requiring dip / swipe with PIN entry.

- The NFC terminals whether enabled for RuPay Cards or not will have the dip & swipe facility for the all types of cards to be accepted.

- Maximum 3 NFC transactions are allowed per day
- In this type of card, two types of balance will be available as under:
  i) Account Balance
  ii) Card Balance (Stored Value)/Offline Wallet

There is no restriction upon the number of times in a day for the wallet transactions.

i. **Account balance:** To be used for all online transactions across retail, E-commerce, ATM.
ii. **Card Balance (Stored Value)/Offline Wallet** - to be used for all offline transactions across transit, toll, parking, retail and smart cities. This value will be reckoned as the card Wallet.

The Offline wallet balance limit for the NCMC cards will be as below

1. Classic Card -	Rs.1,000=00
2. Platinum Card -	Rs.2,000=00

As of now Bank is launching the classic variant of NCMC debit card which is for domestic use only.

Balance in the offline wallet can be added/topped up in two ways

1. Through Cash
2. Through Debit Card

Through Cash:

i. A customer may approach a merchant authorized to perform top up transaction

ii. The customer will pay the amount to be topped-up in Cash to the merchant and the customer will tap the card on the POS and perform a money add/reload transaction

iii. This money add transaction shall be authorized by the issuer host and topped-up amount will be added at the host side in the wallet account

iv. This amount will be added into 'Card Balance' of RuPay contactless Card post successful issuer authorization

Through Debit Card:

i. A customer may approach the merchant to perform top up of the card using account.

ii. All such money add transactions shall be authorized by the issuer host.

iii. Dedicated RuPay contactless terminal will perform these transactions.

iv. Topped up balance will be added to the RuPay contactless card in 'Card Balance' after successful approval from Issuer

Security

- The Contactless cards are just as secure as any other chip card and carry the same multiple layers of security protection.
- Featuring a distinctive contactless mark, the cards have a tiny antenna embedded into the card, which securely transmits payment information to and from the contactless reader.

- During a contactless transaction the card never leaves customer's hand; customer retains control of his card during the transaction, which significantly reduces the risk of card loss and fraud due to counterfeit (skimming).

Usage Process

1. Customer has to look at the contactless symbol/logo the point of sale.

2. The cashier enters the purchase amount into the NFC terminal. This amount is displayed on the NFC terminal reader

3. PIN authentication will be by-passed for low value transactions up to Rs. 5000/-

4. Beyond this transaction limit, the card will be processed as a contact payment and authentication with PIN will be mandatory

5. Transactions are permitted on non- NFC terminals with PIN authentication.

6. On Non-NFC terminals, below Rupees 5000 even the PIN authentication is mandatory as NFC feature will not work on such terminals.

Issuance and Annual Mainteance Charges

Particulars	**Charges**
Issuance Charges	Rs. 150/-
Annual Maintenance Charges	Rs. 150/-
Card Replacement Charges	Rs. 150/-
Repin Charges	Rs. 60/-
Green Pin	Free

Finacle Menu:

Branches can raise the request through menu "ADCREQ" as below:

Card	Card Type In ADCREQ	Instapin series for menu	Cash Withdrawal limit per day	Purchase+ E.Comm. limit per day
RuPay	**"1"**	**7-series**	**Rs. 15,000**	**Rs. 25,000**

Procedure for issuance of RuPay Contactless NCMC Debit card

- Branch to invoke menu ADCREQ
- Select Option "A" and enter the account number Select the card type "1"
- The record will be added successfully.
- After the record is successfully verified a virtual account will be opened by the system which is referred to the wallet account.
  Note: The offline wallet payment feature may be available in select cities and at select merchant.
- For Contactless RuPay Classic Nation Common Mobility Card (NCMC) the virtual account will be 16-digit number ending with "1 ".

  For example, request for the card is entered in the account number 010110110000023 the wallet account will be 0101101100000231 wherein 1 being the identifier of the RuPay virtual account.

Please note that offline wallet payment feature may be available in select cities and at select merchants in due course.

What is Bank of India's Contactless RuPay Classic Debit Card (NCMC)?

- The RuPay National Common Mobility Card is a Contactless Card. It also has the feature of offline wallet. Therefore, it is called as Debit and Prepaid Card. A single card that can be used for making all kinds of payments at transport, parking grocery, toll and transit.
- Can be used as in Domestic ATMs/POS/E.com.
- Supports offline transaction multi utility card of its kind.

What are the key features of RuPay Contactless?

- Service Compartments: It comes with a unique feature that enables acquirer to create and use their own space on the card, referred to as 'Service Compartment'. There may be multiple independent service compartments on the same card catering to different business implementations. Acquirers/merchants may build their own specific programs such as transit, loyalty, etc. on these areas as per their business agreements with the card Issuer.
- Multi-level Wallets: qSPARC specification supports creation of wallets in the card at two different levels - Global i.e. at card level and Local i.e. at service level. Global balance is maintained by issuers and local balance is maintained by acquirers/operators. While the local balance may be utilized for transactions only at service provider specific outlets, the global balance may be utilized for payments at all outlets where RuPay chip cards are accepted.
- Shorter transaction processing time - Transactions amounting less than Rs.5000 can be approved offline without additional factor authentication.
- Interoperability

What is contact, contactless and dual interface?

- **Contact Interface:** A card based on contact interface can interact with terminal only when the card is in contact (dipped or swiped) with the terminal.
- **Contactless Interface:** A card based on contactless interface can interact with terminal when the card is in the range of the terminal. The card does not need to be in contact with the terminal to initiate a transaction.
- **Dual Interface:** These cards support the properties of both the contact as well as contactless interface. A transaction can be initiated by either interface depending upon the capabilities of terminal.

What is contactless technology?

Contactless cards have an embedded antenna in the plastic so that when they are used at a contactless reader, they securely transmit purchase information to and from the contactless reader.

During a contactless transaction, the card never leaves the hands of the customer. This greatly reduces the risk of card loss and fraud through counterfeit/skimming. The contactless card has its own, unique, built-in, secret key, which is used to generate a unique code for every contactless transaction, thus making it more secure

Is there a limit for a contactless transaction amount?

Payment through the contactless mode is allowed for a limit of maximum Rs.5000/- for a single transaction in India. For any transaction amount more than Rs.5000/- the customer will be asked to provide your Debit Card PIN.

How to identify whether a Contactless payment at a merchant can be made?

If the merchant terminal has a contactless mark •))) then it is NFC enabled. The contactless symbol is a small logo that has four waves or four curved lines, just like a toppled Wi-Fi-symbol.

Can I use my Contactless Card at other merchants who are not enabled for contactless payment acceptance as well?

Yes, for the merchants not enabled for contactless payment acceptance, the customer can use this card as normal dip or swipe transaction.

Could I be debited twice if I have more than one contactless card?
No, as contactless readers will only communicate with one card at a time. If the shop's reader finds more than one contactless card in your wallet or purse, the customer will be asked to select one card to pay.

Can I unknowingly have made a purchase if I walk past the reader?
No. Your card has to be waved within 4cm of the card reader for than half a second and the retailer must have first entered the amount for the customer to approve. Terminals can only process one payment transaction at a time, therefore reducing transaction errors.

Is there any difference in the process for ATM and Internet transactions for Contactless Card?
There is no difference in transaction process for ATM or any Ecom transactions. For ATM transactions you need to enter the PIN and for Ecom transactions you need to enter your PIN and OTP (One Time Password).

Can I use my contactless debit card if the purchase amount is more than Rs.5000?
Yes, based on the amount of transaction the customer will be asked input the Debit Card PIN. If the transaction amount is greater than 5000 the customer will be required to enter their Debit Card PIN, for transactions less than 5000, the customer will not be required to enter any PIN, provided the terminal supports Contactless Transactions.

Can the cardholder use it for contactless payment if the card is in his wallet or purse?
As long as the card is within a 4 Cm range, and is not being blocked by any metal object which may prohibit the signal, one can use the card even from his/her purse or wallet.

What are the other Uses?
In addition to the offline wallet that can be utilized for making low value payments for various segments like Transit, Smart Cities, Toll, Parking, the card can be used for making contactless payments at NFC enabled terminals which are being progressively deployed by various merchants, these cards would also work as regular debit cards i.e. a customer can withdraw cash from ATM, shopping at merchant outlets, online/ecommerce transactions etc.

How will the cardholder come to know if the transaction is successful?
Cardholder will receive a charge slip from the merchant, and also receive an SMS/Emailer on your registered contact details.

What is the validity of this card?
The validity of this card is 6 years from the date of issuance

What if the antenna embedded in the card gets damaged before the expiry of the card?
Bank uses certified and established processes for manufacturing the card through the vendors ensuring a long life for the card. However, given the instance that the any of the elements of the card gets damaged, card holder may contact the branch, and he /she will get replacement of his/her card.

How to identify whether a Contactless payment at a merchant can be made?

If the merchant terminal has a contactless mark then it is NFC enabled. The contactless symbol is a small logo that has four waves or four curved lines, just like a toppled Wi-Fi symbol.

What happens if the card is lost or stolen? What are the risks associated with the card if the card is stolen or lost?

In case of lost or stolen contactless debit Card

1) A fraudster may use the contactless card for a maximum value up to Rs.5000/¬per transaction at a merchant location where the contactless payments are accepted, before the loss is reported and the card is blocked.
2) The fraudster may do a maximum of three contactless transactions for a maximum value not exceeding Rs. 6,000/- in a day.
3) The number of fraudulent transactions in a day will be dependent on; how many contactless transactions have already been done on the card before losing the debit Card.
4) The amount available in the offline wallet can be used at where the facility is available.

Is this a "Chip card"?

Yes. This is a form of chip card technology. Like chip cards, it uses an advanced computer chip embedded in the card's plastic to perform secure transactions. Contactless Debit Card is secured with a Contact & Contactless Chip along with Magstripe and NFC antenna. The NFC antenna is used for Contactless transactions. The Chip and the magstripe portion are used for purchases at POS and transactions at A TM and where Contactless payments are not accepted.

What are the liabilities of the customer in case of lost or stolen card?

In case of a lost or stolen contactless debit card, a customer may immediately contact the Bank Customer Care to report the loss of his/her Debit Card. The Bank will not be liable for any financial loss arising out of the unauthorized use of the card until such time the customer hotlists the card. The customer can call on 18004251112, 022- 40429123 for hot listing the debit card.

Prepaid Cards

Product features:
These cards are General Purpose Reloadable (GPR) Pre-Paid Cards and will be valid in India. At present it is affiliated with Visa International. It is a non-personalized PIN enabled cards which can be issued and reloadable in INR. It is accepted at all ATMs, POS and E-com channels in India. Cash withdrawal is permitted for the card within predefined limit.

The maximum limit for the card will be Rs 50,000.00. Cardholder can load his/her card multiple times in a month but within the monthly cap of Rs 50,000.00.

BOI GENERAL PURPOSE RELOADABLE PREPAID CARD

(Enhanced EMV chip based Prepaid Visa/Mastercard Card)

Features	1. Prepaid Cards can be issued in INR for a max of Rs.50,000/- 2. BOI Prepaid Cards are reloadable in nature and maximum value shall not exceed Rs.50,000 at any given point of time. 3. This card would be used on all payment channels, via, Cash Withdrawal, POS and ecommerce transactions. 4. This card will be PIN based. The branch will issue instapin separately when the card is issued. 5. **The card is valid for seven years from the date of issuance.** **6. First transaction not necessary on ATM.**
Note:	Branches are to ensure that Full KYC of the purchaser as well as ultimate user is to be obtained and kept on record. These prepaid payment instruments shall be loaded/reloaded only be debit to the bank account, which are subject to full KYC.
FEE	Issuance Charges – Rs. 50/- + GST per card Reloading charges – Rs. 50/- + GST per card Repin Charges – Rs. 10/- + GST Monthly Limits – Rs. 50,000/- ATM withdrawal fees – Rs.10/- + GST ATM Balance Inquiry charges – Rs.5/- + GST
Transaction Limits	Rs. 15,000/- on ATM per day Rs. 35,000/- on POS and eCom per day
Re-loadable Cards	All Cards issued will be re-loadable. These cards can be loaded/reloaded through Bank Branches. These cards will be loaded/reloaded in INR. Load/Reload transaction will not happen if the card is not activated, hot listed, cancelled or expired.
Related Queries:	1. Inquiries regarding balance available, expiry date etc. can be made at our Service Provider's 24x7 Helpdesk No. 022 40426006. 2. Hot listing of gift card can be done 24x7 on All India Toll-free No. 1800 22 00 88 or 022-40426005 or via email through branch to email id HeadOffice.CPDprepaidcard@bankofindia.co.in 3. In case of any enquiry from branch , email id : HeadOffice.CPDPrepaidcard@bankofindia.co.in

Youfirst Prepaid CARD

Features	1. Youfirst prepaid Cards can be issued in Indian Rupees for a max limit of Rs 50000/-. (Monthly cap of RS.50000/-) 2. Youfirst Prepaid Cards can be issued by any branch 3. Youfirst prepaid card is affiliated with Visa International. It is a non-personalized PIN enabled cards which can be issued and reloadable in INR. 4. It is accepted at all ATMs, POS and E-com channels in India.
FEE	Issuance Charges: Rs 50/- per card Reloading Charges: Rs 50/- per card Re-PIN Charges: Rs 10/-
Cash withdrawal from ATM	Cash withdrawal is permitted for the card within predefined limit
PROCEDURE FOR ISSUING CARD	1. Branch will take KYC documents of the customers/Prepaid card holders. 2. Branches will provide the customers on-boarding and loading/reloading details in prescribed format to boi.cards@youfirst.co.in with a copy to HeadOffice.CPDSettlement@bankofindia.co.in 3. The loading or reloading of card shall be done only on receipt of the customer's details and transfer of amount to the Escrow account. 4. Card activation and loading of amount will be done on T+1 basis after receiving of amount in designated account.
Related Queries:	For any query/inquiry mail to boi.cards@youfirst.co.in Contact Number: 022-49062022; 022-49062024 In case of any enquiry from branch, email id: HeadOffice.CPDSettlement@bankofindia.co.in

BOI INTERNATIONAL TRAVEL CARD

Features:

1. Available in currency: U S Dollars.
2. The card is a VISA Card.
3. Minimum loading of USD 250.00
4. Valid up to the expiry period mentioned on the card.
5. Backed by extensive VISA Network. (It can be used in over one million ATMs and over 14 million Visa Merchant outlets across the world, except India, Nepal and Bhutan.
6. Competitive Exchange rates.
7. Savings on cross currency charges (when used in other than currency denominated countries)
8. Dedicated 27x7 help line.
9. Convenience of reloading the card for repetitive usages during the validity of the card.
10. Fee of Rs.100/- for re-issue of card in lieu of lost card
11. BOI Travel Card can be issued by AD Category branch only

Related Queries:

Customer can call Bank of India 24-hour Customer Care Center for free customer support. From within India, call Toll Free: 1800 22 0088 Mumbai: 022-40426006.

In case of any enquiry from branch, email id:-
HeadOffice.CPDSettlement@bankofindia.co.in

BOI GIFT CARD

HOBC 107/150 of 30.10.2013 & HO BC 109/61 dated 21.6.15
(Magnetic Strip Based Prepaid Visa Card - valid in India, Nepal & Bhutan)

Features	1. Visa Card (Domestic Card) 2. Non reloadable 3. Gift Cards can be issued in Indian Rs for a min of Rs. 500/- thereafter in multiples of Rs.1/- with a maximum amount up to Rs. 10,000/- 4. BOI Gift Cards can be issued by any branch 5. Gift Card is acceptable at all Visa Merchant Establishments in India, Nepal and Bhutan and can be used any number of times up to the amount loaded (Balance available in the Gift Card) 6. **The card is valid for one year from the date of issuance (branch has to ensure that the card which are issued must have at least one-year validity period.)** 7. **E.com transactions not allowed.** 8. Free balance inquiry with transaction receipt indicating the balance online at - http://www.bankofindia.co.in/giftcardform
Note:	The enhanced features (limit & validity) are not applicable to the Gift Cards already issued. Only the Gift Cards issued henceforth would have these enhanced features. However, the stock of Gift Cards available at the Branches be continued to be issued for maximum amount of Rs 10,000/- and with validity period of one year from date of issuance.
FEE	Rs 50/- + GST irrespective of the amount
Cash withdrawal from ATM - NOT PERMITTED	
PROCEDURE FOR ISSUING CARD	1. Obtain application form duly filled in and duly signed by the purchaser of Gift Card (In case the purchase is not our customer then additional documents as listed below) 2. Enter the application particulars online on the basis of maker / checker concept. Each branch would be given two User ids for entering the application data and for verification of the same. 3. "**Giftcard**" Menu in CBS for entering the request. 4. The 12- digit reference no. on the envelope along with the amount is to be entered. At a time, 5 requests can be entered if the reference nos. are in series. 5. The amount in the online Application Form should be the total amount i.e. Amount of Gift Card+ Amt of Fees. 6. After verification of the Online Application form, the gift card will be activated. The beneficiary can use the card from the next day.
Documents required	The branches, whilst issuing Gift Cards, should ensure to collect the following documents from the applicant: 1. Up to Rs. 1000/- any acceptable identity document of the applicant. 2. Up to Rs. 5000/- any "officially valid document' defined under Rule 2(d) of the Prevention of Money Laundering Act as proof of identity. 3. Above Rs. 5000/- and up to Rs. 10,000/-, KYC requirements of RBI, issued from time to time is to be followed and documents obtained accordingly.
Related Queries:	1. For issuance of Gift Card in lieu of Lost Card a charge of Rs. 100/- will be levied. 2. Inquiries regarding balance available, expiry date etc. can be made at our Service Provider's 24x7 Helpdesk No. 022 40426006. 3. Hot listing of gift card can be done 24x7 on All India Toll-free No. 1800 22 00 88 or 022-40426005 or via email through branch to email id HeadOffice.CPDprepaidcard@bankofindia.co.in 4. In case of any enquiry from branch, email id: HeadOffice.CPDPrepaidcard@bankofindia.co.in

Credit Card

Eligibility for Credit Card

Individuals	**Deposit Customers:**	**BOI Staff/ Ex-Staff**	**Corporate Cards:**
Resident/NRI / Person of foreign Origin residing in India on employment and regular source of income	NRI's, students, Senior Citizens, House wives and small businessmen, traders.	No-disciplinary action initiated/pending/contemplated against him/her	Proprietorship/Partnership firm/ Private Limited Company/ Public limited Company/ registered institutions/ Societies Net Worth: Min 1 Crore Profit making any two years out of preceding 3 financial years.
Age-18 Yrs. and above			

Not Eligible of Credit Card: Mobile Number not seeded in account, Minor, Accounts in the name of Government and Quasi-Government, Insolvent persons/entities, Illiterate persons (except special schemes), Accounts operation is frozen by Court / Government Authorities / Bank, Minor.

Document Obtained for Issue Credit Card: Application form along with Photograph, KYC, ITR, Salary Slip (Three Months), Balance Sheet (For Corporate Card only)

Processing for Issue Credit Card: All New/fresh Credit Card Request must be processed through CAPS except Corporate credit card (Corporate Card Sanction in Hardcopy Form).

Document Kept in Branch Record: All document obtained for Processing and CIBIL Report, Sanction Memorandum, Sanction Letter

All New/fresh Credit Card Request must be processed through CAPS except Corporate credit card.

Add on Card

For Corporate Credit Card	**Other than corporate Credit Card**
Add-on card shall be issued to Director/ Proprietor/ Partner /Executives /Employees of Company/Firm	Add-on Cards, maximum up to 5 close relatives, as defined below, subject to minimum age criteria of 18 years: Parents, Spouse, Major Child, Brother, Sister

- ✓ Specimen signature and KYC of all the add-on card holders are obtained and held on record
- ✓ Request for issuance of add-on card shall be made by the Principal Card holder in writing duly signed, with specimen signature on Bank's record.

Credit Card Limit

Retail	Staff / ex-staff	Corporate	Against TDR/Swadhan
20% of Gross annual income and also can be considered up to 40% on merits of the case.	Maximum 20% of Gross Annual Income. Staff on Probation: Officer: Rs.30,000/- Clerk: Rs.20,000/-	Minimum Rs1, 00,000/-. Maximum 2% of Tangible Net Worth of the Corporate as per last audited Balance Sheet	Minimum Rs. 24,000/- Maximum: Rs.250 Crore (80% of TDR amount) **(Minimum Margin 20%)**

For Against TDR/Swadhan: Deposit to be held in the name of the proposed Card holder. Minimum Term Deposit should be for 12 months. Auto-renewal must be available i.e. Auto-renewal flag must be set to "Y".	**Combined limit of Principal Card and all Add-on card shall not exceed the limit of sanctioned for Principal Card**

Cash Withdrawal Limit:

- 15% of the Principal Card Limit subject to minimum Rs. 1,000/- and maximum Rs.15, 000/- per day.
- 15% of the Add-on card Limit subject to minimum Rs. 1,000/- and maximum Rs.15, 000/- per day.
- Maximum Card Limit shall be 50% of the Spending/Credit Limit.
- For Corporate Credit Cards, both Primary and Add on, limit for cash advance shall be Nil.

Revolving Credit

- ✓ Card holder may opt for Revolving Credit, request in writing or through Call Centre / electronic mode.
- ✓ This is available for all card holders, including Staff/Ex-Staff.
- ✓ Minimum 10% shall be payable at the end of each Billing Cycle and the balance allowed to be carried over with applicable charges/Interest.

Easy Pay Scheme (EMI)

Minimum Purchase – Rs.5000/-, Minimum EMI – 3, Maximum EMI - *3=6, 9, 12……. up to 36

Purchase at POS, e-commerce (Cash withdrawal Not Applicable) Total interest payable for the full tenure @ +GST One-time processing fees shall be charged along with first EMI	Request through Call center or email @ Toll Free no: 1800220088 Email - Dinesh.brid@worldline.com

Renewal of Credit Cards

- Credit Card shall be automatically renewed, at least two months prior to expiry date of the card.
- Renewed Card shall be delivered to Card holder's registered address
- Card Not Renewal – Hot listed Card, Dues / EMIs / Revolving Credit amount / applicable charges is not recovered, Customer not initiated transactions validated through Credit Card during the last six months at the time of processing of card renewal

Replacement Card

Branches can issue Duplicate/Replacement Card in lieu of lost/misused card, only after-

I. verification of signature and mandate of the customer and

II. Ensuring hotlisting of the Card.

Replacement card shall be issued by Head Office, Card Products Department to the customer's address or the Branch through approved Courier/Speed Post and inform the customer through SMS

Credit Card Billing Related Information:

- ✓ Billing dates for credit cards is **15th** of every month for all variants cards.
- ✓ Bill period of 16th to 15th. due date will be 5th/ 6th /7th /8th of next month following billing period irrespective of number of days in a month.
- ✓ Any credit amount in card before 03 working days of due date will be adjusted in current billing amount.
- ✓ Excess credit amount in credit card above sanctioned card limit will be refunded to charge account on due date in next billing.
- ✓ Limit of the card will be blocked for Debit balance/over drawn in Charge Account and for NPA / Dormant / Invalid / Freeze Charge Account.
- ✓ If sufficient Balance is not available on due date in the charge account then amount will not be debited and full card limit will be blocked. Advise card holder to maintain sufficient balance in charge account. System will try debit the overdue outstanding amount on daily basis, whenever sufficient balance will be available in charge account. It will get debited and card limit will be restored within 48 hours.
- ✓ If amount credit card dues not recovered on due date then amount will become overdue in credit card. So, penalty and interest will be applicable as per credit card management policy.
- ✓ Hard copy of the Bill, free of cost, shall be sent through ordinary mail to the card holders registered address.
- ✓ E-statement shall be sent to the card holder to the registered mail id in a password protected mode using the data, known to the card holder only

- ➢ **Limit Enhancement request must be sent along with Memorandum Sanctioned by competent Authority (for Staff – SZLCC, Delegation follow Credit Card Management Policy)**
- ➢ **Replacement Card request send through Email after hot listing the same (If lost/damage etc.)**

Charge Account for credit card must be Pension Account for BOI Ex- Staff and Salary Account for present serving Staff.

TYPES OF CREDIT CARDS

MASTER	**VISA**	**RUPAY**
1. India Card **2.** Platinum International	**3.** Visa Gold International **4.** Platinum Privileged Card	5. SwaDhan RuPay Platinum **6.** RuPay Platinum International

Annual Maintenance Charges

Type of card	AMC Primary	AMC Add-on	Replacement	Type	Photo card
India Card	0	0	500	Domestic	Photo &Non-photo
SwaDhan RuPay Platinum	0	0	0	International	Non-photo
RuPay Platinum	1500	800	500	International	Non-photo
Visa Gold Int.	1500	800	500	International	Non-photo
Visa Privilege (Platinum)	1500	800	500	International	Non-photo
Master Platinum Int.	1500	800	500	International	Photo card

❖ **AMC is Nil for Staff/ Ex Staff/ Senior Citizens**

DELEGATION (For Non-Staff) ₹ In Lakhs

Scale	I	II	III	IV	V	VI	VII	CAC	M.Com
Credit card Limit	0.50	1.00	4	6	10	25	100	2500	Full Power
Against TDR	2.00	5.00	7.50	10.00	30.00	50.00	100	2500	Full Power

DELEGATION (Staff/ex-staff): Delegation as per normal loan sanctions practice. However, Ceiling limit for Officers and Clerks under probation or who are yet to be confirmed shall be ₹30,000/- and ₹20,000/- respectively.

Hot listing of Credit Card	Toll Free Number: 1800220088 Land Line Number: 022-40426006/6005 Mail Id: wl-in.boicreditcards@worldline.com
All types of enquiry	Toll Free: -1800 220 088, Land Line: (022) 40426005/40426006
Merchant Enrolment	Land Line: (022)61312937

- ✓ Branch cannot delete Credit Card from Link a/c through CCMNT Menu and Branch cannot close the account.
- ✓ For close the a/c, First Hotlist the credit Card and send email to **HeadOffice.CPDcreditcard@bankofindia.co.in**
- ✓ Hot listing through a/c Number then all card will be hot listed including add on Card
- ✓ Once card is hot listed cannot be Revoke and to replace automatically
- ✓ AMC will be recovering after hotlisting also for this year.

Fail transaction of Credit Card on ATM and POS, it will auto revere within 15 days and adjusted in Bill.
If not Reverse then email to as per card : HeadOffice.Visachargeback@bankofindia.co.in, HeadOffice.Masterchargeback@bankofindia.co.in, HeadOffice.RupayChargeback@bankofindia.co.in

Reversal/Cancellation of transaction like IRCTC, Flip Cart reverse when amount is recived from then if not recived with in TAT then Send email to as per card HeadOffice.Visachargeback@bankofindia.co.in, HeadOffice.Masterchargeback@bankofindia.co.in, HeadOffice.RupayChargeback@bankofindia.co.in

BOI Credit control Apps for Credit Card
It is integrated into BOI Mobile Banking App

For registration:

1. Post installation, click on Registration Tab
2. Enter 16-digit Active Primary Card Number & Expiry in MM/YY
3. Post this customer will receive an OTP on registered Mobile Number
4. Enter OTP on the application and create User ID, Password & 6-digit MPIN
5. Once validated, a notification will be sent on registered mobile number regarding successful registration

Features: -

- ✓ Lock/Unlock card
- ✓ Green Pin
- ✓ Set Card Limits
- ✓ Card Usage
- ✓ Keep Track
- ✓ Notification
- ✓ Account Summary
- ✓ User Profile Management

MPIN - This is a 6-digit number which is used for authorizing the changes done to any of the parameter in the application. This is also used for authorizing a device when existing customer changes the handset and login with existing credentials.
Please contact Helpdesk Support- 022-33865300 Extn:22445/22446/22447/22448

Credit Card Loyalty/Offer **BOI Star Rewards Programme -** For every Rs. 100/- spent through a BOI Debit Cards on ECOM and POS, the customer earns 2 Reward Point. All the Points including Bonus Points will be valued at Rs.0.25.
Circular Reference: (1) Credit Card Management Policy Dated 01-04-2019 w.e.f. 19-03-2019 (2) Master Circular: 111/44 Dated 19.06.2017; Modifications: 111/67 Dated: 29.07.2017 (3) Against TDR: 111/114 Dated 11.10.2017; Operational changes: 107/147 dated 24.10.2013 (4) Service Charges Circular: Dated 12.12.2018 w.e.f.15.01.2019 (5) RuPay Credit Card:113/23 Dated 30.04.2019 (6) EMI Scheme on POS:112/79 Dated08.08.2018

Credit Card Operations:

For Payment of Credit Card Dues through CBS for Branch Billing Customers

(BC: HO:CPD:GS:2020-21:01 Dt:16.04.2020)

As per the credit card master circular vide branch circular no:111/44 dated 19-06-2017, branch has to credit CBS account: 010190200000001 (Credit Card Dues Remitted) of Card Products Department with the card number written in the particular's field or remark's field giving the value date of credit for payment of credit card dues for branch billing customers. In this process the credit card limit is restored after two working days of the dues payment. In case of auto debit on due date Card Product Department was recovering the Credit Card dues from card holder's charge account through file based process.

Both processes were creating a lot of inconvenience to our customers as well as to the branches. To mitigate this, we have revamped the process for payment of credit card dues on real time basis through branch channel. By adopting new process, apart from customer convenience, we shall also comply with PCI/DSS guidelines.

Card Products Department has introduced new process to make Credit Card related dues payment/recovery more efficient.

A) PULL PAYMENT (Payment Process by CPD)

I. Present Auto Debit Process

a. Credit Card Management Systems (CCMS) used to provide the file based transactions to Card Products Department.

b. Card Product department runs these files in finacle and the card holder accounts get debited, if sufficient balance is available in the charge account.

c. Card holder's credit card limit gets released on next working day and credit to credit card also get posted on next day EOD as it is presently a manual reconciliation process.

d. In case of holidays/weekly off, the file is processed on the next working day.

e. Due to manual process and intervening holiday, recovery of card dues is not done on daily basis in respect of cards where sufficient balance is maintained in charge account after due date.

II. New Online Credit Card Dues Auto Recovery Process

a. Customer needs to maintain sufficient balance in charge account.

b. On due date, automatic recovery will be done from customer charge account and limit shall be released on real time and customer will get an SMS with updated credit card limit.

c. If recovery is failed from charge account then authorization of that credit card gets blocked and applicable interest/penalty will be applied. **In such scenario free credit period is not available to the customer and interest is charged from the date of transactions.**

d. The system shall attempt recovery of card dues daily including on holidays.

e. Card limit shall remain blocked under the following situations :

- Sufficient balance is not available in the charge account, to honour total amount due.
- Charge account is dormant/ Closed/ Frozen/ Non-KYC/ NPA.
- The customer is not KYC compliant.
- The account is under FCRA 1976 (Scheme Code: SB171, CD269) where these accounts are operated under Foreign Currency Regulation Act, 1976, in which withdrawal through Card is not permissible.
- Charge account is invalid (Like TDR/currency is other than INR/LOAN account).

Branches need to take necessary corrective action in respect of the above mentioned situation. Even if auto recovery fails, branch can remit card dues through PUSH Payment method by invoking **CCPAYMNT** menu in finacle.

B) PUSH PAYMENT (Payment Process by Branch)

I. Previous Process

a. Customer deposits cash/cheque in any of his/her account in the branch.

b. Card dues are credited to MBB A/c no. 010190200000001 through TM/Cash Receipt menu. The full card number of the customer is captured by the CBS user which is mentioned in CBS Transaction under Narration.

c. At end of the day, flat file is generated at HO-CPD, which contains the full card number, amount, date of transaction, transaction ID etc.

d. The file is processed by the Credit card Management System, on the following day (next working day). In case of holidays/weekly off, the file is processed on the next working day causing delay in the release of the credit card limit for the customers.

II. New Process (Through CCPAYMNT Menu)

a. Customer can give the Credit Card Payment mandate for payment of card dues through transfer from his/her account.

b. User shall invoke a new customized menu **"CCPAYMNT"** in Finacle which is integrated with Credit Card Management System through Application Program Interface (API). Here, the credit card holder shall provide his CUSTID and masked card number (only first 4 and last 4 digits of his card) to the CBS user instead of full card number. The card number in CCMS shall be validated through a combination of masked card number and CUSTID. **Branch must not obtain full card details with mandate/cheque.**

c. CBS will show the Minimum Amount Due (MAD) and total amount due (TAD) against that particular card to the CBS user as per the latest billing.

d. The user needs to select the Debit Account Number from the list of the account numbers of the customer, as per the customer mandate. Other operative accounts of the customer along with available balance & status of account shall be displayed to help take instant decision.

e. Based on customer mandate, the CBS will initiate the payment through masked card number, CUSTID, RRN and the amount of transaction.

f. Upon verification of the CBS transaction, the transaction amount shall be adjusted/reflected in Worldline CCMS and the Credit card limit is released on real time basis. The customer shall also receive SMS immediately after the same is accounted in Credit card system. However, if credit card limit is already blocked, it will not be released on real time basis.

g. All payments invoked through **'CCPAYMNT'** are credited to that particular SOL's **XXXXXSUNCR897** account throughout the day. At the time of Data Centre's day end, all credit lying in **XXXXXSUNCR897** account is debited and credit is given to HO-CPD office account (**01010LN008**) for reconciliation purpose.
Note: Branch is not supposed to Debit **XXXXXSUNCR897** account under any circumstances. Branch to only credit this account through 'CCPAYMNT' menu. Branch to write to CPD for any rectification entry and not to manually pass any entry in the Account **XXXXXSUNCR897**.

h. To activate payment through Internet/Mobile Banking/Payment Gateway, separate communication shall be sent.

Debit Card

- **For Issue of Debit Card account must be Active, KYC complied and Mobile Number seeded.**

Eligibility:

- saving accounts,
- Current accounts
- Overdraft accounts.
- Cash Credit account
- Kisan Credit Card (KCC) a/c
- Special Schemes of a/c

Not Eligible:

- Mobile Number Not seeded in a/c (Except Special Scheme)
- Company, Trust, Club, Societies, Government and Quasi-Government Departments
- Cash Credit (except KCC & Mudra)
- Illiterate persons (except special schemes)

Operation Instruction:

- ✓ **Jointly Operated account not eligible for Debit Card.**
- ✓ For "Either or Survivor" OR "Any one of Us", Card may be issued to all joint account holders (The number of cards issued in an account will not exceed the number of joint account holders).
- ✓ For "Former or Survivor", In such case Debit Card shall be issued to Former/First Account holder only joint accounts.
- ✓ For partnership (as per the operating instructions mentioned in the partnership agreement)
- ✓ For HUF Operative Accounts to KARTA with the consent of all co-parceners.
- ✓ For mandate, letter of authority/Application for issuance of Debit Card is executed by all the account holders.
- ✓ For NRE self or Power of Attorney (POA) / Mandate.

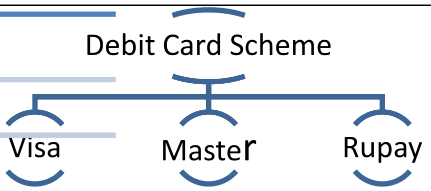
- **Illiterate persons – Aadhar enabled/biometric card only. Allowed other cards only if under special schemes**

- **Self-operated Minor's Account where age is 15 years and above, with limited facility (BINGO Card)**

Forms of Card

Personalised

Non -Personalised



How to issue Debit Card

- At the time of a/c open.
- Enter in ADCREQ Menu (Personalized and Non-Personalized
- Ready Kit (Non-Personalized "Name not Printed on Card)
- Welcome Kit (Non-Personalized)

Replacement/Re-issue of Card

Enter in ATMCRA for Personalised or reissue (Before reissue delete existing Card) the ready kit for Non-Personalised. (Charges applicable)

Renewal of Card

All cards which are going to expire are auto Renew in Advance and send to customer address.

Card not Renew:

- ✓ Transactions not initiated during the last six months of expiry date of the card, closed account, Cards are hotlisted/inactive.
- ✓ Account closed/dormant/NPA

PIN/INSTA PIN:

- All Personalized Card PIN should be issued by Branch through ATMCRA or Card holder cans Generate Green PIN through BOI ATM only.
- Ready kit/Welcome Kit PIN already Kept in Kit need not to issue

RE-PIN:

Branch can Issue Re-PIN through ATMCRA (Charges applicable)

Green PIN

Card Holder can Generate/Regenerate the PIN through BOI ATM only (For Generation of PIN, Necessary OTP send to Card holder registered Mobile number only)

Delivery of Card

All Personalised card (New/Renewal/Replacement) send to Customer Address which is mention in cumm through Register post as per TAT it should be delivered within 7 days. If it is return then send to Branch. (SMS is sending for return card).

Card Track

Personalised Card can be track through CARDTRAK Menu in Finacle (Return Card Also) after 3 day enter in Finacle.

Activation of Card

- ✓ Personalized card already activated branch can Issue PIN or Card holder can generate Green PIN through BOI ATM only
- ✓ **Non-Personalized Card (Ready Kit/ Welcome Kit)** activated with in same day (twice in day by 2.00 p.m. and 9.00 p.m.**)**

Activation of PIN/Green PIN

- ✓ Green PIN activated immediately
- ✓ PIN issued by Branch activate 4 times a day (11.00am; 1.00 pm; 5.00 pm and 9.00 pm**)**

Types of PIN/INSTA PIN

1. Master Card pins start with 4. Eg. 4000 0000 9008
2. Rupay Pins start with 7 eg. 7000 0000 1234
3. Visa 4052 BIN Card PIN start with 5 eg: 5000 0000 5647
4. Visa all other BINs(except 4052) start with 6 eg: 6000 0000 9876

VISA						
Product Name	**BIN**	**Code**	**Cash Limit**	**POS Limit**	**Valid In**	**Whom to issue**
VISA Classic EMV	459845	C	15000	25000	International	All SB, CD & OD
Visa PayWave	457624	M	50000	100000	International	Only diamond a/c
VISA EMV Platinum	457624	E	50000	100000	International	Only diamond a/c
VISA Business Debit	483830	V	100000	250000	International	Only CD (6 months satisfactory operation)
Master						
Master Debit	526495	D	15000	25000	Domestic only	All SB, CD & OD
Master Titanium	517394	I	15000	25000	International	All SB, CD & OD
Master EMV Platinum	557589	P	50000	100000	International	Only diamond a/c
Master BINGO	519622	B	15000	25000	Domestic only	SB (Age-15-25)
Welcome KIT	519622	W	15000	25000	Domestic only	Only SB
Master Business Debit	514840	S	100000	250000	International	Only CD (6 months satisfactory operation)
RuPay						
RuPay Debit	606998	Y	15000	25000	Domestic only	All SB, CD & OD
RuPay NCMC	607947	1	15000	25000	Domestic only	All SB, CD & OD
RuPay Platinum	652165	F	50000	100000	International	All SB, CD & OD
RuPay SANGANI	607713	U	15000	25000	Domestic only	All SB, CD & OD

RuPay Star Vidhya	504493	A	15000	25000	Domestic only	All SB, CD & OD
RuPay Jandhan	607927	J	15000	25000	Domestic only	JAN DHAN a/c (Govt. Scheme)
RuPay Kisan	607002	K	15000	25000	Domestic only	KCC a/c (Govt. Scheme)
Mudra Card	607036	Z	15000	25000	Domestic only	Loan a/c (Govt. Scheme)
RuPay Punjab Arthia	607265	L	15000	25000	Domestic only	a/c arthia code (Govt. Scheme)
RuPay Punjab Farmer	607265	G	15000	25000	Domestic only	a/c arthia code (Govt. Scheme)
RuPay Haryana Arthia	607530	O	15000	25000	Domestic only	a/c arthia code (Govt. Scheme)
RuPay Dhan Aadhar	508505	H	15000	25000	Domestic only	KCC account (Govt. Scheme)
RuPay PMKVY	508885	N	15000	25000	Domestic only	PMKVY a/c (Govt. Scheme)

- ✓ Govt. Scheme Debit Card Send Directly without any request from A/c Holder to Customer address
- ✓ Cash Limit is per day limit on BOI ATM, per transaction is Rs.15, 000.
- ✓ Cash Limit for Other ATM only Rs.15, 000/- per day and per transaction is Rs.10, 000.
- ✓ POS/e com transaction limit is per day limit, no per transaction Limit
- ✓ Maximum 3 transaction on ATM per day.

Debit Card Charges (excluding GST)				PIN Charges (excluding GST)		
Card Type	New	Annual Fee	✓ Non-Personalized (Ready Kit Welcome kit Rs.150 for new ✓ Additional/Replacement Card Rs.150.	New INSTA	Green PIN	Re PIN
Classic	150	150		Free	Free	100
Platinum	200	200		❖ Staff / Ex- Staff are free from any type of charges in Staff account only		
Business	300	250				
Contact Less	200	200				

If Balance not available then it will debit when balance available

ATM transaction Charges on Debit Card				Surcharges on Debit Card (IRCTC & Fuel)	
	BOI ATM	Other ATM	Charge	✓ 2.5 + GST (18%) on transaction amount. ✓ Minimum Rs.25 IRCTC and Rs.10 on Fuel	
Financial	Unlimited Free	3- Free in Metro	20 +GST		
		5- Free in other		**International transaction Charges**	
Non-Financial	Unlimited Free	3- Free in Metro	8 +GST	Financial	2.5 % + Currency Conversion
		5- Free in other		Non-Financial	@25 Per transaction

Charges not Applicable

- ➢ Star Doctor Plus (OD) – Free including Annual Charges
- ➢ Star Benefit CD Plus - Individual and Proprietorship free for 1st year. Annual charges from 2nd yr. onwards.
- ➢ Star Diamond Savings Account – Platinum Debit Card Free including Annual charges.
- ➢ Star Power Salary Account - SB - Free ATM International Debit Card for 1st year, Annual Charges applicable from next year.
- ➢ BOI Saral Salary Account Scheme - Free Debit Card to all. Free Platinum Debit Card to employees with minimum take home salary of Rs.25000/ p.m. or AQB in S/B Account is Rs.1 Lakh.

- ➢ Star Suraksha Savings Bank Plus - Free Debit Card for first year, Annual Charges applicable from next year.
- ➢ Star Senior Citizen Savings Bank - Free Global Debit cum ATM Card. NIL Annual Charges from next year.
- ➢ Star Mahila Savings Bank - Free Global Debit cum ATM Card-NIL Annual Charges from next year.
- ➢ Star Gurukul Savings Bank - Free global Debit cum ATM Card to all. NIL Annual Charges from next year.
- ➢ Free Platinum Card for higher salary earners - Annual charges applicable from next year.
- ➢ Bingo Cards - Nil Issuance charges for the first year. Maintenance charges from the 2nd year

Hot listing of Debit Card

Toll-free / Landline number E-mail for hot listing. (27x7)	**Toll Fee No.-** 1800 425 1112 **Land Line:**(022) 40429123 / (022)40429127 **Manual:** (044) 39113784 / (044) 71721112 **Email:** PSS.hotcard@fisglobal.com (27x7)
Informing the branch in writing	Branch send an email to - PSS.Hotcard@fisglobal.com (27x7)

- ✓ Delete from ADCREQ Menu Card is not Hot listed immediately, it will hotlist by DC in two times in a day
- ✓ Hot listing through a/c Number then all card will be hot listed including add on Card
- ✓ Once card is hot listed cannot be Revoke and to replace automatically
- ✓ AMC will be recovering after hotlisting also for this year.

Debit Card Disputed/Failed Transaction and Reversal

- ✓ If transaction fails during transaction on ATM and POS, it will auto reverse within 48 hours, not reverse then process to ATMREV and POSREV.
- ✓ ATM and POS Refund claims also initiated though our Bank Website

	Master	VISA	RuPay
ATM Reversal	5 days	5 days	5 days
POS Reversal	45	15	15

- ❖ Customers are getting SMS of ATM and POS Reversal, in each level acceptance, rejection and Pre arbitration also.

- ❖ **Pre-arbitration:** Rejected claims disputes in first level are raised in within 15 days for Visa and RuPay, 45 day for Master of rejection of disputes in First level.

Debit Card Transaction Remarks

CWDR- **ATM** withdrawal CWRR- ATM Reversal transaction	MEDR- POS or e com transaction MERR - POS or e com reversal transaction

Debit Card Apps - "BOI Card Shield"

It is integrated into BOI Mobile Banking App

For registration:

6. Click on New User and enter the card details. 6-digit security code will be generated and sent on the registered mobile number with Bank. Set your username and password. Use a minimum password length of 8 or more characters including lowercase and uppercase alphabetic characters, numbers and symbol
7. You will receive a confirmation email for successful registration.
8. Login to your app using created Username and password.

Feature of "BOI Card Shield": ✓ Switch card on/off the Card. ✓ Control by location ✓ Set Spend Limits ✓ Set Transaction Types	✓ BOI CardShield enables you to add multiple debit cards by using option "Manage account". BOI Card Shield allows you to add your dependent's card through OTP authentication. You can set control preferences and limits for them as well and receive alerts. This will allow you to monitor and track your dependent's spending behavior. ✓ Please contact Helpdesk Support +912233865300 extn: 22445/22446/22447/22448

✓ Set Merchant Categories ✓ Instant transaction alerts ✓ Other Self Service	

Debit Card Loyalty/Offer

BOI Star Rewards Programme - For every Rs. 100/- spent through a BOI Debit Cards on ECOM and POS, the customer earns 1 Reward Point., All the Points including Bonus Points will be valued at Rs.0.25.

Points earned	Awarding Points	Point Value	**How to Redeem**
1 Point per Rs.100	Rs. 0 to Rs. 5,000 in Months	25 paise	Visit - **www.boistarrewardz.com** **Toll Free Number – 18002099299** **(Customer can redeem star Points 27x7 by: Visiting website ang logging into your personal BOI Star Rewardz account OR calling our toll-free Number from 9 am to 9 pm (Monday to Saturday) Download the apps from play store – BOI star Rewardz**
1.5 Point per Rs. 100	Rs. 5001 to 10,000 in Months Customer will be awarded 0.50 Bonus Point only for the transaction value between Rs. 5,001/- to Rs. 10,000/- and not for all the transactions ones he crosses the Rs.5001/- threshold limit.	25 paise	
2 Point per Rs. 100	Rs. 10,001/- and above, in a month. It is clarified that the Customer will be awarded 1 Bonus Point only for the transaction value Rs. 10,001/- above and not for all the transactions ones he crosses the Rs.10, 001/- threshold limit.	25 paise	

Airport Lounge Access

- ✓ RuPay and Master **Platinum** Card Holder access the Airport Lounge 2(Two) times in a Quarter, Charges @Rs. 2 for RuPay and @25 for Master.
- ✓ Airport Lounge list available on RuPay and Master Website**.**

Offers on Debit Card

- ✓ Various offer of BOI Debit card of Master, RuPay and VISA available on time to time
- ✓ Offer details updated on in Bank/Scheme Website, BOI Twitter account and sending through SMS also.

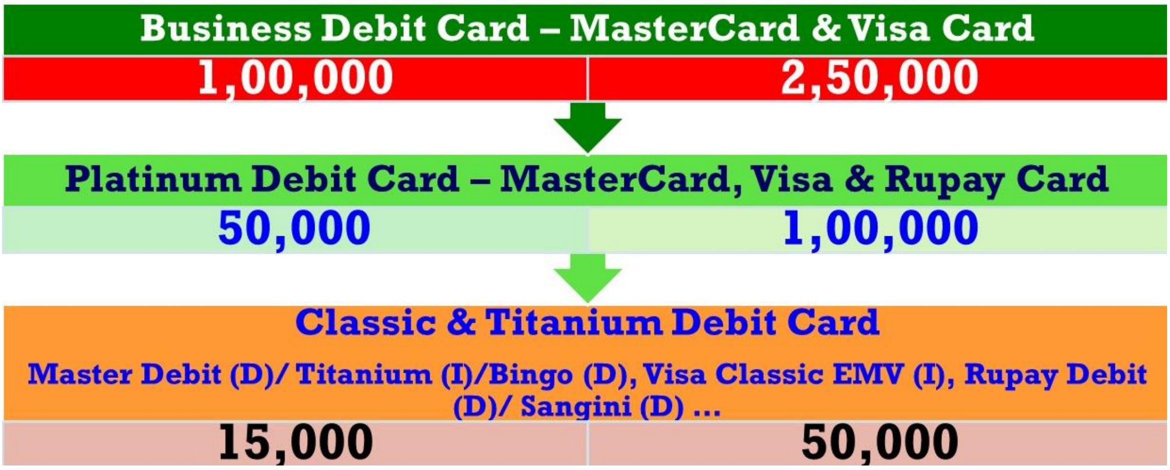
Reference/ Circular:

- 109/083, 08.07.2015, INTRODUCTION OF BUSINESS CARDS - DEBIT & CREDIT
- 107/223, 06.03.2014, Launch of Debit Card, specially designed for women account holders
- 107/144, 21.10.2013, Debit Cards: Operational Changes (Automatic Unblocking of cards)
- 107/083, 01.08.2013, Pins for Personalized Debit Cards Change in Delivery Procedure
- 107/029 18.05.2013 Mandatory Use of Debit ATM Card by Staff Members
- 107/022 03.05.2013 Bank of India -Debit Cards - Master Circular
- 105/127 28.10.2011 Launch of "BOI Star Reward Programme" for Debit Card Holders
- 104/091 03.11.2010 Introduction of BINGO Cards Specially designed Debit Card for the Youth
- 104/083 13.10.2010 Introduction of Bank of India's Platinum Debit-Cum-ATM Card
- 104/073 08.09.2010 StarConnect Retail Internet Banking Services - Addition of Facility Debit-cum-ATM card Hot list/ Pin Change/ Reset and Unblock.
- 103/098 02.09.2009 Issuance of Instant-Pin for ATM cum Debit Card at the Branch
- CEADC: CPD: NK: 2019-20/40 dated 30.05.2019 - “BOI Card Shield”
- **113/076** 09.07.2019 HO: PD:SB:2019-20: 16 REPORT FOR DEBIT CARDS RETURNED TO BRANCH

- 113/005 01.04.2019 CPD:CM:2019-20/02 Policy/2019-20 /02 "Debit Card Management Policy”
- Service Charges Circular: Dated 12.12.2018 w.e.f.15.01.2019

This is only for handy and quick reference based on latest circular/ Policy for Internal used only

Debit Card Limits Summary



Business Debit Card – MasterCard & Visa Card	
1,00,000	2,50,000

Platinum Debit Card – MasterCard, Visa & Rupay Card	
50,000	1,00,000

Classic & Titanium Debit Card Master Debit (D)/ Titanium (I)/Bingo (D), Visa Classic EMV (I), Rupay Debit (D)/ Sangini (D) ...	
15,000	50,000

Charges for Credit Card – At a glance.

Interest free period.

- For Cash Advance – Nil.
- For Other Transactions - 21-51 days (applicable only on retail purchases and if previous month's outstanding balance is paid in full).

Charges on Revolving Credit.

Secured Credit (SwaDhan).

I. 1.20% per month (15.40% p.a.) on daily balances.
II. In case of default service charges is 1.70% p.m. (22.45 % p.a)

Unsecured Credit (Other than SwaDhan).

I. 1.70% p.m. (22.45% p.a.) on daily balances.
II. In case of default service charges is 2.50% p.m. (34.50 % p.a).

Minimum Repayment Amount - 10% of Total Outstanding, if revolving credit is opted + EMI (all EMI due) + other amount due.

Cash Advance Limit - For both Principal and Add-on card.

a. 50% of Spending Limit or available limit, whichever is lower.
b. Cash withdrawal up to 40% of spending limit of Primary card and up to 20% on Add-on Card.
c. Cash withdrawal per day Rs.50,000/- for Platinum card and Rs.15,000/- for rest variant.

Cash Advance Charges.

a. BOI ATM - 2% (minimum Rs. 50/-) for each transaction.
b. Other ATM - 2.5% (minimum Rs. 75/-) for each transaction.
c. Overseas ATM - 2.5% (minimum Rs. 125/-) for each transaction and Currency Conversion Charges, presently 2%.
d. Interest on dues / overdue applicable.

Star Easy Pay (EMI).

a. Processing Charges - One-Time i.e.1.00% of the Purchase (Existing 2.20%).
b. Finance Charge.
    I. 1.25 % of the Purchase (existing 1.50% p.m. on original amount).
    II. In case of default service charges is 2.50% p.m. (34.50 % p.a).
    III. Prepayment Charges – Nil.

Balance Enquiry Charges at ATM.

a. BOI ATM - Nil.
b. Other Bank ATM in India - Rs. 20/-.
c. Other Bank ATM Abroad - Rs. 25/-.

Payment of charges (Cash / Cheque / Online / NEFT / RTGS) – NIL.

Charges on over limit account (Purchase / Cash).

a. Secured Credit (SwaDhan) - 1.70% p.m. (22.45 % p.a) on daily balances.
b. Unsecured Credit (Other than SwaDhan) - 2.50% p.m. (34.50 % p.a) on daily balances.

Usage Over Spending Limit - Rs. 100/- per occasion.

- Outstation Cheque Processing Charge – As per prevailing rates.
- Payment Return Charges - Rs. 100/ - per instrument.
- PIN replacement Charges - Rs. 50/- (per occasion).
- Duplicate Bill Charges - Rs. 50/- per quarter (after 12 months).
- Retrieval of Charge Slip - Actual or Rs. 100/- whichever is higher.
- Balance Transfer Processing Charges – NIL.
- Fuel Transaction Surcharge - 2.5% of transaction amount (minimum Rs. 10/-) or
- Actual charges claimed by the Acquirer bank, whichever is higher.
- Railway Ticket Purchase or Cancellation Fee - Rs. 30/- charged by Railways + 2.5% (Min. Rs. 25/-) or Actual charges claimed by Railways / acquirer bank.
- Foreign Currency Transactions - 2% Currency Conversion Charges for all currencies, (excluding INR, being home currency). For all types of transaction, including cash withdrawal and transactions through POS / e-commerce / online.

Goods and Services Tax (GST).

a. Applicable on all Fees, Interest and other Charges.
b. The applicable GST would be dependent on place of provision and place of supply.
c. If POP and POS are in the same state then applicable GST would be CGST and SGST/UTGST else, IGST.
d. GST for fee and Charges / Interest transactions billed on statement date will reflect in next month statement.
e. GST levied will not be reversed on any dispute on Fee and Charges / interest.

Escalation Matrix

Nature of Issue	E-MAIL ID	Contact No.
Hot listing of Debit Card (For Branch/AMO/Zone/NBG as well as Customer)	PSS.Hotcard@fisglobal.com (27x7) ➢ Compulsory mention a/c No. or Card No. ➢ If only account number is Provided then all card will be hot listed ➢ If only Card No. is provided then only Particular Card will be hot listed	**Toll Fee No.-** 1800 425 1112 **Land Line:**(022) 40429123/ (022) 40429127 **Manual:** (044) 39113784/ (044) 71721112
Bulk Hot listing of Debit Card	Headoffice.CPDdebitcard@bankofindia.co.in ➢ Send mail in Proper format i.e. Notepad file (Kept in KRISH folder)	
Debit Card not active/activated, Card invalid, not working on POS or online, OTP not received, Green PIN not Generate	switch.support@fisglobal.com ➢ (For Branch/AMO/Zone/NBG use only)	9833996639
Debit Card not Received (New /Renewal/ Replacement)	Headoffice.CPDdebitcard@bankofindia.co.in ➢ Before email please Check through "CARDTRAK" Menu in Finacle	022-61312940 022-61312939
Request for PINS & Ready Kits	Headoffice.CPDdebitcard@bankofindia.co.in	022-61312940 & 39
Debit Card Apps (BOI Card shield) related Issue	HeadOffice.CPDCardShield@bankofindia.co.in Poonam.Kumari7@bankofindia.co.in	022-61312946
Insurance claims for Fraudulent transactions through Debit Card **(Not for UPI and Internet Banking)**	HeadOffice.CPDInsurance@bankofindia.co.in	022-61312937
Card active but not reflecting in CARDSTAT Menu (Finacle)	Kovendan.V@bankofindia.co.in RAMYADEVIS.S@bankofindia.co.in Gautam.Kumar5@bankofindia.co.in	
ATM failed transaction, ATMREV or any transaction refund issue	nfs.isg@bankofindia.co.in HO.ATMcell@bankofindia.co.in	022-61319474 (Offus) 022-61319475 (Onus)
POS Failed transaction, POSREV or transaction refund issue pertaining to Debit Card	POS.ISG@bankofindia.co.in HO.ATMcell@bankofindia.co.in	022-61319480 022-61319481
Finacle related issue on Debit card (Unable to add/ verify / cancel and add in Stock etc)	Helpdesk.Escalation@bankofindia.co.in ➢ Also lodge a call on Service Manager	IP-11111
Any UPI transaction related issue like BHIM / GPAY/ PhonePay etc / BUPI TXN	Support.MobileApps@bankofindia.co.in	022-67447025
SMS not received	SMS.Alert@bankofindia.co.in	022-61312986
Card not display on Internet Banking or transaction related Issue BDIPG /STUBP TXN	HO.InternetBanking@bankofindia.co.in Boi.Starconnect@bankofindia.co.in	022-61319487/88 022-61319489/90
Request for Welcome kit	Headoffice.CBOD@bankofindia.co.in	022-61312976
Debit Card Insurance (Accidental) claim (RuPay only)	rupay@newindia.co.in Headoffice.Financialinclusion@bankofindia.co.in	022-26591702 022-66684658
Loyalty Reward points for Debit and Credit Card	membersupport@boistarrewardz.com nilambari.toke@loylty.com	1800 209 9299 022- 61312959

- ✓ Any query related to Debit card mail to Headoffice.CPDdebitcard@bankofindia.co.in **-022-61313940**
- ✓ Always mark a copy **to Headoffice.CPDdebitcard@bankofindia.co.in** in each and every mail request to vendor.

RuPay Chargeback

In case of any fraudulent ATM/POS/ECOM transactions (Debit/Credit Cards), where customer claims that he/she has not done the transaction, kindly follow the below mentioned process:

STEP-1: **Hotlist** the Card immediately.
For Debit Cards: Mail to pss.hotcard@fisglobal.com (Toll Free No. 18004251112, 022-40429123/7)
For Credit Cards: Mail to -
headoffice.cpdcreditcard@bankofindia.co.in;
CC to wl-in.boicreditcards@worldline.com
(Toll Free No. 022-40426005/6; 1800220088)

Step-2: Ask the customer to lodge the Police Complaint (if disputed amount is less than Rs.50000/-) and FIR (if disputed amount is more than Rs.50000/-) It may raise to Rs. 1,00,000/- next year.
NOTE: Police Complaint/FIR is compulsory only in case customer is filing for Insurance (given in Step-4). No police Complaint/FIR is required for lodging Chargeback (given in Step-3)

STEP-3: **Chargeback/Reversal Request**: To be lodged maximum within 60 days from the date of transaction.

- For POS/ECOM Transactions (Finacle Narration starting with MEDR) – Upload request in Finacle menu POSREV or customer can lodge the same through Internet Banking. Please send mail for MEDR txn to - POS.ISG@bankofindia.co.in and CC to - ho.atmcell@bankofindia.co.in along with reversal Ref. No.
- For ATM Transactions (Finacle Narration starting with CWDR) - Upload request in Finacle menu ATMREV or customer can lodge the same through Internet Banking. Please send mail for CWDR txn to - nfs.isg@bankofindia.co.in and CC to - ho.atmcell@bankofindia.co.in along with reversal Ref. No.
- For Billdesk Transactions (Finacle Narration starting with BDIPG/STUBP) – Mail all details of the transaction to - Boi.Starconnect@bankofindia.co.in in below format.

Sr. No.	Date of Transaction	BDIPG/STUBP ref. No. (in Full)	Amount (Rs.)	A/c no.

STEP-4: Insurance Claim:

- All thirteen documents (2 copies) to be submitted in one go for onward submission to Insurance Company (attached herewith as insformat.rar). All documents should be properly checked, verified and signed with bank seal. Please refer the attached excel (Insurance_claim_checklist.xlsx) for further clarification about the documents to be submitted. (As per email shared with all zones/branches)
- All the documents need to be shared (only hard copy) at below mentioned address within 180 days from the date of disputed transaction.
- In case of any clarifications: contact 022-61312942 or send mail HeadOffice.Rupaychargeback@bankofindia.co.in

Address:
Bank of India, Head Office,
Card Product department – RuPay Chargeback,
First Floor, Star House 2, C-5, G-Block, Bandra Kurla Complex,
Bandra (E), Mumbai – 400051

Master Chargeback

ISSUER

NATURE OF QUERY/PROCESS	RESOLUTION PROCEDURE AND RELATED TAT
Chargeback for disputed transaction	Chargeback to be lodged within 120 days from date of transaction. The e-mail or document provided for raising chargeback should clearly mention the details related to transaction for which chargeback is to be raised.
Representment time	For Cash transactions after lodgment of charge back TAT is 8+2 days and for POS transactions TAT is 45+2 days.
Rejected Chargeback	In case of rejection of chargeback, supporting documents are provided to branches and/or customers. If requires, the Bank can apply for pre-arbitration.
Pre arbitration /Pre compliance	After rejection of representment, pre arbitration can be raised within 30 days or time expired for representment which is earlier.
Retrieval request for copy for disputed transaction	Retrieval request can be raised within 120 days from date of transaction.
Arbitration / compliance	After rejection of Pre arbitration, Arbitration can be raised within 45 days or time expired for representment which is earlier.
Good faith	After expiry of chargeback time good faith request can be raised but refund of disputed amount depend on the mercy of acquirer bank.

ACQUIRER

Chargeback against Merchant for disputed transaction	When the Bank receive the chargeback against the Bank's merchant, the disputed amount will be debited from the merchant's account on the same day/T+1 day. The same is informed to branch and merchant via e-mail and also ask for necessary document so that we can represent the same.
Representment	Once the Bank gets the required correct documents, the Bank will credit the disputed amount back to the merchant' account. If merchant has not sent any document then after the expiry of the 45 days, Bank will not be liable to refund the disputed amount debited.

For lodgment of chargeback or any other query related to Master Credit Card, below is the e-mail-id: Master chargeback Department HeadOffice.Masterchargeback@bankofindia.co.in
Contact Number: 022-6132934

Visa Chargeback

Issuing Chargeback:

For all the Visa credit card complaints received through Emails/Call center/By phone, process the chargeback for the reversal of the amount. Below are the stages of chargeback with Time Limit.

Process Name	**Visa**
Transaction Processing Time Limits & Dates	Timelines for acquirer processing of all India domestic transaction maximum up to 5 calendar days from date of transaction. Exception- Cruise liner, Lodging merchant (Hotel), Vehicle rental merchant for India domestic transaction- 7 calendar days.
Retrieval Request for Copy for Disputed Transaction	Retrieval request can be raised within 60 days from date of transaction as per applicable reason code
Chargeback for Disputed Transaction	Chargeback request can be raised within 60 days from date of transaction as per applicable reason code
Re-presentment Time	FOR Cash transactions after Lodgment of charge back TAT is 8 days and for POS & E COM transactions TAT is 15 days
Pre-arbitration / Pre-compliance	After rejection of re-presentment, pre-arbitration can be raised within 10-15 days or time expired for re-presentment which is earlier.
Arbitration / Compliance	After rejection of Pre-arbitration, Arbitration can be raised within 5 days or time expired for re-presentment which is earlier
Good faith	After expiry of chargeback time good faith request can be raised but refund of disputed amount on the mercy of acquirer bank

Acquiring Chargeback:
The chargeback received against our merchants will be processed under acquiring chargeback. Merchant Account will be debited once we receive the chargeback. We follow up with Merchant/Branch for the supporting documents. Once we receive documents from merchant and our chargeback will be accepted by the Issuing bank, we will credit back the amount to merchant. Time Limits for the re-presentment will be same as issuing as chargeback.

Escalation: HeadOffice.VisaChargeback@bankofindia.co.in

****

Forwarding letter

Date:

THE NEW INDIA ASSURANCE COMPANY LIMTED

Centralized Claim Hub, MRO –I

12th Floor, New India Centre, 17/A,
Cooperage Road, Mumbai – 400 039

Dear Sir,

Subject: INSURANCE CLAIM – BANK OF INDIA DEBIT/CREDIT CARD

This is with reference to the insurance claim of Mr. / Ms. (name). We hereby confirm that the customer held an account in Bank of India and held a valid Bank of India Debit/Credit Card at the time of the occurrence of the event for which the claim is being made. We certify that the details of the customer as per the records maintained by Bank of India are as follows:

Claim filed for	I Lost Card Liability II Purchase Protection III Personal Accident
Name of the Customer	
Date of Occurrence	
Account Type and Number	
Debit/Credit Card Number	
Debit/Credit Card Valid From – Valid To	
Policy No (to be filled as per advise from Central Office)	
First transaction Date of the Debit/Credit Card	
Residential Address	
Date of Birth	

We also confirm that the following documents (duly attested by a notary public, gazetted officer or Bank of India, Branch Head) have been submitted as per the requirements of **The New India Assurance Company Ltd**.:
(Please tick the documents enclosed)

I Lost Card Liability

- □ Completed Claim Form (English / Hindi)
- □ Attested copy of FIR / General Complaint to Police (If in regional language then submit English / Hindi translation)
- □ Bank Statement (indicating forged transaction)
- □ Attested Copy of Final Report from Police (If in regional language then submit English / Hindi translation)
- □ Certification from Bank of India certifying the Date & Time of blocking of the Debit/Credit Card after intimation from Card Holder regarding the loss of the same.

□ Attested Identity proof of Claimant

<u>II Counterfeit/Skimming card Liability</u>

□ Completed Claim Form (English / Hindi)
□ Attested copy of FIR / General Complaint to Police (If in regional language then submit English / Hindi translation)
□ Bank Statement (indicating forged transaction)
□ Attested Copy of Final Report from Police (If in regional language then submit English / Hindi translation)
□ Certification from Bank of India certifying the Date & Time of blocking of the Debit/Credit Card after intimation from Card Holder regarding the loss of the same.
□ Attested Identity proof of claimant

III Purchase Protection

□ Completed Burglary/ Fire Claim Form (English / Hindi)
□ Attested copy of FIR / General Complaint / CR to Police
□ Photocopy of Debit/Credit Card
□ Proof of purchase (bill, charge slip, bank statement)
□ Bank Statement (indicating transaction)
□ Attested Copy of Final Report from Police
□ Attested copy of fire brigade report in case of fire
□ Advance letter of subrogation on a Rs. 20/- stamp paper in case of burglary / theft
□ Attested Identity Proof of claimant

III Personal Accident

□ Completed Claim Form (English / Hindi)
□ Attested copy of FIR to Police
□ Attested copy of Panchnama / Inquest Panchnama
□ Photocopy of Debit/Credit Card
□ Attested copy of Post Mortem Report
□ Attested copy of Statement of Witness, if any lodged with police authorities
□ Original Death Certificate
□ Burial Certificate (wherever applicable)
□ Attested copy of Drivers License (In case of a motor / vehicular accident where the deceased was driving)

Thanking you,

Yours Sincerely,

Branch Head
Branch Name
Bank of India

****

Claim Form

THE NEW INDIA ASSURANCE COMPANY LIMTED
CLAIMS-HUB, MUMBAI REGIONAL OFFICE –I
12th Floor, New India Centre, 17/A, Cooperage Road, Mumbai – 400 039.
Ph: 022-24620377, Fax: 022-22045100, email: ch11@newindia.co.in

Claim Form For All Risk Insurance

Notification of Physical Loss or Damage
(The issue of this form is not to be taken as an Admission of Liability)

PLEASE ANSWER ALL QUESTIONS FULLY

S. N.	Details of Insured	
1	Name	
2	Bank of India Debit Card/Credit Card Number	
3	Bank of India Account number	
4	Occupation	
5	Address for Correspondence	
6	Contact no./ Email ID	
7	Nature of loss/damage (Cash/ Purchase)	
8	Place & address where the loss took place.	
9	Date and time when loss was first discovered	
10	Is SMS facility activated	
11	Date and time of SMS received to lost amount	
11	Estimated value of loss/damage	
12	Date & time of filing FIR	
13	Name & address of Police station	
14	Have you sustained loss of the same nature state debit/credit card number	

15	Any additional information relevant to processing of claim	
16	Type of claim	Lost Card /Skimming Cases

I/We hereby agree, affirm and declare that:

i. The statements/information given/stated by me/us in this claim form is true, correct and complete.

ii. This is to certify that Mr. ____ has a saving /current/ other account No.____ and possesses debit/Credit/Other card no. _____________________________________ on which we have reported Lost card / counterfeit liability of Rs. ______________ , we have verified the detail and found correct in all respect and no claim is made of the same to another Institution/company.

iii. No material information which is relevant to the processing of the claim or which in any manner has a bearing on the claim has been withheld or not disclosed.

iv. If I/We have given/made any false or fraudulent statement/information, or suppressed or concealed or in any manner failed to disclose material information, the policy shall be void and that I/We shall not be entitled to all/any rights to recover there under in respect of any or all claims, past, present or future.

v. The receipt of this claim form/other supporting related documents does not constitute or be deemed to constitute an agreement by the company of the claim and the company reserves the right to process or reject or require further/additional information in respect of the claim.

Signature of Bank of India with seal
Branch Head/ Operation Head

Name in full:
S. R. No.-
Branch Name:
Designation:

Signature of Claimant
Name in full:-

Address:-

****

Claim Voucher

THE NEW INDIA ASSURANCE COMPANY LTD

CLAIM VOUCHER

Received from THE NEW INDIA ASSURANCE COMPANY LTD / (Bank of India) through its Policy Issuing Office (/ Bank of India Branch) the sum of Rs. __________ (Rupees _______________ Only) in full and final settlement of my/our claim in respect of the event dated __/__/____involving (description of event)_______________________ _____________________________________ lodged for Mr. / Ms. _____________________ who had been using Credit/Debit card No.__________________________ with Bank of India at (Branch)__________________________ and was issued Credit/Debit Card No. _________________

I / We agree that this payment absolves THE NEW INDIA ASSURANCE COMPANY LTD and Bank of India from any future liability whether now or hereafter in respect of this even Special Contingency Insurance Policy No. _____________________ and Serial No.____________________

Name and Address of the Assignee:

Please affix a revenu

Signature of the Assignee (in full)

Witnessed by:

Name	Address	Signature
1.		
2.		

Copy to be forwarded to AVP – Cards, Bank of India, Retail Banking Department, Central Office

Ref: Policy No ______________________

S. No ______________________

****

LETTER OF SUBROGATION

(TO BE EXECUTED BY THE INSURED
AND THE WITNESS WITH THEIR SIGNATURE)

LETTER OF SUBROGATION

THE NEW INDIA ASSURANCE CO LTD
BO/DO
Centralized Claim Hub, MRO-I
12th Floor, New India Centre, 17/A
Cooperge Road,Mumbai-400039.

Dear Sirs,
Re : Cardholder's Name.________________________
Debit / Credit card no.______________________
Account No. ________________________________
Interest Covered __________________________

We hereby acknowledge receipt of a sum of Rs.__________ (RUPEES ______________________________) which you have paid to us and which we have accepted in full & final settlement of our claim in respect of a claim preferred by us for loss of property occurred due to ________________on _____________.

We further declared and agreed that by virtue of the aforesaid payment the underwriter concerned became subrogated to all our rights, interest and remedies in respect of the aforesaid subject matter in accordance with the laws governing the contract of insurance. We also declare and agreed that the said New India Assurance Co Ltd. shall have unequivocal rights and authority to use our name to the extent as may be necessary to effectively exercise all or any such rights and or remedies that we will furnish them with any assistance they may reasonable require of us when exercising such rights and whilst on their part they will indemnify us against liability for costs, charges, expenses arising out of and in connection with any proceedings which they may initiate in our name in exercise of such rights and remedies.

DATED THIS __________DAY OF __________20____________AT ____________.

SIGNATURE OF THE INSURED (Bank of India):
NAME:
ADDRESS:

WITNESSED BY
SIGNATURE
NAME
ADDRESS

Assignee Signature
Name
Address

****

Branch Investigation Report

Name of Claimant-

Card – Credit card / Debit card

Card no.-

Account no (in case of debit card)-

Type of card- Normal / Platinum

Maximum limit of insurance provided- upto one lac for Normal card / upto four lac for Platinum card

Claimed amount on the card-

Date of fraud-

Place of fraud-

Date and time of request of hot listing-

Date and time of hot listing

Date of filing Police complain / FIR-

Date of filing Chargeback

Date of rejection of chargeback

Brief history of SMS delivered- Yes / No

TXN DATE	TXN TIME	SMS Delivery Status	Registered Mobile no	Amount Debited	TXN details (CWDR/MEDR/BDIPG)

Any other information helpful in processing the claim
Brief detail of Incident of fraud-

Here I confirm that there is no involvement of any bank official/staff in this fraudulent act and this is done by fully cloned card.
Name
Designation
Emp. Code- Signature with seal of Bank official
Date:

****

SMS Delivery Report

BANK OF INDIA

BRANCH -

SMS DELIVERY REPORT

TXN DATE	TXN TIME	CARD NO	CBS A/C NO	REGISTERED MOBILE NO AT THE TIME OF TXN	TXN AMOUNT	TXN DETAILS CWDR/ MEDR/ BDIPG	DELIVERY STATUS YES/NO

****

Check List of Document

SR. NO.	CHECK LIST DOCUMENT FOR BRANCH FOR INSURANCE CLAIM	YES	NO
1	INSURANCE CLAIM FORWARDING LETTER BY BRANCH		
2	CLAIM FORM		
3	CLAIM VOUCHER		
4	LETTER OF SUBROGATION		
5	INVESTIGATION REPORT BY BRANCH		
6	SMS DELIVERY REPORT		
7	INITIAL INTIMATION BY CARD HOLDER		
8	POLICE COMPLAIN / FIR COPY / FINAL REPORT		
9	CHARGE BACK REJECTION REPORT		
10	HOTLISTING REPORT OF CARD		
11	PHOTO COPY OF HOTLISTED CARD		
12	ID PROOF OF CARD HOLDER		
13	ACCOUNT STATEMENT		
ALL ABOVE-MENTIONED FORMS ARE TO BE FILLED PROPERLY AND TO BE SIGNED BY CUSTOMERS AS WELL AS BRANCH OFFICIAL WITH BRANCH SEAL WHERE EVER REQUIRED			

We attached herewith all claim forms and check list for record and needful action. Please be guided by **Branch circular No. 108/34 dated 03-05-2014** for dealing with disputed Card transactions.

In case of wrongful withdrawal reported by customer, branch to follow procedure as under

>Hotlist the card on pss.hotcard@fisglobal.com

>Lodge the charge back claim in Finacle system (Menu- **ATMREV for CWDR** & **POSREV for MEDR** and send mail to Internet banking dept. / star connect dept. for BDIPG transactions)

>Wait for cooling period of 7 days for cash and 15 days for other than cash transaction.

>The process of the activity can be obtained from HO ATM CELL / Star connect dept.

>If chargeback is rejected, lodge insurance claim.

**For lodgment of insurance claim, Branch should submit the attached documents.

Please ensure the Forms are filled in completely and get the signatures at proper space on the forms

Claim form for all risk insurance --- to be signed by cardholder as well as by Branch Head with seal.

For All insurance related issue contact to – 022-61312937
Email Id: HeadOffice.CPDInsurance@bankofindia.co.in

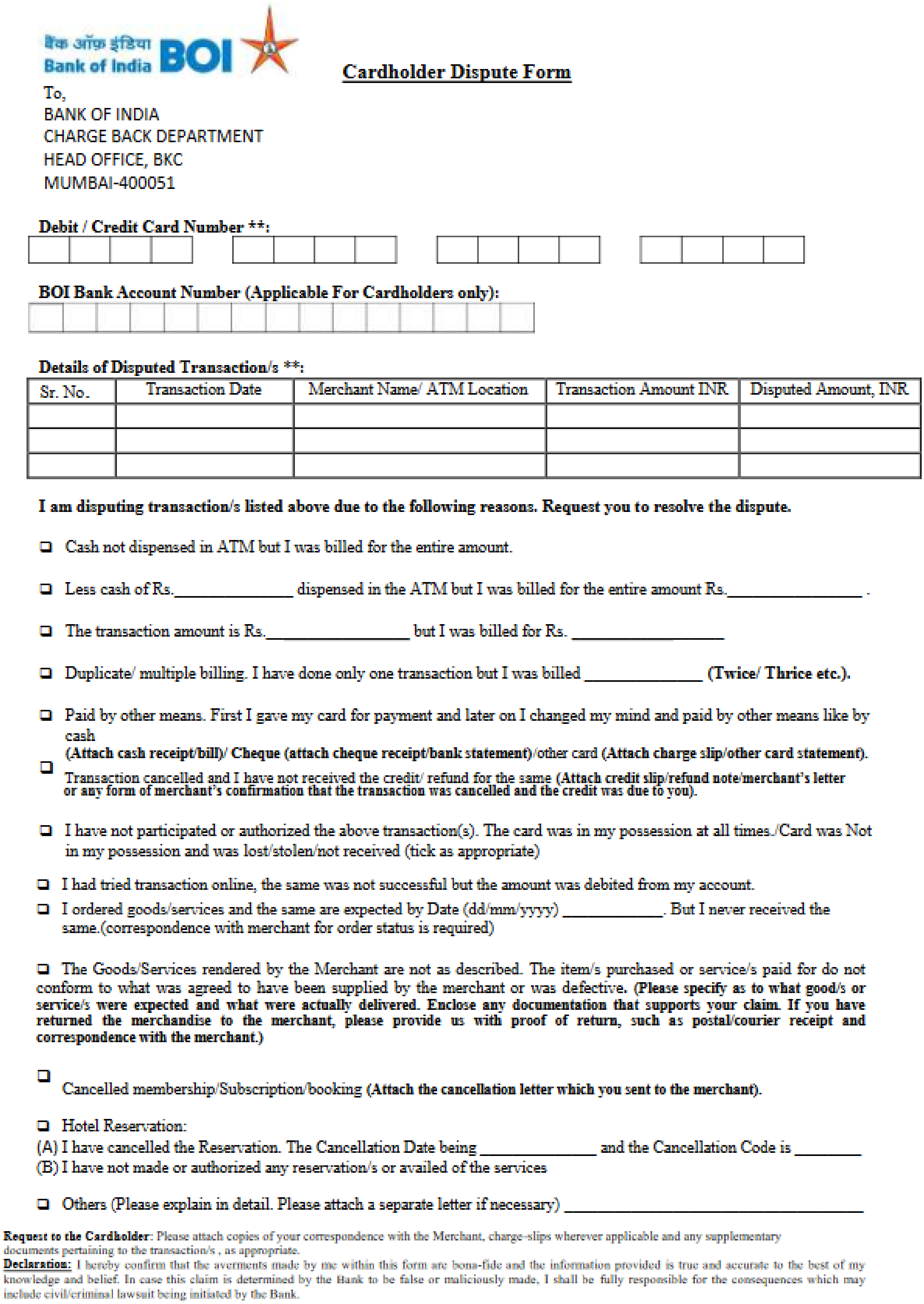
For chargeback Rejection Report of Debit card (CWDR / MEDR) –
HO ATM Cell
Contact no- 022-61319468, 9488, 9461, and 9487
Email Id: HO.ATMCell@bankofindia.co.in
For BDIPG txn – Internet banking dept.
Contact No - 022-61312988, 2990, 2991, 7501
Email Id: HO.InternetBanking@bankofindia.co.in

Chargeback rejection report of credit card (Master card)-022-61312934
Email Id: HeadOffice.Masterchargeback@bankofindia.co.in

Charge back rejection report of credit card (Visa card) – 022-61312935
Email ID: HeadOffice.Visachargeback@bankofindia.co.in

Charge back rejection report of credit card (RuPay card) – 022-61312942
Email ID: HeadOffice.rupaychargeback@bankofindia.co.in

Address where insurance claim document to be sent:
➔BOI Head office, Card product dept., Star House -2, 1st floor, C-4, G-Block, Bandra Kurla complex, Bandra (E), Mumbai-400051.



बैंक ऑफ इंडिया Bank of India BOI

Cardholder Dispute Form

To,
BANK OF INDIA
CHARGE BACK DEPARTMENT
HEAD OFFICE, BKC
MUMBAI-400051

Debit / Credit Card Number **:

□□□□ □□□□ □□□□ □□□□

BOI Bank Account Number (Applicable For Cardholders only):

□□□□□□□□□□□□□□□

Details of Disputed Transaction/s **:

Sr. No.	Transaction Date	Merchant Name/ ATM Location	Transaction Amount INR	Disputed Amount, INR

I am disputing transaction/s listed above due to the following reasons. Request you to resolve the dispute.

❑ Cash not dispensed in ATM but I was billed for the entire amount.

❑ Less cash of Rs.______________ dispensed in the ATM but I was billed for the entire amount Rs.________________ .

❑ The transaction amount is Rs.________________ but I was billed for Rs. ________________

❑ Duplicate/ multiple billing. I have done only one transaction but I was billed ______________ **(Twice/ Thrice etc.).**

❑ Paid by other means. First I gave my card for payment and later on I changed my mind and paid by other means like by cash **(Attach cash receipt/bill)/ Cheque (attach cheque receipt/bank statement)**/other card **(Attach charge slip/other card statement).**

❑ Transaction cancelled and I have not received the credit/ refund for the same **(Attach credit slip/refund note/merchant's letter or any form of merchant's confirmation that the transaction was cancelled and the credit was due to you).**

❑ I have not participated or authorized the above transaction(s). The card was in my possession at all times./Card was Not in my possession and was lost/stolen/not received (tick as appropriate)

❑ I had tried transaction online, the same was not successful but the amount was debited from my account.

❑ I ordered goods/services and the same are expected by Date (dd/mm/yyyy) ____________. But I never received the same.(correspondence with merchant for order status is required)

❑ The Goods/Services rendered by the Merchant are not as described. The item/s purchased or service/s paid for do not conform to what was agreed to have been supplied by the merchant or was defective. **(Please specify as to what good/s or service/s were expected and what were actually delivered. Enclose any documentation that supports your claim. If you have returned the merchandise to the merchant, please provide us with proof of return, such as postal/courier receipt and correspondence with the merchant.)**

❑ Cancelled membership/Subscription/booking **(Attach the cancellation letter which you sent to the merchant).**

❑ Hotel Reservation:
(A) I have cancelled the Reservation. The Cancellation Date being ______________ and the Cancellation Code is ________
(B) I have not made or authorized any reservation/s or availed of the services

❑ Others (Please explain in detail. Please attach a separate letter if necessary) ______________________________

Request to the Cardholder: Please attach copies of your correspondence with the Merchant, charge-slips wherever applicable and any supplementary documents pertaining to the transaction/s , as appropriate.

Declaration: I hereby confirm that the averments made by me within this form are bona-fide and the information provided is true and accurate to the best of my knowledge and belief. In case this claim is determined by the Bank to be false or maliciously made, I shall be fully responsible for the consequences which may include civil/criminal lawsuit being initiated by the Bank.

Cardholder's Name:_________________________________ Place: ________________________

Signature: X____ Date: ________________________

Email:______________________________@_____________ Phone: ________________________

Supporting Checklist

INSURANCE CLAIM DOCUMENT CHECKLIST-		
SR. NO.-	RECEIVED DATE-	
NAME OF CLAIMAINT-		
CARD NO		
DATE & NATURE OF TRANSACTIONS /LOSS (MEDR/CWDR/BDIPG)		
CLAIM AMOUNT (RS)		
BRANCH NAME / ZONE		
LINK SB A/C NO-		
DOCUMENT REQUIRED	**AVAILABLE**	Additional Information about the Documents (for Branch clarification)
1. INSURANCE CLAIM FORWARDING LETTER	YES / NO	Contained in attachment
2. CLAIM FORM	YES / NO	Contained in attachment
3. CLAIM VOUCHER	YES / NO	Contained in attachment
4. LETTER OF SUBROGATION	YES / NO	Contained in attachment
5. INVESTIGATION REPORT BY BRANCH	YES / NO	Contained in attachment
6. SMS DELIVERY REPORT	YES / NO	Contained in attachment
7. INITIAL INTIMATION BY CARD HOLDER	YES / NO	Written request from Customer to branch
8. POLICE COMPLAIN / FIR COPY / FINAL REPORT	YES / NO	To be received from Customer police complain upto Rs 50000/-, FIR with police above 50000/- Police final report above one lac required.
9. CHARGE BACK REJECTION REPORT	YES / NO	FOR CWDR / MEDR TXN - BY HO ATM CELL, FOR BDIPG TXN- BY HO INTERNET BANKING DEPT.
10. HOTLISTING REPORT OF CARD	YES / NO	Sent Mail for debit card to - PSS.Hotcard@fisglobal.com
11 .PHOTO COPY OF HOTLISTED CARD	YES / NO	If Card is lost, only branch confirmation in investigation report will do.
12. ID PROOF OF CARD HOLDER	YES / NO	To be obtained from Card Holder
13. ACCOUNT STATEMENT	YES / NO	From CBS / Finacle.
Remarks, if any		

Address where insurance claim document to be sent:
BOI Head office, Card product dept., Star House -2, 1st floor
C-4, G-Block, Bandra Kurla complex, Bandra (E), Mumbai-400051

ATM/POS Online Refund - URLs

ATM Refund Claim
https://www.bankofindia.co.in/forms/AtmFailedTransaction

POS Refund Claim
https://www.bankofindia.co.in/forms/OnlinePOSTransaction

Online Bill Payments Refund Redressal
https://www.bankofindia.co.in/forms/RefundRedressal

Internet Banking – Key Features

	Retail Internet Banking	Corporate Internet Banking
Constitution	• Individuals • HUF • Sole Proprietor	• Non-individuals • Partnership • Trust • Private Ltd Companies • Public Ltd Companies • Society • Body Corporate
Trade Finance Facility	• No	• Yes

Retail Internet Banking Transaction Limits

Transaction Type	**Default Transaction Limit (Per transaction max. limit) in Rupees**	**Maximum Daily Transaction Limit in Rupees**
Tax Payments / Custom	25.00 lacs	No limit
NEFT	5.00 lacs	15.00 lacs
RTGS	15.00 lacs	25.00 lacs
Third Party Fund Transfer (within Bank of India account)	5.00 lacs	15.00 lacs
IMPS payments	2.00 lacs	15.00 lacs
Utility Bill Payments	5.00 lacs	5.00 lacs
Self-transfers	15.00 lacs	No limit

Corporate Internet Banking Transaction Limits

Transaction Type	**Default Transaction Limit (Per transaction max. limit) in Rupees**
Tax Payments	5 Crores
NEFT/RTGS	25.00 lacs
Third Party Fund Transfer (within Bank of India account)	25.00 lacs
Utility Bill Payments	10.00 lacs
Self-transfers	10.00 lacs

Bulk Upload RTGS / NEFT through Corporate Net Banking.

Corporate Internet Banking user can upload a file in pre-defined format and processes the transaction in bulk for RTGS / NEFT. This facility will be extended to all corporate internet banking users presently having the upload facility means Profile 'G' has to be extended.

The file may contain both types of transactions RTGS and NEFT in a single upload file, the system will identify the type of transactions (NEFT or RTGS) and accordingly the same will be sent to the related gateways.

The data of the file will be validated for correctness of the IFSC and debit account. The IFSC code will be verified with the details of IFSC code available in Internet Banking database.

The facility will also support multilevel workflow i.e. multiple approvals can also be defined for RTGS / NEFT Bulk Upload.

Using this module, the customer can initiate RTGS or NEFT payment without registering beneficiaries. This module also saves the customer from the hassle of managing hundreds of beneficiaries.

If the user is having multiple approvals for file upload facility, the same fund transfer rule will be replicated for RTGS / NEFT file upload by default and hence the existing users having file upload facility will be able to use this functionality immediately after the same is moved to production.

The module is having all Limits related features. There is also a facility to define a separate Monthly / Daily Transaction limit for RTGS and NEFT Upload Transactions.

The module will provide the status of uploaded file and about all the transactions of the file. The user will be able to generate status wise report – which can be saved / printed.

Process of uploading of RTGS / NEFT Bulk Upload File.

a. Corporate customer logs in to the corporate Internet Banking application using his Corporate ID, User ID and password. The RTGS / NEFT upload feature is placed inside the 'Upload' Menu option.
b. The customer clicks on the 'Upload a File' link in the file upload side menu. On this page the customer has to select the debit account and type of file. The customer has to enter the file name and description (for reference) and the total debit amount and click on the 'Browse' button to select the file from the 'Choose file' dialog box and click on 'Upload File' button.
c. Once the file content is successfully uploaded / received by the server, the new web page is displayed. Based on the total debit amount the workflow rules are also applied on the web page.
d. After successful validation of the workflow rules and validating the file contents, the new web page is displayed to the customer. On this page the details of the individual transactions mentioned in the uploaded file is displayed. The user has to verify all the details and enter the OTP sent on his registered mobile number and click on submit.
e. If the uploaded file fails in the validation checks then the customer is informed about the errors in the new web page instead of displaying the earlier page. All the errors caught in the validation checks are displayed to the customer. The customer has to rectify these errors and upload the file again.
f. Once the OTP is validated the customer has to enter his user ID and transaction password to submit the request.

g. The transaction password is validated and the cyber receipt page is displayed on successful authentication. On this page the customer is given the provision to save the cyber receipt in excel format, print or send a mail to his internal mailbox.
h. After the file is successfully uploaded, the system takes care of the rest of the procedure to process the file. The uploaded files are processed at certain pre-defined intervals. The customer can check the intermittent status by accessing the 'View File Status' link on the side menu. On this web page the collective status of the file is displayed.

StarToken NG

StarToken is the next generation Internet banking security solution that is being offered by Bank of India to all its Internet Banking customers (Retail as well as Corporate). StarToken works as a Two Factor Authentication (2FA) solution. StarToken facilitates the Internet banking users with an extra level of security while performing online banking operations. StarToken is powered by the next generation REL-ID technology and is the first of its kind which provides security against loss of funds due to theft of login credentials, phishing attacks and most of the malicious software on the computers. StarToken provides the most secure Internet Banking Environment to its users. With StarToken you do not need to use any 3rd party browsers for doing banking on Internet.

StarToken protects you from the problem of Internet Banking frauds that are on the rise every passing day. StarToken is for your overall Internet banking safety. Below are some reasons;

a. StarToken controls the loss due to you losing your Internet banking username and password.
b. StarToken protects you from the loss of your money (while performing Internet banking) due to various known Internet banking threats such as Man in the Middle, Man on the Machine and Man in the Browser.
c. If you are using StarToken, you are assured that you are connecting to authentic Bank of India website and not a phishing website.
d. If you are using StarToken, then Bank of India can distinguish between you and a thief on Internet, thereby protecting you – which is otherwise extremely difficult without StarToken.

Introduction of BBPS Branch Module to our Customer in Finacle

(BC: 113/33 Dated: 22.05.2019)

Bank has introduced Bharat Bill Payment (BBPS) module for utility bills payment, exclusively for our customers, which is to be linked to Bank's Finacle System through BBPS Branch Module using "**BBPS**" menu.

Following task can be performed using BBPS Branch Menu in Finacle-

- Recharge a DTH
- Pay
    - Electricity bill
    - Post-paid mobile
    - Water
    - Gas
    - Post-paid landline
    - Post-paid broadband bills

    Etc… gradually more categories would be covered under BBPS

The major benefits of enabling Bank of India's customers to use BBPS Menu are –

- Customer can pay utility bills by visiting the nearby branch and thus avoid long queues.
- BBPS Menu offers our customers an additional platform to make utility bill payments.
- As this is a part of Finacle, the said module can be to effect bill payments PAN India at any of the Branches.
- Bank will earn revenue for every transaction done using BBPS Menu.
- CASA account will increase.

Non-delivery of Personalized Cheque book -

Intimation to customers through SMS on registered mobile no.

(Circular Letter: 2019-20/120 Dated: 27.02.2020)

Non-delivery of Cheque Books is a matter of great concern as this invites unnecessary customer dissatisfaction, grievances and complaints. This is also matter of concern as Branches are expected to devote precious time by handling such cases and attempting multiple calls to individual customers for advising them and requesting for collection from Branch. It is observed that at times undelivered cheque books are lying in Branches unnoticed for a longer period whereas customers are facing lots of challenges for non-receipt / late delivery of cheque books.

To overcome the present challenges and to ease out the process, new menu **"DLVSMS"** have been developed in **Finacle** system. Branches are advised/ expected to capture necessary information/details through the menu for undelivered cheque books as and when the same is received undelivered at branches. On verification of entry through the same menu, system generated automatic SMS will be sent to the Customer's registered mobile number, advising/informing them to collect their cheque book from the branch.

Upon receiving message as above, whenever customer approaches branch for collection of said cheque book, Branches must ensure to correct their latest communication address and update the system immediately in order to avoid late/ non-delivery of cheque books to their communication address in future. This will save precious time of Branches, improve customer service and at the same time latest information of customers will be available in FINACLE system.

SMS Based Requests/ Banking

Cheque Book Request

Circular Letter – **2015-16/71 dated 24.07.2015**

Facilities: For SB, CD, CC, OD account holder

Pre requisite: -

- In Finacle, "Mobile No." must be inserted in the appropriate filed in CUMM (with country code)
- In Finacle, Cheque Book allowed field should be "Y"
- Account must have required minimum balance
- Account must be "Active" and not "Dormant"
- Customer ID must me "KYC compliant"
- **1st request of cheque book must be through branch** by submitting the required "Requisite Slip"

- Customer can request for "n" number of cheque books using "N" number of SMS.
- Presently on SB account cheque is being deliver at "Communication Address" and for rest type of account it is delivered to concern branch.
- Postal Code (PIN) is mandatory for overseas address (for NRI customer); otherwise cheque book will be delivered to concern parent branch.

Format: -

CHBS<>15 Digit A/C No.<>ADR **(Delivery- Customer address)**
Send the message to **7669300024**
CHBS<>15 Digit A/C No.<>BR **(Delivery – Branch)**
Send the message to **7669300024**

NRI customer has to send his/her request by putting +91 before 7669300024. Thus, SMS is to be sent to **+917669300024**

[If request is not executed a message is send to customer – "Cheque Book Request is Unsuccessful"]

Auto Generation:

Finacle will identify accounts in which 75% of Cheque leaves are utilized, a request of personalized cheque book will be generated and the request will be in "V" (verified) status.
{A system generated SMS will be sent to the customer advising "You have utilized 75% of your cheques, we are processing your new cheque book which will be delivered at your branch/home within 8/10 working days"}

IMT related request

@ Adding IMT Beneficiary:
IMT Ben 10DigitMob.NO#Ben Name#Ben Add#Ben PIN Code
Send the above message to +919223009988
@ Delete Benf.:-
IMT BENC#Ben Mob No. => +919223009988

QSAM (Query Service on Aadhaar Mapper):

A common code *99*99# has been adopted for all TSPs. It is called QSAM (Query Service on aadhaar Mapper) that allows the users to check the Aadhaar seeding status in the bank account along with the last updated date.

Dial -*99*99#

a. Know Aadhar Link Status
b. PMJDY A/C Overdraft Status

Missed Call Balance Enquiry:

Missed Call Balance Enquiry –

For domestic customers -	1.	9015135135
	2.	9266135135
For NRI customers		+919015190202

SMS in Vernacular Language

Presently, our customers are being provided various financial and non-financial SMS alert messages only in English Language generated from various channels like FINACLE, IB, MB, UPI, ATM, POS, e-COM. There are request from Customers to consider providing such messages in their mother tongue for the benefit of Customers in general who are not comfortable with English or have limited knowledge of English language or take pride in using their mother tongue over English language. Our bank has considered their requested and adapting new process & feature through which customer would be in a position to receive such messages in their preferred language. Accordingly, enhancement in CBS have been made to accommodate customer preferred language. So far, following languages are enabled based on State code available in permanent address field in the customers master in Finacle as default preferred language for SMS alerts.

Since we are taking default preferred language based on permanent state code available in customer master, all customer by default will receive SMS in the language stated as above. However, we have provided facility to customers to change / choose other languages or go back to English as preferred language. To change SMS preferred language following options are available to customers/Branches.

A. Branch (Offline):

- Invoke menu option CUMM in CBS.
- Select Function 'M' and enter Cust_id and press F4
- Press F6 and go to last page of CUMM and modify the Free _Code_3 after selecting the language code from F2 menu.

B. SMS (Online):

- Customer may change preferred language by sending SMS using code "UATLANG" keyword and sent on to no. **7669300024** using their registered mobile number.
- As soon as they sent this code, customer will receive SMS which will provide details of preferential language code available to choose and format in which request has to be sent.
- Customer will text/message the preference language code in prescribed format (i.e. <language_code><space><cust_id>) on long code 7669300024
- On successful completion of process, customer will get the status through SMS on his/her registered mobile number.
- Kindly advise the customer that maximum limit for changing SMS vernacular language using SMS mode is 2 times per day.

BOI Star Rewardz

BOI Star Rewardz is Bank of India's Credit/Debit Card loyalty program. Every time you use your Credit/Debit Card for shopping or making payments, you earn StarPoints which can be redeemed to get products & services for free.

Objectives of the programme

The main objectives of the BOI Star Rewardz Loyalty Programme for Credit & Debit Cards are: -

- To increase the transaction counts and purchases on POS and e-Commerce.
- To introduce a wide portfolio of redemption options to the customers.
- To generate additional revenue for the bank in the form of interchange.
- To increase customer base using BOI Credit cards.
- And to encourage our existing customers for cash less transactions.

On BOI Star Rewardz app you can

- Track your StarPoints
- Redeem them to get clothes, utilities, jewellery, kitchenware, electronics & more for free
- Redeem Points for free mobile/DTH recharge
- Use Points to get free movie tickets
- Redeem Points on the spot at any store using mPoint
- Locate Max Get More partner stores to earn upto 5X Points

Earn Reward Points

Always shop using your Bank of India Credit/Debit Card & earn StarPoints. These are equal to cash & can be redeemed to get anything for free. Shop at Max Get More partner stores to earn Points faster.

Redeem your Reward Points anywhere using mPoint

With this new feature, your redemption options are unlimited. You can redeem your Points at any store of your choice for any shopping - at your local grocery store, medical store, restaurant, general store & more.

All you need to do is generate an mPoint QR Code for the amount you want to redeem on your BOI STAR REWARDZ app. Show it to the shopkeeper/cashier who will scan it on his smartphone using mPoint Business app. The amount is directly transferred into his/her bank account and your StarPoints are redeemed against the product/service.

In case of insufficient point balance, you can pay the remaining amount using your debit/credit card to generate mPoint for the required value.

You can also redeem your StarPoints on app & choose from over 10,000 products in our product catalogue, book movie tickets for free & get mobile/DTH recharge for free.

Debit Card – Points:

To be able to start redeeming Bank's Credit Card customers will need to achieve a threshold of 100 Points.

Points need to be redeemed within three years (36 months excluding the month of accrual) of accruing them. Unredeemed Points will expire at the end of 36 months.

Slabs	Amount Spent Per Month	Points per Rs. 100/- spent Per Month
Slab 1	Upto Rs. 5,000/-	1 Point
Slab 2	From Rs. 5,001/- to Rs. 10,000/-	1.5 Points
Slab 3	Rs. 10,001/- and above	2 Points

(1 Star Point = Rs.0.25/-)

50% MORE Star Points (Loyalty Reward Points) to Sangini Debit Card Holders. You get 1.5 Points in place of 1 Point for every Rs.100 spent, for every card usage at POS/e-commerce transactions.

Credit Card - Points

To be able to start redeeming Bank's Debit Card customers will need to achieve a threshold of 100 Points.

Points need to be redeemed within three years (36 months excluding the month of accrual) of accruing them. Unredeemed Points will expire at the end of 36 months.

2 Star Points for every Rs.100/- spent
1 additional Star point for every Rs.100/- – for purchases on preferred category.
(1 Star Point = Rs.0.25/-)

PoS & M-PoS

EDC/POS/MPOS/Bharat QR/BhimAadhar Familiarization

- For Merchant Acquisition Business
- Bank is installing Electronic Data Capture (EDC) machine or Point of Sale (POS) terminal(s)/, QR Codes, Bharat QR Code, BhimAadhar pay system at merchant's outlet(s).

Merchant Category (as per RBI)

1. **Small merchants** (with turnover up to Rs.20 Lakhs during the previous financial year)
2. **Other merchants** (with turnover above Rs.20 Lakhs during the previous financial year)

Eligibility:

- Operative Account (Saving/Current Overdraft/Cash Credit) Holder of the Bank for at least 6(six) months.
- The conduct of the account should be satisfactory.
- The requirement of six-month satisfactory conducted account may be diluted in the following circumstances:
    - Other Group accounts being more than 6 months old. 2. The Bank has sanctioned the ME business loan. 3. In case of reputed / well known canvassed accounts. (Satisfactory conduct of 2 years of a/c in any Public/ private Bank)
- Merchants having business in Jewelry, Diamonds, Handicrafts, Carpets should be done only when their credentials, creditworthiness, integrity are well established through enhanced due diligence.
- Any deviation in eligibility criteria listed above should be specifically approved by an authority not lower than the **Zonal Manager.**

Not Eligible Merchant

1. Fire arms, Hazardous materials
2. Fake/banned/illegal Goods and services
3. Regulated goods for which authorization is not obtained
4. Fake/banned Drugs and unlicensed Medical Practitioner, Illegal tests
5. Trading of Live/endangered Animals/species, body parts
6. Activities involving copyright violation
7. Adult goods and services
8. Gambling and Gaming
9. Hacking, Cracking, Cheating and Forgery
10. Offensive/Crime Goods
11. Currency, Exchanges and Financial Products and Services
12. Foreign Contributions, Political Funding, Hawala Transactions

Document Required:

- Financial Documents of the Merchant
- If the merchant is corporate Audited Financial statements for last three years is required.
- Limit for audited financial statement shall be applied as per relevant statute;
- Financial documents shall include 6 months bank statement, ITR filed or Audited Balance sheet.

Documents are submitted by Merchant

- Application in the prescribed format has to be complete in all respect and signed.
- Photograph (individuals & authorized personnel.
- Know Your Customer Document, including Proof of Identity and Proof of Address for Merchant.

➢ If merchant is already enrolled by another institution, status report from the institution/banker shall be obtained. ➢ **CIBIL/ Credit Bureau report for the business entity and its partners/ directors/ promoters / proprietors/ authorized signatories shall be generated and should be acceptable to the Bank. Report should not contain any overdue or legal action for recovery of dues/ written-off accounts. If the issues are technical or the details are not updated, based on available documentary evidence, the sanctioning authority may relax the condition by incorporating full details in the proposal.**	✓ Permanent Account Number (PAN) ✓ GST Registration number. In case of small merchants, who do not have registration number/ license, the copy of Aadhaar/ PAN should be obtained ✓ Merchant should submit all principal financial statements like audited balance sheets, Income / Wealth Tax returns etc. for past 3 years. If new in business, then the personal IT / Wealth Tax returns of the promoters, for previous years. ✓ **If the applicant is Corporate:** ➢ UIN Number ➢ Certificate of Registration / Incorporation, ➢ Certificate of Commencement of Business ➢ Memorandum & Articles of Association and Board Resolution (In case of Company) / Authorization (in other cases). ➢ Personal details of the authorized signatories.
Inspection of Merchants (Once in quarter) Merchant Business verified and recorded in inspection report/endorsement in application. **Type of location:** To Determine the type of location of the merchant, such as storefront, indoor shopping mall, or office etc. **Time of location:** Period for which the business has operated at the present location. **Type of Activity:** Business activity, as mentioned in the application, should be visible at the location. The expected turnover must also be in line with the business activity. **Market Report:** Market report of the Merchant shall be taken.	**Due Diligence:** ⇨ Proper due diligence shall be done while processing the request of Merchant. ⇨ The entity should be a legal entity recognized by law, in cases other than individuals. ⇨ The ME should be well established in the business and should be in business for a reasonable period – at least six months. In case of new accounts, whether canvassed or not, ⇨ There should be no adverse market reports. ⇨ If the business premises as well as residence of the proponents, both, are rented, the proponent should be residing in that place for at least 2 years or more.

All document of Merchants keeps in record along with, ME Enrolment Report, Records of MID & TID and ME Do's & Don'ts

Cost-Benefit Analysis -> Analysis before Approval **->** Analysis on Annual Basis

⇨ For carrying out annual analysis, the historical trend of last one year, shorter if installed within the year, shall be taken into account.

⇨ It shall be the responsibility of the Branch head to ensure that Annual Review is done. Approval/decision of Zonal Manager shall be obtained and kept on record within 3 months of expiry of one year, failing which the concessional rates may be withdrawn by Head Office.

Bulk Terminals

Merchants having more than 5 terminals, endeavor should be made to obtain security deposits for the 3 years rental of all terminals in the form of TDR/ Bank Guarantee etc. and lock in period of terminal should be 36 months. In deserving cases, relaxation may be approved by General Manager, National Baking Group / Head Office.

Rent

Vendor - M/S Worldline (ATOS)

Terminal type	**Monthly Rent**	
GPRS	975 + GST	Printed Slip
PSTN	520 + GST	Landline Phone with STD connection
Paytivo 6210	350 + GST	Only e-charge slip not printed slip
Paytivo 7210	975 + GST	Printed Slip

Vendor - M/S Indiatransact Services Ltd (ONGO)

GPRS	349 + GST	749 + GST one-time installation charges
MPOS	249 + GST	349 + GST one-time installation charges Smart Phone with Internet Connection

Vendor M/S Synergistic Financial Pvt Ltd (Mosambee) through Worldline

MPOS	250 + GST	Smart Phone with Internet Connection	

M/S Plutus Plus solutions (M/s Pine Labs) through Wordline

Model	Multiple acquiring	Sole acquiring
ICT 220 Pine EDC (Internet connectivity)	320 + GST	570+GST
DGPRS (Desktop GPRS) Pine EDC (Including GPRS SIM)	320 + GST	670+GST
GPRS (Handheld) Pine EDC (Including GPRS SIM)	320 + GST	975+GST

Bharat QR

QR code	60 + GST	200 + GST one-time installation charges

BHIM Aadhar

Biometric Device	0	2065 + GST Installation Charges

- **Rent Borne by Bank – Charges through Zone SUS071**
- **PL a/c for EDC/POS Machine Rent is PLOE096**
- **Close, Invalid/ Freeze etc a/c Rent Charged by respective Branch SUS073, and it will be recovered from merchant only.**
- **Before De-installing the terminal/ Close the account, all pending rent should be recovered.**

MDR (Merchant Discount Rate)

The merchant discount rate is the rate charged to a merchant for payment processing services on debit and credit card transactions. (**This is the transaction fee, deducted per transaction**)

Debit Card				Credit Card
Transaction up to 2000 - NIL				➢ 1.75 to 2.00 % as per bank Sanction
Transaction above 2000	Small Merchant	0.40 +GST		
	other Merchant	0.90 +GST		

Sanction Authority	
Branches headed by Branch Managers up to Scale III **Deputy.** **Zonal Manager** Branches headed by Scale IV **Branch Head (Chief Manger)**	**Any deviations** in any eligibility norm/ MDR / Rent: **Zonal Manager only**
Only Bharat QR by Branch Manager	
Other Facility ⇨ **Cash @ POS also available in all active for Cash @ POS terminals with Incentive as per NPCI/RBI Guideline.** ⇨ **International Card activation facility also available.** ⇨ **Offline pre-authorization facility also available.** ⇨ **Merchant customization facility also available.**	
Review of Merchants: - Cost-Benefit Analysis, transaction -> Quarterly Charge Back, Fraud, Conduct of Merchants-> Annually Branches ensure yearly Review of Merchants are done by the branches Official	
For Installation	
Send Work order of Excel sheet with Sanction Memorandum to headoffice.CPDedc@bankofindia.co.in	
De-installation of terminal	
✓ Send email to respective vendor as per escalation matrix or headoffice.CPDedc@bankofindia.co.in with MID/TID and account number of Merchants. ✓ After de-installing pending rent will be recover on next months.	
Reference/ Circular: ➢ HO: CPD:PM:007 dated 28.02.2019 ➢ 110/181 dated 22.12.2016, ➢ 110/173 dated 08.12.2016, ➢ 110/125 dated 04.10.2013 ➢ 107/82 dated 01.08.2013 ➢ Ref: HO: CPD: Accts: IVN: BRANCH CIRCULAR NO. 98/20, Sub: General Instructions 2004-05/4, Date: 10.05.2004	

This is only for handy and quick reference based on latest circular/ Policy for Internal used only

<u>Introduction of menu option “EDCMSTR” for on boarding - PoS merchants through CBS</u>

(Pl. Refer Branch Circular Ref. HO:DBD:SS:2020-21, Dt. 21.12.2020)

Digital Banking Department is handling Merchant Acquiring Business (PoS) through two vendors M/s Worldline India Pvt Ltd and M/s India transact services Pvt Ltd.

Presently work order in respect of PoS is consolidated at Zonal Office level and is sent to Head Office through email. The request received at Head Office is then shared with the respective vendors for installation of the PoS terminal as requested by the merchant.

It has been observed that the data which is being received at Head office is incomplete/incorrect/ missing. Further there are no checks and controls to ensure accuracy of the data submitted. This results in delayed installation of PoS terminals and a lot of complaints from branches and the customers.

In order to rectify the issues faced and to automate the process, BOI has now introduced a menu option "**EDCMSTR**" in **CBS** for onboarding of merchants. Branch user will invoke the menu **EDCMSTR** in CBS and the following options will be available.

Branches can now enter request for new PoS terminal through menu option "**EDCMSTR**" in CBS. Upon invoking the menu, following options will be available.

- REQUEST
- RECOMMEND
- CANCEL
- SANCTION
- INQUIRE
- MODIFY

Branches will receive on a T+1 basis, an auto email which will contain the detail of the PoS machine request sanctioned/approved by them. The customer will get an SMS once the PoS machine will be sanctioned on his/her mobile number.

Report option will be available in DR in MISRPT-OTHERS-EDCMSTR through which branches/zones can download the report for the records entered through EDCMSTR.

From 1st January, 2021 onwards fresh request for PoS terminals will be accepted through EDCMSTR menu only.

****

POS (POINT OF SALE TERMINAL) – Some important tips

- This actually refers to the machine or terminal which is used at a Point of Sale location for making payment. The payment is not by Cash but by using the Plastic money, i.e., using a Card issued by any Financial Institution. Be it a,
- Credit Card
- Debit Card
- Value Loaded Card i.e., Prepaid Card or
- Gift Card
- Thus, POS is a machine used to swipe a credit/debit/prepaid card so that the sale can be completed by parting with the goods against the value received through the swipe of the card.
- In other words, issuing of POS terminal actually refers to enrolling of a merchant by the Bank, for accepting payment by electronic means, i.e., by Cards.

- Apart from issuing of Cards (both Debit and Credit Cards) Bank has to enrol merchants also as this is another important activity which generates income for the Bank.
- Professionals like Doctors, Lawyers, Chartered Accountants also providing expert services for money. Thus, they are also doing business. Hence these professionals also are falling in the category of merchants. Hence, they can also be enrolled for accepting fees through cards for the services rendered by them.
- Buying and selling of goods or services is the core activity of any merchant

Who can be provided PoS

- Any merchant or businessman carrying on a legitimate business activity, by adhering to the rule of law and doing business to earn a living, is eligible to apply for a POS terminal.
- Similarly, a professional offering professional services for money is also eligible to be enrolled as a merchant.
- Customers of the Bank are enrolled for being our merchants. New Accounts canvassed by our Marketing staff can also be provided POS.

Types of PoS

At present our Bank is issuing 3 types of POS Terminal machines:

1. PSTN Terminals:

- These terminals require Landline Telephone connections.
- Through dial-up facility these are connected and the approvals are communicated. Fixed telephone connection is mandatory.

2. GPRS Terminals:

- These terminals do not need Landline telephones. These have a SIM Card and similar to mobile phones, these get connected through the SIMs

3. MPOS Terminals:

- These terminals are connected through Bluetooth with a Smartphone (Android) and the transactions are processed. The APP has to be downloaded from Play store.
- On the Smartphone and through the phone the device is connected to network.

Requirements for providing PoS

- The Merchant should have a legitimate business or commercial activity
- The Merchant should be operating a satisfactorily conducted Current/C.C. Account with the Bank for at least 6 months. In case the account is new the account and the POS usage should be monitored and if needed, corrective action to be taken immediately.
- The Merchant should have obtained a valid Licence for running the business or activity he is engaged in.
- The financial position should be satisfactory i.e. the merchant should be earning profit from the activity he is engaged in.
- Latest KYC Documents of the customer should be obtained and verified to the satisfaction of the Branch.

- CIBIL report to be generated by the Branch and the score should be satisfactory.

Cost Benefit Analysis – PoS:

- If the ME fulfils all the requirements as mentioned above, the Branch will now work out a cost benefit analysis based on the turnover of the merchant and the commission rate negotiated with the merchant.
- On the income side, the following parameters will be considered.
- Yield to the Bank, on the Deposits held by the merchant @6.7%
- Sale through Debit Cards – Commission @ 0.75% for value <2000
- Sale through Debit Cards – Commission @ 1.00% for value >2000
- Sale through Credit Cards – Commission @ the negotiated rate
- Rent of the POS Terminal (If ME has agreed to pay the same
- On the expenses side, the following items will be borne by the Bank
- Commission @ .8% to be paid to Visa/MasterCard on all debit card transactions
- Commission @ 1.45% to be paid on all credit card transactions
- Rent for the POS to be paid to the Service providers

Approval:

- Branch has to submit the recommendations to the competent authority and request approval for issuing POS to the merchant.
- While submitting the proposal, Branch will bring forth the following facts:

  a) The account is conducted satisfactorily
  b) The proprietor/Partner(s)/Company has obtained Licence for running the business
  c) The ME has submitted the KYC documents and also the fact that the business premises owned/rented by the proponent
  d) The cost benefit analysis is showing profit or loss

- If there is no deviation from the norms, Chief Manager and above can approve enrolment of ME. However, if there is any deviation, then Zonal Manager is the only competent authority for enrolling merchant

What is M-POS (Mobile POS Terminal)

An M-POS (Mobile point of sale) is a smartphone, tablet or dedicated wireless device that performs the functions of an electronic point of sale terminal. With m-POS one can harness the power of a smartphone, tablet or other mobile device to accept payments on the spot.

Presently two variants of M-POS are being launched

1. App Based
2. M-Swipe

The App based M-POS will be available in two variants

a) Mosambee
b) Ongo Merchant

In the app-based M-POS there is a requirement of a smartphone or tablet on which the app is downloaded and paired via Bluetooth of the smartphone or tablet with the M-POS device.

M-Swipe variant of the M-POS is a standalone device and there is no requirement of smartphone or tablet for carrying out the transaction.

Key Features of M-POS

- Suits small business men and merchants: From individuals offering professional services to small to small and medium business set ups – M-POS is a perfect payment solution. Smaller merchants cannot afford to use traditional POS due to various reasons, but with M-POS all they need is a smartphone with internet access. M-POS eliminates the requirement of a fixed line, hassles of applying and maintaining POS from banks; thus saving merchants time and money.
- Cheaper as compared to conventional POS machine: Compared to a regular POS, MPOS comes with a much lesser monthly maintenance cost.
- Convenient to use: M-POS is a convenient option as employees can meet consumers on the floor, help them check out without standing in line, and aid them in their decision-making process without risk of consumers opting for their phones as an aid.

Rental: Mosambee and M-Swipe machines will be provided by existing vendor M/S Worldline @ monthly rental of Rs.350/- per terminal.

Ongo merchant M-POS will be provided by M/S India Transact Services Limited. In this model there will be a onetime set up fee of Rs.749/- per M-POS terminal and monthly rental of Rs.349/- per terminal.

Government of India has advised to charge Rs.100/- only as rental per month on POS (Conventional/MPOS) to incentivise the merchants to use POS and promote cashless banking. Zonal Managers are competent authority to take a view on it on a case to case basis. It is suggested to charge Rs.100/- for first three months from the date of boarding till 31.03.2017(Branch Circular No.110/181 dated 22.12.2016).

Merchant Discount Rate: In the normal POS terminal installations, for Debit cards the MDR is as per the RBI guidelines (waived till 31.12.2016) and for Credit cards we are charging @ 1.65% or as per sanction of Zonal Manager. The same MDR rate shall be applicable for M-Swipe and Mosambee model whereas for the Ongo model, it being an Aggregator model, the vendor shall be charging us MDR as under, in lieu of end to end management with all expenses attributed to the vendor:

a) Debit as per RBI guidelines
b) Credit Cards–Standard (1.4%), Premium (1.95%) & Super Premium (2.20%)
c) Credit Cards-International Cards (2.50%).

BOI Mobile Functionalities

BOI Mobile is a Bank of India Mobile Banking Application for Retail Banking Customers. "BOI Mobile" app was launched on 1st August 2018. It allows you to bank anytime, anywhere through your mobile phone. You can access your banking information and make transactions in your Operative Accounts at absolutely free.

It's completely safe. All the details entered in app will be encrypted end-to-end across all networks. It's available in Google play store and apple store.

BOI customer can enrol themselves for mobile banking application by downloading the app from respective play store/App Store.

There are two types of Users.

1. View User
2. Financial user.

View users can view his account Balance, Account Details, Mini Statement and M-Passbook

Financial users can perform all type of fund transfer related transactions including bill payments.

Customer can convert himself from view user to financial user by using his debit card credentials. This option will be available under settings menu.

Various functionalities are as follows: -

1. Registration as View User/Financial User
2. Change Transaction Password
3. Forgot Transaction Password
4. Change Login PIN
5. Forgot Login PIN
6. Multiple Languages (presently 12 languages)
7. Locator
8. Contact Us
9. FAQ
10. Card Control
    a) Debit Card Services
    b) Credit Card Services
11. Balance Enquiry
12. Mini Statement
13. View Account Details

14. Positive Pay Systen

15. Generate MMID

16. View MMID

17. Loan statement

18. Loan Interest certificate

19. View Nominee details of Deposit Account

20. Term Deposit and Recurring Deposit opening

21. Pre closure of Deposit Account and Recurring accounts opened through Mobile Banking

22. Interest Rate Chart

23. Passbook

- a) Date wise
- b) Last Month, 3 Months, 6 Months and 1 year
- c) Last number of transactions
- d) Last number of Days

24. Request for Account Statement through Mail and PDF

25. Fund Transfer

- a) Self-Account
- b) Third Party
- c) IMPS – P2A (Account number & IFSC) & P2P (Mobile number & MMID)
- d) NEFT
- e) RTGS

26. BBPS Bill Payment

27. Adding biller as Favorite

28. Bill Payment History viewing

29. Beneficiary management for fund transfer

- a) Beneficiary Addition
- b) Beneficiary Deletion
- c) Make Beneficiary as Favourites

30. Opening and viewing Government schemes

- a) Pradhan Mantri Jeevan Jyoti Bima Yojana - PMJJBY
- b) Pradhan Mantri Suraksha Bima Yojana - PMSBY

31. Retrieval of Transactions

32. Request for Cheque book

33. Stop Cheque payment

34. Enquire Cheque Status

35. De-registration of User-ID

36. Transaction Limit Management for all Financial Transaction

37. Customer Profile

38. Refer a Friend

39. OTP Auto Fetch

40. Notification for Transactions

BOI Mobile Banking App Pre-Login FAQs

Introduction

- What is BOI Mobile?
  BOI Mobile is a Bank of India Mobile Banking Application for Retail Banking Customers. It allows you to bank anytime, anywhere through your mobile phone. You can access your banking information and make transactions in your Operative Accounts at absolutely free.

- Other Bank Customer can use BOI Mobile?
  No. Currently it's only available for BOI customers.

- BOI Mobile is safe to use?
  Yes, it's completely safe. All the details entered in app will be encrypted end-to-end across all networks.

- How to Download the App?
  It's available in Google play store and apple store.

- Which OS version does this app support?
  Any version of Android above 5.0.2 and iOS version 8.0 above is supported by the Application.

Registration

- How to register with BOI Mobile?
  BOI customer can enroll themselves for mobile banking application by downloading the app from respective play store/App Store.

- What are the type of users?
  There are two types of Users. View User and Financial user.

- What is view user?
  View users can view his account Balance, Account Details, Mini Statement and M-Passbook.

- What is Financial user?
  Financial users can perform all type of fund transfer related transactions including bill payments.

- How to convert from view user to financial user?
  Customer can convert himself from view user to financial user by using his debit card credentials. This option will be available under settings menu.

- If I don't have card how to convert from view user to financial user?
  You can approach your parent Branch for Debit card facility to avail the facility of financial user.

- I am getting a prompt "Sending SMS from your mobile failed" while registration. What should I do?
  Please check your mobile balance and network connectivity. Please reach us on 1800 220 229for further assistance.

Existing User
Re-Installation for existing users.

- ❖ Can I change my mobile device?
  Yes, you can change your mobile. Please download and install the app from the play store/App Store.

- ❖ Do I have to follow the registration process for new device?
  No, it's not required Just re-activate by clicking proceed button in the first page.

- ❖ Whether the registered SIM is mandatory for reactivation?
  Yes, Registered SIM is mandatory for new device.

- ❖ I have changed my mobile number at branch but can I still use the BOI mobile app?
  Yes, Mobile application will ask for the update.

Accessibility
Login

- ❖ What are the various credentials used for Login?
  You can use your user id / mobile number / customer id and Login PIN.

- ❖ How many times can I try with wrong login PIN?
  Maximum 3 times per day.

- ❖ If my user id is locked then how to release it?
  You have to wait for 24 hours to auto release or approach the bank for reset.

Forgot User ID

- ❖ What is Forgot User ID?
  If you have forgotten your User ID this option will be used to retrieve the User ID from server.

- ❖ What are the inputs do I need to give to retrieve the user id?
  If you are view only user you need to provide OTP. If you are transaction user you need to provide OTP and Transactions Password

- ❖ If I have forgotten transactions password or transaction password is expired how do I reset?
  If you have forgotten transactions password or if password has expired then use Forgot Transactions Password link to reset the Transactions Password.

Forgot Login PIN

- ❖ What is Forgot Login PIN?
  If you forget your Login PIN then use this option to reset the Login PIN.

- ❖ What are the inputs I need to give to reset the Login PIN?
  View user can reset the pin with OTP facility and financial user needs to provide OTP and Transaction Password.

BOI Mobile Banking App Post Login FAQs

My Account

Operative Accounts

- What are the accounts that will be showed under operative account?
  All the Savings, Current and Overdraft account will be displayed under operative account.

- How can I view Mini Statement or spending pattern of particular Operative account?
  You may click a particular account to view mini statement and spending pattern.

- Can I initiate fund transfer from my operative account?
  Yes, Fund Transfer facility is available

- Which type of Joint Accounts will be shown under My Accounts?
  Accounts having or either or Survivor/ Former or Survivor will be available under my account.

Loan Accounts

- Can I see all my loan account along with outstanding amount?
  Yes

- Can I see summary or statement of a particular loan account?
  Yes

- Can I download loan interest certificate of loan account?
  Yes, you can download the loan interest certificate in PDF format up to Last 10 years.

Deposit Accounts

- Can I see all my deposit account along with current balance?
  Yes

- Can I see summary of deposit accounts?
  Yes

- Can I open new deposit account?
- Yes

mPassBook

- What is mPASSBOOK?
  mPASSBOOK or mobile passbook is yet another innovative offering from Bank of India. This is an electronic passbook which can be used for generating your statement of a/c.

- Can I download the statement?
  Yes, you can download the statement in PDF format in mobile.

- Can I send email of my statement?
  Yes, you can send email statement of your account on your email id register with bank.

Favourite Transaction

- ❖ What is Favourites?
  Favourite option is used to save the successful transaction beneficiary as a favourite one. You need not to enter the details again for further transactions for the same Beneficiary.

- ❖ Can I delete the favourites?
  Yes, it can be deleted by swiping the left side of the displayed favourite Beneficiary nick name.

- ❖ Can I view the favourites?
  Yes, details can be viewed by swiping the left side of the displayed favourite Beneficiary nick name.

- ❖ Can I modify the favourites?
  No

Service Request

Cheque book request

- ❖ Can I apply for cheque book request in mobile app?
  Yes
- ❖ How many leaves of cheque book can I apply?
  For current account 50 leaves and for savings account 25 leaves.

- ❖ Can I receive the cheque book delivery to my registered address?
  Yes, it can be delivered to the registered address.

Cheque status

- ❖ How can I view my cheques status?
  You can view the cheque status by entering the cheque number or by viewing all cheques status after a particular date.

- ❖ What are the various type of cheque status that are available?
  The cheques status displayed are
  1. Un-used
  2. Passed
  3. Stopped

Stop cheque

- ❖ What type of cheque can I stop?
  You can stop cheques that are not regularized.

Settings

Transaction Limit

- ❖ What is Transaction Limit?
  Transaction Limit is the maximum amount which a user can transact for a specific period i.e. Transaction limit facility is provided to restrict the quantum of amount needs to be transact through Mobile application.
- ❖ Can I set daily, weekly and monthly transaction limit?
  Yes.
- ❖ For Which transaction type can I set Transaction Limit?
  Transaction limit can be set for
  1. Self-account Transfer

2. Third party transfer
3. NEFT
4. RTGS
5. IMPS (Account No + IFSC)/ (MMID + Mobile)

- ❖ What is the minimum and maximum transaction limit?

Sr. No.	Transaction Type	Per Transaction	Daily Limit
1	Self-Link	50,000	2,00,000
2	Third Party	25,000	1,00,000
3	IMPS	25,000	1,00,000
4	NEFT	25,000	1,00,000
5	RTGS	3,00,000	3,00,000

Change Login PIN

❖ What is Change Login PIN?
User can change his existing login pin using this option.

Change Transaction Password

❖ What is Change Transaction Password?
User can change his/her existing Transaction Password using this option

Forgot Transaction Password

❖ What is Forgot Transaction Password?
User can reset his/her Transaction Password using this option

De-register, Change of Mobile Number.

❖ What is De-register?
User can deregister himself from mobile banking application using this option and he will no more be a Mobile banking application user

Change Language

❖ What is Change Language?
User can change application language using this option.

Fund Transfer

Self-Account

❖ What is Self-Account fund transfer?
This feature allows user to transfer funds between their his/her own Bank of India accounts. Self-Link fund transfer is available among Saving, Current and Overdraft accounts. This facility is also available to NRE customers also.

❖ What are the conditions for Self-Transfer?
You can transfer funds between accounts having registered mobile number.

Third Party

❖ What is third party fund transfer?
This feature allows transfer of funds from your Account to another Bank of India Customers A/C.

❖ I am unable to transfer to Third Party with the error “Unable to process please try again later”.

Please verify beneficiary details. In case issue persists please contact us on 1800 220 229.

Unified Payments Interface (UPI)

Since its launch in 2016, UPI has grown exponentially at a CAGR of 414%, clocking 1,246 million transactions in March 2020. However due to COVID-19, UPI transactions declined by 20% to 999 million in April 2020. Since then, there's been a huge upswing in UPI transactions, with an all-time high of 1,800 million transactions having been recorded in September 2020. With new use cases around UPI and growth in person-to-merchant (P2M) transactions, we expect UPI to see continued growth in FY21–22.

As per industry sources, P2M transactions accounted for 40% of the total number of UPI transactions in the last financial year, and grew by almost 100% in the last six months.6 With many innovative P2M use cases in the market, we are expecting P2M to grow at a higher pace in the coming years – a trend that will be supported by the latest instructions from the regulators on B2B payments.

Growth in P2M use cases	Overall digital payment growth fuelled by UPI	Other growth drivers
1. Top players have already onboarded more than 20 million offline merchants. 2. Various new use cases like ASBA and AutoPay have emerged. 3. UPI has also been enabled as a payment mode for FASTag recharges, credit card outstanding payments, etc.	1. The digital payment user base is expected to reach 300 million by 2022. 2. UPI is the second largest payment mode in India. 3. UPI is giving tough competition to e-wallets for P2M payments. 4. NPCI is looking to expand UPI's reach to the international market.	1. As per the Government mandate, MDR will not be charged on UPI transactions for now. 2. There are various use cases under the Ministry of Finance's UPI 2.0 mandate for merchants with a revenue <INR 50 crore to offer UPI, UPI QR, RuPay and other digital payment modes.

UPI 2.0

UPI 2.0 is a new and updated version of the previous UPI. In this new version, users will get more new features which will make their experience more smooth, and some bugs have also been removed, and it's the better and advanced version of the previous interface.

UPI 2.0 Key Features & Benefits

Some of the most useful features have been launched with the UPI 2.0. Some of the new features of UPI 2.0 are overdraft account linking, enhanced transaction limit, invoice in the inbox, one-time mandate, signed intent and QR code and many more.

Transaction Limit Has Been Enhanced

This is also a great addition to the UPI 2.0 where the maximum transaction limit has been increased up to Rs 2 lakh. So, now you can transact more money without any hassle.

Over-Draft (OD) account as an underlying account in UPI

This feature lets you add your overdraft account to the main account. This option is very helpful when you need to give more than you have in your main bank account. Then you can use your overdraft account to spend the money. However, you can spend money from your overdraft account until a certain limit, but, overall, this feature is very helpful for users who use their current bank account on UPI.

For any OD accounts, whenever a customer needs to check balance of his OD account, customer's bank shall return 2 balances i.e. available & actual/usable balance. All UPI Apps need to display the same",

- UPI acts as a digital channel for accessing the OD account. On-boarding and registration processes for OD account remains same as the existing CASA accounts.

- Customer discovers/fetches the existing OD account and links to UPI for transaction.

- Customer has a choice to set new UPI ID/UPI Pin or use existing UPI ID/UPI Pin (used for current linked UPI account), as decided by his/her bank.

- A transaction to OD linked UPI ID would mean a repayment of OD by the customer.

- P2P & P2M transactions are allowed from a secured OD account. However, for unsecured OD accounts, only P2M transactions are permissible (excluding the categories prohibited by any regulator).

- Bank is responsible to get agreement on terms and conditions agreed with the customer.

- All existing UPI dispute management rules shall apply for the transactions.

- The OD providing bank must take the required consumer consent and make him aware about the terms and conditions of taking OD from the bank.

- The OD providing banks must communicate to the customer the due dates, outstanding amount, interest charges or any such information required at regular basis.

Note:
The customer account balances cannot be stored or used by PSP Bank or 3rd party app provider for any purpose as 'Customer Sensitive payment data'. Members may refer UPI circular no NPCI/UPI/OC No. 44/2017-18 dated January 11th 2018. This applies to UPI 2.0 equally.

Invoice in the Inbox Function (view attachment & pay)
Most of the users care about their money, and while transacting online, the majority of the users want to make sure that the transaction amount is set correctly. That's why National Payment Corporation of India (NCPI) has added this feature on the UPI 2.0. For this function, users will get an invoice in their UPI inbox before making the transaction where all the details about the transaction will be mentioned clearly so that the user can make sure the amount he or she is transferring is accurate.

(Using this feature customer can check/verify the invoice or attachment prior to authorizing the payment via a secure link received in the collect/intent message. To start with, the facility can be availed by verified merchants.)

- This creates a provision by which the merchants can share Invoices with customers before the transaction is authorized.

- This provision requires all UPI Apps to display an option -'Click on attachment to view details' or equivalent and open the same in a browser or equivalent display with the facility of 'Return' back to the main app, to the user.
- This option is feasible for collect, intent and OR code-based transactions.

- Transaction history details should also reflect the link under which the Invoice was presented and the same should be retained for at least 2 months by the merchant.

<u>One Time Mandate</u>
This is the most interesting and helpful feature for most of the users who love to shop online using cash on delivery as their payment method most of the time. This feature can be used on UPI 2.0 while you purchase any product or get any service like OLA etc. online.

Consumer can pre-authorize a transaction and block the funds in his account for a debit to be initiated later. UPI mandate can be used in a scenario where money is to be paid later after obtaining the service; however, the money in the account gets blocked instantaneously. The customer accounts shall get debited when the UPI mandate is executed by the merchant or payee. The mandate is digitally signed and stored at customer's account holding bank and also customer's PSP bank (app providing bank). During the debit the customer's account holding bank and customer's PSP bank need to validate the digital signature and verify the parameters.

- The mandate shall have key parameters such as "purpose code", "from & to date", "amount" & "frequency" (set to 'One time').

- Customer can authorize one time use mandates to different or same payee's at the same time.

- UPI mandate can be created by push or pull transactions i.e. QR, Intent, Collect or by create mandate option in UPI App. The mandate cannot be initiated by Payee for Person to Person (P2P) transaction.

- A UPI Mandate creation is fully authorized by the consumer by two factor authentications using 'what you know' (UPI Pin) and 'what you have' (Device binding).

- User/Merchant can Create, Modify or revoke the UPI Mandate as per defined rules. For some use cases the modification may not be allowed or allowed only up to specific date.

- UPI mandate can be executed up to the amount authorized by the consumer. Once executed and if partial, the remaining amount is returned to the customer's account. The customer's bank shall remove the block after expiry of the mandate.
- Till the time mandate is executed, the funds remain in blocked condition in customer's account and he/she continues to earn an interest depending on the type of underlying account.

- All existing UPI dispute management rules shall apply for the transactions.

- The notification to customer on both stages, i.e. block and mandate execution (debit) is mandatory.

- In case of revocation (wherever permissible), the block on the money should be released immediately reinstating the money to the customer's account. The revocation date should be prior to the execution date/ expiry date.

- The bank providing mandate with block functionality shall return 2 amounts on balance inquiry i.e. available and actual/usable balance or Sanctioned Limit and Drawing Power. All UPI Apps need to display the same.

If you pay using the One Time Mandate feature of the UPI 2.0, it will automatically block the amount on your account, but it won't be deducted until you get the product or service completely. This will prevent problems which comes when you pay online but don't get delivered to your address. If the order gets cancelled, the amount will also be unlocked from your UPI 2.0 account, and you will be able to reuse it.

Signed Intent And QR Code
This option let users use signed QR codes to accept payments online using UPI 2.0. This basically, makes sure that the merchant is trustworthy and verified. Then the payment will be made securely by scanning the signed QR code. This feature improves the connection between users and merchant and thus online transactions will be easier to use for the normal public.

Key Notes – UPI 2.0
UPI 2.0 was launched in 2018 with the aim of expanding UPI with more use cases. Invoice verification, linking of overdraft account, additional security through signed intent and QR are some of the features introduced in UPI 2.0. Apart from these features, a one-time mandate was also launched which can work as a post-dated cheque.

In July 2020, the NPCI extended this one-time mandate to a recurring mandate. Customers can now set a recurring mandate with UPI and pay mobile bills, electricity bills, loan EMIs, entertainment/OTT subscriptions, insurance premiums, mutual fund investments, transit fare, etc., up to INR 2,000 without PIN-based authentication. If the amount is more than INR 2,000, a PIN is required to execute every instalment/subscription.

Recurring payments can be a game changer in terms of UPI payment adoption and growth in India. This can provide a major push to the volumes and revenue for UPI players.

MDR (revenue)
The Government has mandated a zero MDR for all domestic UPI transactions, except some B2B, EMI, overdraft transactions, etc., to promote UPI payments in India. This move has impacted the revenue numbers for all major UPI players and hence, the revenue pool of UPI as a payment mode.

*****

UPI Related Queries - Guidelines to Branches

On daily basis we are receiving many queries from the branches on UPI related challenges/ issues/clarifications. Based on the queries received, we have identified few frequety asked questions and accordingly reproduce herewith some of them for the benefit of all the users to enable them to serve customers more effectively.

1- UPI transactions related inquiry
UPI system has been integrated with CBS for fetching information/data and passing financial transactions. Being standalone system, most of the information related to UPI transactions remains in UPI system and therefore, branches were facing challenges in guiding / advising Customers appropriately and were dependent on UPI team to provide information.

To overcome the challenges, new menu option **"HUPIINQ"** introduced in Finacle to inquire UPI related transactions. This will help branches to provide better & prompt customer service and resolve their grievances if any without delay.

However, please note importantly that entire process of identifying whether funds credited to beneficiary or reversal required to remitters for failed / timed out transactions is possible only after receiving the required information (after settlement) from NPCI which normally takes place on T+1 working day. Therefore, in normal condition UPI transaction inquiry will be available on T+ 2 basis (T is the date of transaction). The detailed procedure and functionality covered through menu option "HUPIINQ" provided in Annexure -2 which is attached with this document.

2- Customer is unable to on-board / Register in UPI

While customers are trying to on-board / registere themselves on UPI, there are few validaion availabe in CBS. Customers to be eligible for boarding on UPI, all the validations available must be passed successfully. Following validation available in CBS

I. Mobile Number used for on boarding must be present in Customer Master (CUMM).

II. Customers having scheme type SBA / CAA / ODA are eligible for on boarding on UPI.

III. Following Mode of Operation and constitution code are eligible for on boarding UPI:

S. No.	**Mode of Operation**	**Code**
1.	Self	001
2.	Either or Survivor	003
3.	Former or Survivor	004
4.	Anyone or Survivor	005
5.	Karta of HUF	011

S. No.	Constitution Code	Code
1.	Individual (Male)	41
2.	Individual (Female)	42
3.	Staff (Male)	43
4.	Staff (Female)	44
5.	Staff relatives(Male	47
6.	Staff relatives (Female)	48
7.	Proprietary Concerns	51
8.	Joint Family HUF	52

Branches are advised to check and ensure that all the above mentioned criteria met. It is observed that in most of the cases, which are referred to us, customers do not qualify on these validations. In such cases either branch can make necessary changes in Finacle or guide the customers suitably.

In case Customer is still facing challenge in on-boarding / registration, they may write to us for further clarification and support on support.mobileapps@bankofindia.co.in with subject line "Unable to on-board / register"

3- Customer facing challenges with invalid debit card details

There were complaints from the customers that though they are able to use ATM Card for cash withdrawal however the same card is not working while trying to register in UPI.

Looking to the issue, we have changed the entire process of card validation. Now we are validating card details directly from ATM Switch. Hence, none of the customers will face such challenge.

In case, customer still complains the same issue, branches may validate themselves and guide him/her appropriately.

4- Non-Receipt of funds by beneficiary or reversal by remitter for Timed out transactions

In case of any transaction failed / timed out, the amount is either required to be credited to the beneficiary or reversed back to remitter. However the entire process is possible only after receiving the required information (after settlement) from NPCI which normally takes place on T+1 working day (where T is the date of transaction)

Our team takes cognizance of NPCI reports for all such scenarios and passes entries to either beneficiary or remitter based on the fate of transaction.

So, if the failed / timed out transaction is of current day and is not reversed automatically, then branches are requested to advise the customer to wait for at least T+2 working days (i.e. settlement reports from NPCI is available to us and our team takes required corrective action) for the transactions to settle. For better understanding, a scenario with following example is provided:

Customer named XYZ, did UPI Transaction on 25th Jan 2019 (Friday) for Rs. 1,000/- and his account debited successfully, however, respective credit neither reflected to beneficiary account nor reversed to his / her account.

26th Jan being Public holiday and 27th Jan being Sunday, NPCI settlement reports would be available only on 28th Jan 2019 and corrective actions may be initiated only by EOD on 28th.

Referring to example given, if the amount doesn't reflected in beneficiary / remitter's account after end of next working day i.e. 28th Jan, write an email to Mobile Application Support - support.mobileapps@bankofindia.co.in with the subject- "UPI Amount not credited", we will suitably revert on that. Kindly provide the following details for early resolution of issues:

- UPI Reference Number (12 Digit no.)
- Date of transaction
- Amount transacted
- Remitting Bank
- Beneficiary Bank

5- Fund Transfer to wrong account

a) Where our Bank is beneficiary

Whenever our Bank's branch receives email / communication from customer or remitter bank / branch or from Head Office about wrong credit, branch has to confirm the same in Finacle. If wrong credit confirmed, branch has to immediately mark lien on that particular account for the amount mentioned. Lien in the account should be properly recorded and maintained at beneficiary branch.

In case of insufficient balance in the account, branches may mark the lien for the amount mentioned and may follow-up with the beneficiary customer for availability of funds.
Branches may also follow due diligence by taking consent from the customer for debiting their account for wrong amount. Branch needs to send the Signed Scan Copy with attachment of that written consent in email with Subject- "UPI funds Transfer in Wrong account".

Please importantly note that in such cases branches must insist for indemnity from remitter bank on bank's letter Head complete in all respects. Letter must be signed by Authorized signatory with Name, Designation & Branch seal. Sample indemnity form attached as per Annexure – 2. Thus, in case remitter bank directly approaches branch for reversal of amount, branches has to insist for indemnity letter. After receiving indemnity letter from remitter bank, branch has to write an email with attached scanned copy of indemnity letter with transaction details to support.mobileapps@bankofindia.co.in with subject: "UPI funds Transfer in Wrong account".

After following all Beneficiary Branch may debit beneficiary account and may return the amount to remiter Bank.

b) Where our Bank is remitter
In case of UPI transfer to wrong beneficiary account done by our customers, respective branch should send email to support.mobileapps@bankofindia.co.in with transaction details as

- UPI Reference no,
- Date of transaction,
- Amount,
- Beneficiary bank
- Remitter bank.

Branch should attach Indemnity Letter as per Annexure-2 on branch's letter Head complete in all respects. Letter must be signed by Authorized signatory with Name, Designation, P.F. Number & Branch seal. Branch must satisfy itself regarding genuineness of the reversal request of the customer and obtain proper application, if fault is on the part of customer.

We will forward the indemnity letter to beneficiary bank based on which they will initiate the process of recovering the amount from wrong beneficiary and reversal of amount to our Bank. Please importantly note that providing indeminity is not guarantee that funds will be revesed by beneficiary Bank, it depends on availability of funds in the account.

Please provide / share following Information to Customer to avoid recursive follow-ups:

- Beneficiary Bank may take up to 60 Days in accepting or rejecting our request based on Beneficiary bank policy.
- Reversal of funds depends upon the availability of funds in wrong beneficiary account.

- Advise customer to check the account statement for keeping track of the request.
- Advise the customer to follow up/contact with Beneficiary Bank/Branch to expedite the recovery.

6- Fraudulent UPI Transactions

If a customer approaches branch claiming that UPI Fraud happened in his/her account. In that case, branch need to check the details of beneficiary in HUPIINQ-Finacle Menu and if branch really feels that said transaction is a fraudulent transaction, they can forward the matter to their respective General operations Department of their respective zone.

Also, the branch can advise customer to **reset UPI PIN** as well as ATM Pin and not to share any PII (Personal Identifier information) like card details, ATM PIN, OTP, CVV, UPI PIN with anyone to avoid any financial loss in future.

Also, Customer can be guided to use wrong UPI Pin thrice to block the UPI. He can reset his UPI Pin only after 24 hours. So, if a customer suspects any suspicious UPI transaction in his account, he can disable his UPI by entering wrong UPI PIN thrice.

7-UPI Transaction related queries

UPI Transaction Reference No. / RRN is the first identifier to track any UPI Transaction at various levels like customer, branch, NPCI etc. In case of any dispute/queries, RRN is the identifier by which the transaction can be uniqely tracked. While communicating with any of the stakeholders, if an RRN is quoted, it becomes easier to track and identify the fate of the transaction.

Branches may inquire the RRN in finacle using the following methods:

- In TM menu - tran particular of transaction as "BUPI/9xxxxxxxxxxx/Date/…"
- (9xxxxxxxxxxx is RRN) and in case of manual reversal the tran particular is as "9xxxxxxxxxxx/Date/UPI/…."
- In TM menu- Ref No. of the transaction is the UPI Reference no./RRN.

Customers may inquire the RRN using the following methods:

- In app (through which transaction was done) in transaction history.
- In the text message received by the customer referred as UTR/Txn id.

****

Annexure -2

INDEMNITY FOR UPI WRONG FUND TRANSFER ON BANK'S LETTER HEAD

To
The Branch Manager/Head
_______________________ (Name of Beneficiary Bank)
_______________________ (Name of Beneficiary Bank Branch)

Subject- UPI Amount transferred to Wrong Account

Dear Sir/Madam,

Our _____________________________ (Name of Remitting Branch) Branch has erroneously initiated UPI on _________ (Date of Transaction) with ref. no. _________________________which has been settled to your bank. We request you to arrange to return the funds urgently to remitter account number ______________________with ______________________ (Name of Remitting Bank) _____________________ (IFSC Code) on priority and confirm us return transaction ref no.

Transaction Details are as follows:

Details	**Transaction Details**
Sender IFSC	
Sender Name	
Beneficiary IFSC Code	
Beneficiary Account No.	
UPI Reference No. (RRN)	
Amount	
Date of transaction	

अगर बनाना है डिजिटल भारत, ई-भुगतान की बनाओ आदत

Aadhaar Pay - AePS

Aadhaar Enabled Payment System

AePS is a bank-led model that uses Aadhar authentication to allow online interoperable transactions at PoS (micro ATMs) terminals through business correspondents of any bank. AePS was launched to facilitate banking services in unbanked/rural areas and disburse Central and state government entitlements under schemes such as the National Rural Employment Guarantee Act (NREGA), social security pension and pension for disabled or senior citizens, using Aadhaar authentication.

Since its launch in 2016, AePS has grown at a CAGR of 137%. It recorded over 400 million transactions in April and May 2020, owing to direct disbursement under the stimulus packages announced by the Government during the COVID-19 crisis.

AePS has gained traction in the market and we believe its adoption would increase in the coming years.

AePS was launched to drive financial inclusion in the country and it has been a game changer for the Government in disbursements.

With the Government looking to promote Aadhar-based payment, the number of AePS-based transactions has increased significantly over the years.

The BHIM-Aadhaar digital payment tool can be a cost-effective method for merchants who don't want to invest in building PoS infrastructure. This can help acquirers who are unable to onboard merchants on physical PoS earn additional MDR revenue. Additionally, it doesn't require customers to bring a physical card to the location while making a payment, which further eliminates the need for them to remember any PIN and creates a frictionless experience.

In order to further speed track Financial Inclusion in the country, Two Working Groups were constituted by RBI on Micro ATM standards and Central Infrastructure & Connectivity for Aadhaar based financial inclusion transactions with members representing RBI, Unique Identification Authority of India, NPCI, Institute for Development and Research in Banking Technology and some special invitees representing banks and research institutions.

The working group on Micro ATM standards & Central Infrastructure & Connectivity has submitted its report to RBI. As a part of the working group it was proposed to conduct a Lab level Proof of concept (PoC), integrating the authentication & encryption standards of UIDAI, to test the efficacy of Micro ATM standards and transactions using

Aadhaar before they are put to actual use. The PoC was successfully demonstrated at various venues.

We can say that AePS is a bank led model which allows online interoperable financial transaction at PoS (Point of Sale / Micro ATM) through the Business Correspondent (BC)/Bank Mitra of any bank using the Aadhaar authentication

The only inputs required for a customer to do a transaction under this scenario are: -

- IIN (Identifying the Bank to which the customer is associated)
- Aadhaar Number
- Fingerprint captured during their enrollment

Objectives:

- To empower a bank customer to use Aadhaar as his/her identity to access his/ her respective Aadhaar enabled bank account and perform basic banking transactions like cash deposit, cash withdrawal, Intrabank or interbank fund transfer, balance enquiry and obtain a mini statement through a Business Correspondent
- To sub-serve the goal of Government of India (GoI) and Reserve Bank of India (RBI) in furthering Financial Inclusion.
- To sub-serve the goal of RBI in electronification of retail payments.
- To enable banks to route the Aadhaar initiated interbank transactions through a central switching and clearing agency.
- To facilitate disbursements of Government entitlements like NREGA, Social Security pension, Handicapped Old Age Pension etc. of any Central or State Government bodies, using Aadhaar and authentication thereof as supported by UIDAI.
- To facilitate inter-operability across banks in a safe and secured manner.
- To build the foundation for a full range of Aadhaar enabled Banking services.

How to get it:

- Provide KYC (Know Your Customer) information to open a new account
- Aadhaar Number should be linked with bank a/c

Service Activation:

- None
- 1-2 minutes post Aadhaar seeding

What is required for Transaction?

- Micro ATM
- Remember Aadhaar
- Give Bank name
- Present self (Aadhaar holder) with Bio-metrics (Finger and/or IRIS)
- Assisted mode

Transaction Cost:

- NIL to customer
- Merchant or BC may get charged or paid based on bank‘s discretion

Disclaimer: The transaction costs are based on available information and may vary based on banks.

Services Offered:

- Balance Enquiry
- Cash Withdrawal
- Cash Deposit
- Aadhaar to Aadhaar funds transfer
- Payment Transactions (C2B, C2G Transactions)

Funds Transfer limit:

- Banks define limit. No limit for RBI.

Disclaimer: The funds transfer limits are based on available information and may vary based on banks.

Service Available from no. of operators:

- 118 banks
- Interoperable

BHIM Aadhaar Pay

BHIM Aadhaar Pay is meant for merchants to receive digital payments from customers over the counter through Aadhaar authentication. It allows for any merchant associated with any acquiring bank on BHIM Aadhaar Pay service, to allow the merchant to accept payment from a customer of any bank, by authenticating the customer's biometrics – currently only fingerprints, directly from the customer's Aadhaar enabled bank account and receive the sale proceeds instantaneously directly into merchant's own bank account.

To be able to effect the same, the merchant must have an Android mobile with the BHIM Aadhaar app and a certified biometric scanner attached with the mobile phone on the USB port AND both the merchant and customer should have had linked their Aadhaar numbers to their bank accounts respectively.

- Facilitates digital payments using thumb imprint on a merchant's biometric enabled device
- App is based on UPI
- App made for merchants and shopkeepers but payers enjoy the benefits
- BHIM Aadhaar Pay is a digital payment acceptance solution.
- It is a merchant mobile application using an Android smartphone and biometric device
- Meant for merchants to receive digital payments from customers over the counter through Aadhaar authentication
- Customer performs transaction by providing his Aadhaar number and biometric.
- The transaction will be interoperable in nature allowing any bank customer to transact on BHIM Aadhaar Pay.
- The merchant funds will be credited real time to the merchant account linked at the time of registration after successful completion of the transaction.
- The per transaction limit is Rs. 2000/-
- BHIM Aadhaar Pay is different from BHIM (NPCI UPI's Product).

Features:

- Only Aadhaar number linked to Bank account required for making payments.
- Fingerprints used for authentication.
- No need to remember passwords, Card PIN and wait for OTP.

Benefits:

- No need to carry any credit/debit card, cash, cheque or mobile wallets.
- Reduction of PoS terminals.
- Customer does not need to download any app when making payments.
- Mobile phone not required while making payments.
- More secured than cash, card, mobile wallets as customer needs to be physically present for making payments.

Requirements for the merchant to start using BHIM Aadhaar Pay:

- Aadhaar seeded account with Bank.
- STQC Certified Biometric Reader with Micro USB / USB C-Type connector.
- Android smartphone with Android version 4.2 or higher with internet connectivity and OTG support for connecting biometric device.
- Phone should be able to power the biometric reader.

Steps to follow before going Live:

- Download Bhim Aadhar Pay.
- Merchant should fill the Application form and sign the Merchant Agreement
- On boarding registration process and Agreement will be carried through Zones

Process Flow of BHIM Aadhaar Baroda Pay:
Merchant Login

- Install Aadhar Payment Application in the smart phone.
- The icon will appear on phone screen after successful installation. Click on the Application Icon to launch the application.
- Enter Aadhar Number of the Merchant and click on "Proceed"
- Application will redirect to fingerprint capturing page. Capture Fingerprints of the Merchant for UID based authentication.

Merchant Pay Transactions:

- Click on Aadhar Pay option.
- Select the bank of the customer and enter Aadhaar number of customer along with transaction amount. Click on "Aadhar Pay" to proceed with the transaction.
- Click on "Yes" to confirm
- Application will redirect to fingerprint capturing page. Capture Fingerprints of the customer for UID based authentication and click on "Proceed".
- Below Receipt will be generated on phone screen after successful transaction.
- Successful payment message displayed on mobile screen of the Merchant with reference number.
- Click on "OK" to continue.

Cost of Biometric device provided to merchants are recovered as per nature of Institutions provides as follow

Select Institution

- These institute are selected by the Government.
- Compulsory using digital payments as mode of accepting payment from the customer like AIIMS, PDS.
- In such cases bank need to absorb the device cost instead of recovering from the institute.

State Government Subsidies

- State government is facilitating the supply by offering devices at subsidized rates.
- In such cases difference between the cost of the device and subsidy obtained will be absorbed by the Bank.

Corporate Institutions

- Bank will collect cost of devices upfront from such Institutions.

Merchants in Tier 5 and Tier 6 cities

- NABARD provides subsidy for device provided to merchant who belongs to Tier 5 and Tier 6 cities.
- In such cases difference between the cost of the device and subsidiary obtained from the NABARD is absorbed by the bank.

BOI Bharat QR

Bharat QR code is an interoperable payment acceptance solution that supports Visa, MasterCard. Amex and RuPay cards & BHIM-UPI for wider acceptance. Bharat QR code will enable rapid rollout of digital payments acceptance infrastructure throughout the country, as it does not involve any upfront investment in Point of Sale (PoS) machine.

To facilitate massive rollout in a short span of time, Bharat QR code-based payment solution is introduced with following advantages:

- ❖ Bharat QR code does not require any upfront expenditure.
- ❖ Bharat QR code is a single unified QR code capable of accepting payments from Visa, MasterCard, RuPay Cards for wider acceptance.
- ❖ Customer can easily make payments through Bharat QR code and does not require to carry physical Debit or Credit card.
- ❖ The risk of data theft or security issues through tampered or cyber-compromised point of sale devices is minimized.
- ❖ Bharat QR code supports dynamic QR codes, which may be printed on electricity bills, gas bills and other utility bills to make payments to the respective vendors.
- ❖ Merchants accepting the payment through Bharat QR code, receives the amount directly in their Bank accounts.

Bank of India Bharat QR – Consumer app is a QR code-based payment solution for Bank of India consumers. It offers a hassle free and secure way to make payments to merchants.

It is a unique solution where the Mobile application can make payment without the need of carrying a physical card.

Consumer scans the Qr code presented by the merchant and initiates the payment through app.

Features:

- Interoperability among QR based payment products of different networks: RuPay, Visa, MasterCard and Amex.
- Substitute for PoS Terminals.
- Low cost acceptance payment solution.
- Push based transaction i.e. transaction originates from card holder.
- No need to share physical card with merchant.

Requirement:

- Bank application which supports Bharat QR code (Required for the card holder to make payment)
- Merchant's Bharat QR code (Provided by bank to receive payment)

Way forward:

- 28 Acquiring Banks and 28 Issuing Banks live on Bharat QR
- Future ready to accept payments from other channels like UPI, Aadhaar Pay, IMPS, BBPS

Bank of India Bharat QR has a number of benefits as below:
1. Consumer pays by just scanning Qr code.
2. Link Multiple cards into the app for payment.
3. Notifications for Payments received.
4. Change mPin of app.

Payment Gateway

The Payment Gateway (PG) enables merchants, corporate and Government entities to process online transactions via the use of Debit Card, Credit Card, IB, UPI etc.

PG supports online payment whether on the Internet or any other electronic channel such as Interactive Voice Recognition (IVR), kiosk, and call center with secure protection and integrity.

How does it work?

Gateway checks for validity, encrypts transaction details, ensures they are sent to the correct destination and then decrypts the responses which are sent back to the shopping cart / billing / account system.
It is integrated with a variety of shopping cart software, databases, Internet merchant accounts and protocol exchange servers.

Advantages of payment gateways

- This method of payment has many advantages over other methods, such as:
- Much faster (and easier) than cheques or manual credit card processing
- Much more secure than manual credit card processing
- No need for the customer to jump between your site and a third-party site (such as PayPal) to perform a transaction

Benefits to the Bank

- Current Account with the bank
- Good float preferably in current account
- Retention of existing customers
- Acquiring additional business through existing customer referrals due to customer service
- Acquisition of new customers
- Readymade MIS to the merchants

Selection of merchants

- Our existing customers
- Through marketing
- Through tenders available in newspapers
- Through websites

Target Clientele:

- Schools College – Education Fees
- Govt Offices - MTNL etc. – Utility bills , Collection of royalty
- Collection of E-auction amt
- Collection on account of sale of books
- Collection of subscriptions
- Collection of donations etc.…

Customer Satisfaction:

- Ready availability of MIS
- Collection expenses avoided

Our Tie-ups:

- Billdesk
- Payu India

Basic Fee Structure

Credit Card Charges	–	1.1% to 1.9%*
Debit Card Charges	–	0.75% upto Rs. 2000/-* 1.0% over Rs. 2000/-*
Internet Banking	–	Rs.15.00 to Rs.17.00*

(*Service Tax as applicable)

Door Step Banking

Present day scenario in Banking has undergone tremendous change and the stress is on availability of banking facilities at customer's doorstep. With this in mind, Bank of India has started providing Door Step Banking facilities to its premium clients.

Eligibility:

- All Corporate customers having value/PSUs/Government departments.
- High Net Worth individuals.
- Full KYC compliance prior to commencement of the service.

Registration:

- Customers to apply for the service through the Branch where they maintain their Account.
- Upon fulfilling the eligibility listed above, their request will be registered.
- Thereafter execution of Agreement with the Bank would be done.
- Customers to apply for the service through the Branch where they maintain their Account.
- Upon fulfilling the eligibility listed above, their request will be registered.
- Thereafter execution of Agreement with the Bank would be done.
- Officer from Zonal office shall be nominated as coordinating officer and his contact details shall be shared with the customer. In case of need, customer/vendor can contact the coordinating officer for resolution of issue

Services provided:

- Cash Pick on Daily/Call basis
- Cash Delivery
- Cheque pick up
- Delivery of DD/Pay-order
- For customers who register for cash pick up on daily basis, cheque pick up/draft delivery would be done initially without any charges.
- Pick up on call basis: Registered customers to call branch minimum 24 hours in advance and inform quantum and time of pick up. Branch would then tie up for pick up with the vendor (service provider).

Maximum Limit:

- For pick up – Rs.100.00 lakhs per day.
- For delivery – Rs.50.00 lakhs per day

Denomination:

- Notes below Rs.100/- will not be accepted.

Cheque Pick up:

- Cheques along with paying in slips will be collected by CE in tamper proof sealed envelopes and handed over to the Branch. To prevent misuse, customer to cross the cheques and write 15-digit account number on the reverse of the cheque.

Draft Delivery:

- Delivery of DD will be done in tamper proof envelopes (issuance of DD by debit to account) as per customer's request in writing/cheque only.

Cash Delivery:

- Cash delivery will only be in packets of 100 pieces.
- Letter of Intent issued to vendor will contain details of persons to whom cash is to be delivered with their photo id.
- Cash packets will be put in tamper proof bags in front of CCTV cameras and CE, sealed with numbered tamper proof seals which will be written on delivery order.
- Customer will confirm that the bag and seal are not tampered, tally the seal number with the one on delivery order.

Charges:

In addition to vendor's charges, Bank will also levy cash handling charges – presently as under:

- Rs.25/- per pick up + Rs.8/- per packet (denomination – Rs.500/- / Rs.2000/-)
- Rs.10/ - per packet (denomination – Rs.100/-)
- FREE - Up to 10 packets – (1 packet – 100 pieces)
- Incidental charges like parking charges for van at customer's place, toll tax etc would be to customer's account.
- Service tax as applicable to be borne by customer.
- Charges will be debited to customer's account on monthly basis based on authorization.

Benefits:

- Helps retention of existing clients
- Income (after paying off vendor's bill) can be substantial. Branch, hence, to negotiate good terms with the customer.
- Availability of float balance would add to Bank's income.
- Customised MIS is available. Based on this, both Bank & customer can ensure deposition of amounts.
- Customer's staff savings accounts can be opened and third party and retail loan products can also be considered to them.
- Can enlist customer's help for addition of clients.

NACH

NACH
NATIONAL AUTOMATED CLEARING HOUSE

National Payments Corporation of India (NPCI) has implemented "National Automated Clearing House (NACH)" for Banks, Financial Institutions, Corporates and Government a web-based solution to facilitate interbank, high volume, electronic transactions which are repetitive and periodic in nature. NACH System can be used for making bulk transactions towards distribution of subsidies, dividends, interest, salary, pension etc. and also for bulk transactions towards collection of payments pertaining to telephone, electricity, water, loans, investments in mutual funds, insurance premium etc.

National Automated Clearing House (NACH) is a centralized system, launched with an aim to consolidate multiple ECS systems running across the country and provides a framework for the harmonization of standard & practices and removes local barriers/inhibitors. NACH system will provide a national footprint and is expected to cover the entire core banking enabled bank branches spread across the geography of the country irrespective of the location of the bank branch.

With the implementation of NACH system, NPCI intends to provide a single set of rules (operating and business), open standards and best industry practices for electronic transactions which are common across all the Participants, Service Providers and Users etc. NACH system also supports Financial Inclusion measures initiated by Government, Government Agencies and Banks by providing support to Aadhaar based transactions.
The NACH system facilitates the member banks to design their own products and also addresses specific needs of the banks & corporates including a refined Mandate Management System (MMS) and an online Dispute Management System (DMS) coupled with strong information exchange and customized MIS capabilities.

The NACH system provides a robust, secure and scalable platform to the participants with both transaction and file-based transaction processing capabilities. It has best in class security features, cost efficiency & payment performance (STP) coupled with multi-level data validation facility accessible to all participants across the country.

NACH's Aadhaar Payment Bridge (APB) System***, developed by NPCI has been helping the Government and Government Agencies in making the Direct Benefit Transfer scheme a success. APB System has been successfully channelizing the Government subsidies and benefits to the intended beneficiaries using the Aadhaar numbers. The APB System links the Government Departments and their sponsor banks on one side and beneficiary banks and beneficiary on the other hand.

NACH System can be used for making bulk transactions towards distribution of: -

- Subsidies
- Dividends,
- Interest,
- Salary,
- Pension etc.

<u>Bulk transactions towards collection of payments pertaining to-</u>

- Telephone,
- Electricity,
- Water,
- Loans,
- Investments in mutual funds,
- Insurance premium etc.

<u>NACH – CR</u>:

NACH – CR is used by us (BOI) for affording credit to a large number of beneficiaries who are our customers

Single debit to the sponsor bank's account and multiple credits to different destination banks' account

Important Features & Benefits

- MICR settlement
- Multiple file processing in a single settlement
- Customized MIS
- Cost effective
- Availability of Recall option before settlement
- Online Dispute Management System (DMS)

NACH Debit:

- NACH-DR provide a better & efficient Mandate based debit services to the banks.
- Automated processing and exchange of mandate information electronically with well-defined timelines for acknowledgement / confirmation.
- Each mandate needs to be accepted/authorized by the debtor bank before the User can initiate a transaction
- Each mandate is uniquely identified by **Unique Mandate Reference Number (UMRN)** which makes tracking of multiple mandate details easier for customers.
- Bank can leverage on the existing CTS instrument scanning infrastructure for scanning and maintaining repository of the mandate's images

Important Features & Benefits

- Standardization and digitization of mandates
- Minimal time taken to activate the Mandate – same day processing possible
- Simplification of the mandate acceptance and recording process
- Reduced operational cost for the banks and its clients
- Higher revenues
- Complete audit trail of the mandate during its lifecycle
- Unique identifier number allocated to each mandate (UMRN)
- Mandates can be processed by the member for any branch across the country
- Allows Corporate clients to directly upload files for approval
- Functions on International Messaging Standard - ISO 20022

Existing Clients:

DICGC for bulk outward credits;

Target Group of Clients:

- All branches of Bank who need to send huge no. of remittances to customers of other banks.
- Dividend payments using NACH platform.
- NBFCs, Registrars and Transfer agents for corporates and mutual funds like Karvy etc.

*** **Aadhaar Payment Bridge (APB) System**

Aadhaar Payments Bridge System facilitates end – to end processing of bulk electronic payment instructions primarily facilitating the government departments to disburse the Direct Benefit Transfers (DBT). In APB system, transactions are routed to a bank based on the mapping of Aadhaar number to the IIN of a bank.

The participating banks have to perform a number of activities to complete the mapping and un-mapping of Aadhaar number in the NPCI mapper database.
The APB System sub-serves the goal of Financial Inclusion and provides an opportunity to the Government to attempt financial re-engineering of its subsidy management program. The implementation of APB System has also led to electronification of a large number of retail payment transactions which were predominantly either in cash or cheque.

RTGS/NEFT/IMPS Contact Numbers and E-mail IDs

RTGS/NEFT/IMPS		
RTGS	Rtgs.boi@bankofindia.co.in	(022) 67447092/ 93
NEFT	Boi.neft@bankofindia.co.in	(022) 61312984/ 61312992/ 61312997
IMPS	Boi.imps@bankofindia.co.in	(022) 61312994/ 61312995
UPI	Support.MobileApps@bankofindia.co.in	(022) 67447025

RTGS System

(Updated as on October 30, 2019)

1. The acronym 'RTGS' stands for Real Time Gross Settlement, which can be explained as a system where there is continuous and real-time settlement of fund-transfers, individually on a transaction by transaction basis (without netting). 'Real Time' means the processing of instructions at the time they are received; 'Gross Settlement' means that the settlement of funds transfer instructions occurs individually.

2. Are the payments under RTGS final and irrevocable?

Considering that the funds settlement takes place in the books of the Reserve Bank of India, the payments are final and irrevocable.

3. What are the benefits of using RTGS?

Ans. RTGS offers many advantages over the other modes of funds transfer:

- It is a safe and secure system for funds transfer.
- RTGS transactions / transfers have no amount cap.
- The system is available on all days when most bank branches are functioning, including Saturdays.
- There is real time transfer of funds to the beneficiary account.
- The remitter need not use a physical cheque or a demand draft.
- The beneficiary need not visit a bank branch for depositing the paper instruments.
- The beneficiary need not be apprehensive about loss / theft of physical instruments or the likelihood of fraudulent encashment thereof.
- Remitter can initiate the remittances from his / her home / place of work using internet banking, if his / her bank offers such service.
- The transaction charges have been capped by RBI.

- The transaction has legal backing.

4. How is the processing of RTGS different from that of National Electronic Funds Transfer (NEFT) System?

Ans. NEFT is an electronic fund transfer system in which the transactions received up to a particular time are processed in batches. Contrary to this, in RTGS, the transactions are processed continuously on a transaction by transaction basis throughout the RTGS business hours.

5. Is RTGS a 24x7 system or are there some timings applicable?

Ans. RTGS is not a 24x7 system. The RTGS service window for customer transactions is available to banks from 7 am to 6 pm on a working day, for settlement at the RBI end. However, the timings that the banks follow may vary from bank to bank.

6. Is there any minimum / maximum amount stipulation for RTGS transactions?

Ans. The RTGS system is primarily meant for large value transactions. The minimum amount to be remitted through RTGS is ₹ 2,00,000/- with no upper or maximum ceiling.

7. What about processing charges / service charges for RTGS transactions?

Ans. With effect from July 01, 2019, the Reserve Bank has waived the processing charges levied by it for RTGS transactions. Banks may pass on the benefit to its customers.

With a view to rationalize the service charges levied by banks for offering funds transfer through RTGS system, a broad framework of charges has been mandated as under:

a) Inward transactions – Free, no charge to be levied.

b) Outward transactions - ₹2,00,000/- to 5,00,000/-; not exceeding ₹24.50/-; (exclusive of tax, if any)

Above ₹ 5,00,000/-: not exceeding ₹ 49.50/-. (exclusive of tax, if any)

Banks may decide to charge a lower rate but cannot charge more than the rates prescribed by RBI.

8. What is the essential information that the remitting customer needs to furnish to the bank for making a remittance?

Ans. The remitting customer has to furnish the following information to a bank for initiating a RTGS remittance:

i. Amount to be remitted
ii. The account number to be debited
iii. Name of the beneficiary bank and branch
iv. The IFSC number of the receiving branch
v. Name of the beneficiary customer
vi. Account number of the beneficiary customer
vii. Sender to receiver information, if any

9. How would one know the IFSC number of the receiving branch?

Ans. The IFSC number can be obtained by the remitter (customer) from his / her bank branch. Alternatively, it is available on the cheque leaf of the beneficiary. This code number / bank branch information can be communicated by the beneficiary to the remitting customer. The list of IFSCs is also available on the RBI website at the link http://rbidocs.rbi.org.in/rdocs/RTGS/DOCs/RTGEB0815.xlsx

10. Do all bank branches in India provide RTGS service? How can a remitting customer know whether the bank branch of the beneficiary accepts remittance through RTGS?

Ans. For a funds transfer to go through RTGS, both the sending bank branch and the receiving bank branch need to be RTGS enabled. Presently, there are more than 140,000 RTGS enabled bank branches, the list of which is available on the RBI website at the link
http://rbidocs.rbi.org.in/rdocs/RTGS/DOCs/RTGEB0815.xlsx

11. What care should be taken while originating a RTGS transaction?

Ans. The following should be ensured while putting through a funds transfer transaction using RTGS –

- Originating and destination bank branches are part of the RTGS network.
- Beneficiary details such as beneficiary name, account number and account type, name and IFSC of the beneficiary bank branch should be available with the remitter.
- Extreme care should be exercised in providing the account number of the beneficiary, as, in the course of processing RTGS transactions, the credit will be given to the customer's account solely based on the account number provided in the RTGS remittance instruction / message.

12. In RTGS, why is credit to the beneficiary given solely on the basis of account number?

Ans. Transactions in RTGS happen in real time and it is not possible to match name and account number before affording credit to the beneficiary. Since name in the Indian context is spelt differently and would not really match with that available with the beneficiary bank, the process of affording credit solely based on the account number of the beneficiary has been enabled.

13. What is the time taken for effecting funds transfer from one account to another through RTGS?

Ans. Under normal circumstances, the beneficiary branches are expected to receive the funds in real time as soon as funds are transferred by the remitting bank. The beneficiary bank has to credit the beneficiary's account within 30 minutes of receiving the funds transfer message.

14. Can a remitting customer initiate a transaction for a future date?

Ans. The RTGS system accepts future value dated transactions from the remitting bank for settlement on RTGS working days up to three days' in advance. Such transactions will be placed in the queue and shall be settled on the basis of the value date of the transaction.

15. Can a transaction be originated to draw (receive) funds from another account?

Ans. No. RTGS is a credit-push system i.e., transactions can be originated by the payer / remitter / sender only to pay / transfer / remit funds to a beneficiary.

16. Can an RTGS transaction be tracked? Would the remitting customer receive an acknowledgement of money credited to the beneficiary's account?

Ans. While the customers do not have the facility to track the transaction, the RBI has implemented the feature of positive confirmation in an RTGS transaction. Under this, the remitting bank would receive a message from RBI (through the beneficiary bank) that the money has been credited to the beneficiary bank / customer account. Based on this, the remitting bank should advise the remitting customer that money has been credited to the receiving bank's beneficiary account.

17. Would the remitting customer get back the money if it is not credited to the beneficiary's account? Is there any time frame prescribed for it?

Ans. Yes, if it is not possible to credit the funds to the beneficiary customer's account for any reason, the funds received by the RTGS member bank will be returned to the originating bank within one hour of receipt of the payment at the Payment Interface (PI) or before the end of the RTGS Business day, whichever is earlier. Once the money is received back by the remitting bank, the original debit entry in the customer's account needs to be reversed.

18. Is a customer eligible to get compensation for delay in returning the payment?

In case of any delay in returning the failed payment, the originating customer is eligible to receive compensation at current repo rate plus 2%.

19. Whom can a customer contact, in case of non-credit or delay in credit to the beneficiary account?

Ans. The customer can contact his / her bank / branch if there is an issue of delay / non-credit to the beneficiary account. If the issue is not resolved satisfactorily, complaint may be lodged at email to - cgmcepd@rbi.org.in or by post at following address giving UTR number and details of the issue -

The Chief General Manager
Customer Education and Protection Department
1st Floor, Amar Building, Fort
Reserve Bank of India
SBS Road, Fort
Mumbai, 400 001

20. What is UTR number?

Ans. Unique Transaction Reference (UTR) number is a 22-character code used to uniquely identify a transaction in RTGS system.

(These FAQs are issued by the Reserve Bank of India for information and general guidance purposes only. The Bank will not be held responsible for actions taken and/or decisions made on the basis of the same. For clarifications or interpretations, if any, one may be guided by the relevant circulars and notifications issued from time to time by the Bank.)

Timings for RTGS

Sr.No.	Event	Time
1	Opening of Business	07:00 hours
2	Customer transactions (Initial cut-off)	18:00 hours
3	Inter Bank Transactions (Final Cut-f)	19:45 hours
4	IDL Reversal	19:45 hours – 20:00 hours
5	End of Day	20:00 hours

IMPS

The full form of IMPS is Immediate Payment Service. It is launched in 2010 by Indian government and is facilitated by NPCI (National Payment Corporation of India). As the name suggests, it completes transactions immediately. It is a service which allows you to make payments using your mobile number. It uses mobile number or Aadhaar number to connect to bank accounts and complete payments. Hence, it is a secure method for transferring funds. The services of IMPS are available 24X7 and even on holidays.

IMPS can be used to avail many services. One of the government's most praised service *99# banking is also based on IMPS.

How It Works?

IMPS uses mobile number or Aadhaar number to connect with a bank account. When you send money to anyone using IMPS, it first connects you to your bank account using your mobile number. Unlike NEFT and RTGS, it does not transfer funds directly to the beneficiary's account. But it first transfers funds from your account to your mobile number. Then it transfers that fund from your mobile number to his/her mobile number. And at last from beneficiary's mobile number to his/her account.

The Benefits of IMPS

- Real-time domestic fund transfer. Money will be credited in Beneficiary's account within a few seconds.

- IMPS is fast, safe, secure and cost effective.
- No minimum amount limit on transactions. You can even transfer ₹ 1 only with IMPS.
- IMPS is available 24X7 and on holidays also.
- You can make intra bank as well as interbank payments.
- Can be used on a mobile phone, internet banking and even ATMs (IMPS through ATMs are presently not available for BOI customers).
- Knowing beneficiary's Account number and IFSC is not compulsory in IMPS. You can transfer funds using MMID, Aadhaar number and mobile number only.
- You get the Debit & Credit Confirmation by SMS immediately.

You can avail following services using the IMPS banking

1. Funds transfer using mobile number and MMID
2. Funds transfer using Aadhaar number (not applicable for BOI customer)
3. Funds transfer using IFSC and Account number
4. Fund transfer to "Chillr" or "Non Chillr" customers
5. UPI – It is a mobile app-based payment method which uses VPA of beneficiary. UPI works on IMPS structure.
6. Merchant payments – You can pay to a merchant using his MMID.
7. USSD banking (*99# Banking) – It gives you fund transfer facility through the feature phone
8. QSAM – By dialing *99*99# and providing Aadhaar number when prompted for, you can know the Aadhaar and bank account link status.

ATMs

ATM machine is broadly classified in three categories
(1) White Label ATM (WLA)
(2) Brown Label ATM
(3) Bank own ATM

What is White Label ATM?

- The Automated Teller Machines (ATMs) which is set up, owned and operated by non-banks is called as White Label ATM (WLA).
- Features and Functions of White Label ATM are same as that of Normal ATM machines.
- Difference is this ATM machine does not have any branding of Bank.
- These machines are usually deployed by NBFC (Nonbanking Financial Institutions).
- The basic idea about White Label ATM is to increase geographical spread of ATM so that more number of people can be incorporated under financial inclusion program.

What we should know about White Label ATM?

- White Label ATMs are like normal ATM. However, cash deposit or cash acceptance facility is not permitted at the WLAs.
- At White Label ATM you will not find logo of any bank like ICICI, SBI etc. You will find logo of White Label ATM operator on these ATMs.
- An Individual can use their ATM-cum-debit cards, credit card for the cash withdrawal at these ATMs.
- In case of fail transaction while using white label ATM you need to report to card issuing bank. ATM card issuing bank is responsible of resolving conflict.

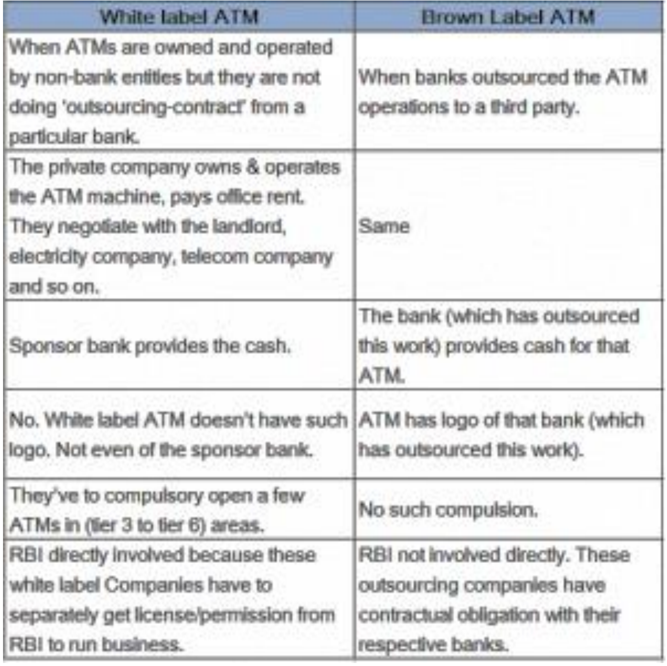
- Cash Management at WLA will be done by sponsor bank. Sponsor bank will make an arrangement with NBFC for the cash at respective locations.
- The Grievance Redressal Mechanism will be the same as that of normal bank ATMs.

How White Label ATMs Functions?
White Label ATMs are operated by NBFC. NBFC need a bank sponsor to settles all issues related to cash management, transaction settlement with other banks etc for this ATM. The sponsor bank has to tie up with the other bank at the place where it is not present.

What is Brown Label ATM?

- Brown Label ATM is sharing cost concept. In Brown Label ATM hardware is owned by service provider, but cash management and network connectivity are provided by sponsor bank.
- Features and functions of Brown Label ATM are same as that of normal ATM Machine.
- This machine contains Logo of sponsor bank.
- Brown Label ATM is cost effective solution for the banks.

Difference White Label ATM, Brown Label ATM



White label ATM	Brown Label ATM
When ATMs are owned and operated by non-bank entities but they are not doing 'outsourcing-contract' from a particular bank.	When banks outsourced the ATM operations to a third party.
The private company owns & operates the ATM machine, pays office rent. They negotiate with the landlord, electricity company, telecom company and so on.	Same
Sponsor bank provides the cash.	The bank (which has outsourced this work) provides cash for that ATM.
No. White label ATM doesn't have such logo. Not even of the sponsor bank.	ATM has logo of that bank (which has outsourced this work).
They've to compulsory open a few ATMs in (tier 3 to tier 6) areas.	No such compulsion.
RBI directly involved because these white label Companies have to separately get license/permission from RBI to run business.	RBI not involved directly. These outsourcing companies have contractual obligation with their respective banks.

What is Bank own ATM?
The Automated Teller Machines (ATMs) which is set up, owned and operated by banks is called as bank own ATMs. Responsibility of cash management, AMC, security lies with banks.

DCC - Dynamic currency conversion

Dynamic currency conversion (DCC) or cardholder preferred currency (CPC) is a process whereby the amount of a Visa or MasterCard transaction is converted by a merchant or ATM to the currency of the payment card's country of issue at the point of sale. This enables our international Customers to feel at home, with the convenience to pay in their home currency

- DCC allows customers to see the amount their card will be charged, expressed in their home currency.
- Facility is optional and cardholder will be given the option to avail the facility at the time of making payment to the merchant, otherwise he can settle in local currency in INR.
- DCC feature will be provided to MEs on their request, where the existing terminal will be replaced by new terminal with DCC capability, at no extra cost.

Yield from foreign card holders and benefits:

- Approx. 0.25% (when settled in INR)
- Excess of 1%, may go up to even 2.5 %
- Financial incentive on each transaction
  (Resulting in substantial growth in non-interest income)

Card Acceptance Infrastructure

General public and the stakeholders are requested to furnish their specific and actionable comments by 15th April 2016 to the Chief General Manager, Department of Payment and Settlement Systems, Reserve Bank of India, Central Office, 14th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai – 400 001. Comments may also be furnished by email by 15th April 2016.

PREFACE

The Reserve Bank of India (the Bank) has been encouraging reforms in the payment and settlement systems of the country, leveraging on the benefits derived from developments in technology. The policy and regulatory framework addresses the need to put in place a bouquet of payment options both for individual as well as institutional users while addressing the safety and security requirements of the systems and the users.

The Bank has also been sharing and signaling the desired developments in payment and settlement systems in the country through its Payment Systems Vision Documents. An over-arching Vision for payment systems in recent times has been the need to ensure greater adoption of electronic payments and migrate towards becoming a "less-cash" society.

The efforts of all stakeholders have resulted in a growing trend in electronic payments. The question of importance is whether further developments in this regard should be left to the users themselves (market forces) or whether this growing trend should be "managed" through appropriate policy framework. While market-forces led growth may address the "economics" of the payments eco-system, it may not always meet the requirements of all segments of users. A structured policy intervention to promote electronic payments may have the advantage of not only addressing the requirements of all sections of society but also enable setting of achievable targets within a definite time-span which can be monitored, reviewed and changed, if necessary.

The Reserve Bank of India has prepared this concept paper on policy framework for expansion of card acceptance infrastructure in the country in consultation with a few stakeholders. The paper outlines the broad contours of a multi-pronged strategy to enhance the growth in acceptance infrastructure and usage of cards including further rationalization of merchant discount rates (MDR) or merchant fees for debit card transactions. In the Fourth Bi-monthly Monetary Policy Statement, 2015-16 it was announced that in order to promote electronic payments and use of cards for transactions, the Reserve Bank will put in the public domain a concept paper for proliferation of card acceptance infrastructure in the country, especially in the tier III to tier VI centres.

Introduction

1.1 The use of electronic channels for accessing banking and payment services is on the rise and is poised for significant growth in the country. The Reserve Bank has been initiating new policies as well as reviewing existing policy measures for facilitating demand and supply of electronic payment services and also ensuring safety and security of such transactions. Recent announcements of the Government also support and reinforce the migration from cash payments to promotion of card and other electronic payments.

1.2 In the eco-system of electronic / alternate payment mechanisms, card payments are perhaps most recognizable. Further, the developments in e-commerce sector have also been significant in encouraging electronic payments, including card payments (credit/debit), which are gradually gaining significance. With the implementation of Prime Minister Jan Dhan Yojana (PMJDY), the card issuance under RuPay network has seen a tremendous growth in a short span of time. Given the high issuance of debit cards to accounts opened under the PMJDY, with benefits to account holders linked to usage of their RuPay debit cards, the imperative to ensure greater usage of cards as well as enhance growth of infrastructure is significant.

1.3 Card payments include payments made using debit cards, credit cards or prepaid / stored value cards. Further, card payments could be done face-to-face (card present / proximity payments) or carried out remotely (card not present / online payments). In all situations, card payments involve a card holder, a merchant / entity with infrastructure to accept card payments, a bank/institution which issues the card and a bank/institution which sets up the infrastructure for accepting card payments.

1.4 As such, even as the growth in ATM infrastructure may be necessary in the short and medium term to meet the cash requirements of consumers, the focus of this paper is on card payments and possible strategies to enhance its acceptance as a means of payment for purchase of goods and services including increasing the growth of related acceptance infrastructure.

Policy framework for safety and security of transactions

1.5 In the context of encouraging card payments and also to ensure that safety and security requirements of card transactions provide the necessary confidence to its users, the Bank has put in place specific policy measures over the last few years for both card-present (CP) transactions (face-to-face, proximity payments) as well as card-not-present (CNP) transactions (remote, online payments).

1.6 Some of these measures include:

- Online alerts to the cardholder for all card transactions – both CP and CNP transactions irrespective of value of transaction to alert customers for transactions done using their card/s; particularly in case of fraudulent transactions, customers are made aware immediately so that preventive / corrective steps can be taken by them immediately;
- Requirement for additional factor of authentication (AFA) for all CNP transactions to authenticate transactions based on information that the customer alone is supposed to know;
- Requirement of PIN@POS for all card present transactions using debit cards to prevent usage of cloned cards and to authenticate transactions with the PIN which the customer alone is supposed to know;
- Issuance of cards for international usage only on specific request by customers, and if issued, it has to be EMV chip and PIN card to prevent fraudulent usage of cloned magnetic stripe cards or online use of cards in other countries where AFA is not required / mandated;
- Setting threshold value for international transactions done using existing magnetic stripe cards enabled for international usage so as to reduce / minimize loss in case of fraudulent use of such cards; and
- Migration of all cards to EMV Chip and PIN to reduce fraudulent use of cloned cards and increase safety in CP transactions

Extant regulatory framework for MDR

1.7 In order to encourage all categories of merchants to deploy card acceptance infrastructure and also to facilitate acceptance of small value transactions through card payments, the Reserve Bank had rationalized the Merchant Discount Rate (MDR)1 for debit cards with effect from September 2012.

1.8 Since then, the MDR for debit card transaction has been capped at 0.75% for transaction values upto Rs.2000/- and at 1% for transaction values above Rs.2000/-

Card transaction: Illustrative Work Flow

1.9 In order to appreciate the economics of card payments, it may be useful to have a perspective on the entities involved in a card transaction and the generic work flow in a card transaction.

Entities involved in the transaction:

- Merchant location: Entity selling goods and services
- Acquiring Bank: The bank which has installed the POS terminal at the merchant location
- Card network: RuPay/ Visa / MasterCard, etc. (transaction routing and settling agency)
- Customer / Consumer: Cardholder
- Issuing Bank: The bank which has issued the card to the customer

Type of transactions:

- ON-US Transaction: where the issuing bank and the acquiring bank are the same entity
- OFF-US Transaction: where the issuing bank and acquiring bank are different entities

Economics of card payments

1.10 Any policy framework structured to drive acceptance of card payments both from merchant as well as from the consumer side, has to balance the concerns, issues and challenges arising from all stakeholders. The economics of card payments has significant costs and benefits to all stakeholders, a brief outline (illustrative but not exhaustive) of which is given below:

Benefits of electronic / card payments:

1.11 The benefits accrue not only to individual users of card payments but also have potential of benefits for the economy as a whole by:

- Providing faster, more secure and convenient way of payment for purchase of goods and services;
- Reducing in cash handling costs leading to increased savings;
- Lowering transaction costs through greater operational efficiency;
- Facilitating better financial intermediation; and
- Providing greater financial transparency by enabling recording of all economic activity, helping in reducing the proliferation of grey economy and increasing tax revenue.

Costs and issues associated with card payments:

1.12 Even though there is the potential to reap the above benefits, there are certain costs and issues that are associated with card payments which inhibit their greater adoption. Some of these are outlined below for different stakeholder segments:

- Merchants – costs related to payment of merchant fees, transparency and taxation, KYC documentation, certification process related to safety and security of transactions/systems, etc. Other issues that act as deterrents include the fact that there could be various stages in supply chain where cash payments are still made; through cash payments transactions are completed immediately whereas settlement of card payments takes some time for processing; etc.

- Consumers – annual fees for cards, levy of convenience charges / surcharge on use of cards, feel of convenience generally associated with cash payments, etc. Other related issues pertain to safety and security concerns, fraud protection mechanisms, concerns regarding consumer grievance redressal mechanism, etc. Last but not the least is the lack of availability of card payment option especially where the consumer spends for day-to-day personal consumption.
- Card issuing banks – costs associated with card issuance, replacement / maintenance, ensuring security requirements at all times, system for addressing consumer complaints and grievances, education and marketing, promotions, putting in place risk and fraud monitoring systems, processing chargeback claims and fraud liability, etc.
- Merchant acquiring banks – costs related to acquiring merchants including capital cost of equipment and maintenance, integration with merchant systems, ensuring compliance with certification, education and training, etc. In addition, investment and constant upgradation of security and risk management systems, fraud protection (underwriting risk), credit evaluation risk, regulatory compliance, etc. are also issues that acquiring banks have to deal with.

1.13 The subsequent chapters address the various issues coming in the way of enhancing the usage and acceptance of card payments, and examine certain strategies that may facilitate in enhancing the card payments infrastructure.

IMT

Instant money transfer - Cardless Cash Withdrawal Facility

Innovative, safe, simple and hassle-free domestic money transfer with cash out facility.

- Self Service – Bank's customer can himself initiate the transaction.
- 24 * 7 * 365, facility availed both by initiator and beneficiary/ receiver.
- Our customer can send money to any beneficiary/ receiver who need not be the customer of BOI or any Bank.
- Beneficiary/ receiver can withdraw money from any BOI IMT enabled ATM without using a card.
- It is useful when beneficiary/ receiver requires cash instantly or emergency Cash.
- It is also useful when beneficiary/ receiver does not have a Bank Account or bank account details are not known.

IMT can be initiated / sent by our Bank's customer either through Retail Internet Banking or our Bank's any IMT enabled ATMs. The beneficiary / receiver can withdraw money, from our Bank's any IMT enabled ATM, without using a card. The withdrawal details are partially communicated to the beneficiary / receiver on his mobile phone and partially by the sender.

The sender of IMT has pre requisite of registering his beneficiary / receiver for a successful IMT. The registration can be done by our customers either through our Retail Internet Banking or through sending a SMS from his registered mobile number.

IMT through Internet Banking

IMT can be sent to receiver/ beneficiary by simply using our Retail Internet Banking facility (with fund transfer facility), as under

- Our Bank customers can login to Bank's Retail Internet Banking facility and initiate IMT. Customer first register receiver/ beneficiaries by entering the beneficiary's name, mobile number, address and his/her Pin code, which is a one-time process.
- Post Registration of a receiver/ beneficiary, sender can initiate IMT by mentioning the IMT Amount and Sender Code (This code should be kept and shared ONLY with receiver/ beneficiary, as the same shall be required by receiver/ beneficiary to withdraw cash from the ATM) and authenticating the transfer.

  Once the IMT is successfully issued, sender receives an SMS on his or her mobile number containing the details of the IMT. The details present in the SMS are:
  - Beneficiary/ Receiver Mobile number
  - The IMT amount
  - IMT Validity Date (In case beneficiary/ receiver omit to withdraw IMT by this date, IMT shall be cancelled by the system and amount shall be credited back to sender's account. Charges for the IMT shall not be reversed.)
  - IMT ID (a unique code which can be used to refer IMT transaction)

Once the IMT is successfully issued, receiver/ beneficiary receives an SMS on his or her mobile number containing the details of the IMT. The details present in the SMS are:

- The IMT amount
- IMT Validity Date (In case beneficiary/ receiver omit to withdraw IMT by this date, IMT shall be cancelled by the system and amount shall be credited back to sender's account. Charges for the IMT shall not be reversed.)
- SMS Pin (System generated code, required for IMT withdrawal)
- IMT ID (a unique code which can be used to refer IMT transaction)

IMT through ATM

Bank' customer can also initiate IMT from Bank's IMT enabled ATM, by providing following details –

- Beneficiary/ Receivers Mobile number
- The IMT amount
- Sender Code (This code should be kept secret and shared ONLY with receiver/ beneficiary, as the same shall be required by receiver/ beneficiary to withdraw cash from the ATM)

Beneficiary/ receiver registration by the sender, as a one-time activity is mandatory. This receiver/ beneficiary's registration can be done by either through SMS or Bank's Retail Internet Banking. The details of the same are provided in section - IMT Beneficiary/ Receiver Registration.

Once the IMT is successfully issued, sender receives an SMS on his or her mobile number containing the details of the IMT. The details present in the SMS are:

- Beneficiary/ Receiver Mobile number
- The IMT amount
- IMT Validity Date (In case beneficiary/ receiver omit to withdraw IMT by this date, IMT shall be cancelled by the system and amount shall be credited back to sender's account. Charges for the IMT shall not be reversed.)
- IMT ID (a unique code which can be used to refer IMT transaction)

Once the IMT is successfully issued, receiver/ beneficiary receives an SMS on his or her mobile number containing the details of the IMT. The details present in the SMS are:

- The IMT amount
- IMT Validity Date (In case beneficiary/ receiver omit to withdraw IMT by this date, IMT shall be cancelled by the system and amount shall be credited back to sender's account. Charges for the IMT shall not be reversed.)
- SMS Pin (System generated code, required for IMT withdrawal)
- IMT ID (a unique code which can be used to refer IMT transaction)

Instances, wherein Beneficiary/ Receiver registration is not done, IMT shall be kept on hold, and sender is expected to provide the Beneficiary/ Receiver, within 24 hours, omitting which IMT shall be cancelled. In case of hold IMT, a SMS shall be sent to the sender.

IMT Beneficiary/ Receiver Registration

Our Customer, as a one-time activity has to register's receiver/ beneficiaries details with the Bank.

In absence of receiver/ beneficiaries details from the customer to the Bank, the IMT shall be in hold status for a maximum of 24 hours, post which it shall be cancelled by the system. Bank shall endeavor to confirm the receiver/ beneficiary's registration to the sender over SMS.

This receiver/ beneficiary's registration can be done by either through SMS or Bank's Retail Internet Banking.

Internet Banking

Our Bank customers can login to Bank's Retail Internet Banking facility register receiver/ beneficiaries by entering the beneficiary's name, mobile number, address and his/her Pin code, which is a one-time process. These details can be subsequently deleted.

SMS

Our Bank customers can send an SMS to +919223009988 from their registered mobile number, with following details/ format –

IMT <Beneficiary Mobile Number>#<Beneficiary name>#<Beneficiary Address>#<Beneficiary Add. Pin Code>

<u>IMT Beneficiary/ Receiver Registration Deletion</u>

The receiver/ beneficiary's registration already done can be deleted by either through SMS or Bank's Retail Internet Banking. The deletion described here in does not have any impact on already initiated IMT, but will impact future IMT by sender.

Internet Banking

Login to Bank's Retail Internet Banking facility and delete receivers/ beneficiary's registration under option - View/ delete beneficiary.

SMS

Send SMS +919223009988, with following details/ format –
IMT BENC # <Beneficiary Mobile Number>

IMT Withdrawal

IMT can be withdrawn by the receiver/ beneficiary from Bank's IMT enabled ATM, as a Card less withdrawal, where in receiver / beneficiary has to provide the following details –

- Mobile number on which he or she has received the IMT details
- The Sender's Code (Communicated by Sender)
- The SMS Pin (Communicated to receiver/ beneficiary over SMS)
- The IMT amount
- Withdrawal of IMT is also notified to Sender through SMS.

Presently, partial withdrawal of an IMT is not allowed, hence IMT is to be withdrawn in full.

IMT Blocking

IMT gets blocked, in case the beneficiary/ receiver exceeds three retries to withdraw an IMT with wrong credential/ details. Once blocked, Beneficiary mobile number is marked as Blocked – i.e. s/he cannot withdraw any IMT.

IMT once blocked, gets unblocked on the immediate next day.

IMT Limits

The present limits for IMT transactions are as under:

Sender limit - Rs.10,000 per transaction (Min. Rs. 100.00 and thereof in multiple of Rs.100.00)

Beneficiary / Receiver limit – Rs. 25,000 per month

IMT Charges

For Customers – The sender will be charged of IMT fee of Rs. 25.00 (inclusive of taxes) for every IMT transaction, he or she issues to a receiver/ beneficiary. This charge shall not be reversed, in case the IMT expires or is cancelled or beneficiary/ receiver details are not provided to the Bank, as per the prescribed process. However, there shall not be any additional charges for cancellation of an IMT.
For Staff – Rs.10.00 for every IMT transaction.

IMT Validity

A life of a successful IMT is only 14 days.
The IMT cancellation/ withdrawal only during this period, post which IMT is reversed. The reversal is done for the IMT amount, by crediting the sender's account. However, IMT Charges/ fee is not reversed

Cancel IMT

The sender can cancel an unpaid IMT issued by him or her from either Bank's IMT enabled ATM or from Bank's Retail Internet Banking.

To cancel an IMT, the sender needs to select CANCEL IMT and provide the IMT Id (on ATM) / Payment Id (on Internet Banking) to cancel the IMT. The IMT Id is communicated to the sender during the initiation of the IMT transaction, while Payment Id is listed on the Cancel IMT screen on Internet Banking.

Cancellation of IMT is also notified to Sender and Beneficiary/ receiver through SMS.

Check Status

The sender can check the IMT issued by him or her either Bank's IMT enabled ATM or from Bank's Retail Internet Banking.

To check the status of an IMT, the sender needs to select Check Status by providing the IMT Id (on ATM) / Payment Id (on Internet Banking).

National Electronic Toll Collection (NETC)

National Payments Corporation of India (NPCI) has developed the National Electronic Toll Collection (NETC) program to meet the electronic tolling requirements of the Indian market. It offers an interoperable nationwide toll payment solution including clearing house services for settlement and dispute management. Interoperability, as it applies to National Electronic Toll Collection (NETC) system, encompasses a common set of processes, business rules and technical specifications which enable a customer to use their FASTag as payment mode on any of the toll plazas irrespective of who has acquired the toll plaza.

FASTag is a device that employs Radio Frequency Identification (RFID) technology for making toll payments directly while the vehicle is in motion. FASTag (RFID Tag) is affixed on the windscreen of the vehicle and enables a customer to make the toll payments directly from the account which is linked to FASTag.

FASTag offers the convenience of cashless payment along with benefits like - savings on fuel and time as the customer does not has to stop at the toll plaza.

The National Electronic Toll Collection (NETC) system has seen steady growth in the last few years. Recent mandates by the Government of India have put NETC on an exponential growth trajectory. NETC volumes were 64 million, 93 million and 110 million in the months of December 2019, January 2020 and February 2020 respectively. However, owing to the nationwide lockdown, the volumes plunged by 90% to 10 million in April 2020. After economic activity resumed in the country and restrictions on inter-state movement were lifted, the volumes gradually returned to pre COVID-19 levels, and 10 million NETC transactions were recorded in September 2020.

National Payments Corporation of India (NPCI) has developed the National Electronic Toll Collection (NETC) program to meet the electronic tolling requirements of the Indian market. It offers an interoperable nationwide toll payment solution including clearing house services for settlement and dispute management. Interoperability, as it applies to National Electronic Toll Collection (NETC) system, encompasses a common set of processes, business rules and technical specifications which enable a customer to use their FASTag as payment mode on any of the toll plazas irrespective of who has acquired the toll plaza.

Currently, NETC covers 390+ national toll highway plazas and seven state toll plazas. We believe these numbers will grow in the coming years. Further, with the emergence of many new use cases and an extended Government push on usage of FASTAGs at tolls, we expect up to twelve times growth in NETC transaction volumes by 2025.

Government push to promote NETC

- FASTag has become mandatory for all vehicles from last year. 18 million FASTags have already been issued and this number is likely to reach up to 25 million by next year.
- All vehicle manufacturers and dealers have already associated with FASTag issuers to enable new vehicles to get RFID tags.
- All national highway tolls plazas are now FASTag enabled. State highway toll plazas are also rapidly shifting to the FASTag system following the Government mandate.

Various new use cases expected-

- Fuel payments using FASTag at petrol pumps, along with purchase of foods and groceries at shops at the petrol pumps
- Various Government or private parking spaces
- Collection of police fines

With the Government's mandate and inclusion of state toll booths under NETC's purview, this can be a great revenue-generating opportunity for the entire ecosystem

Objectives of National Electronic Toll Collection system:-

To create a composite interoperable ecosystem.	Provides an interoperable secure framework capable of use across the country.
Simple and robust Framework.	It increases transparency and efficiency in processing transactions.
To serve the sub goal of Government of India.	Electronification of retail payments.
	Reduce air pollution by reducing the congestion around toll plaza.
	Reduce fuel consumption.
	Reduce cash handling.
	Enhance audit control by centralizing user account.

What is FASTag?

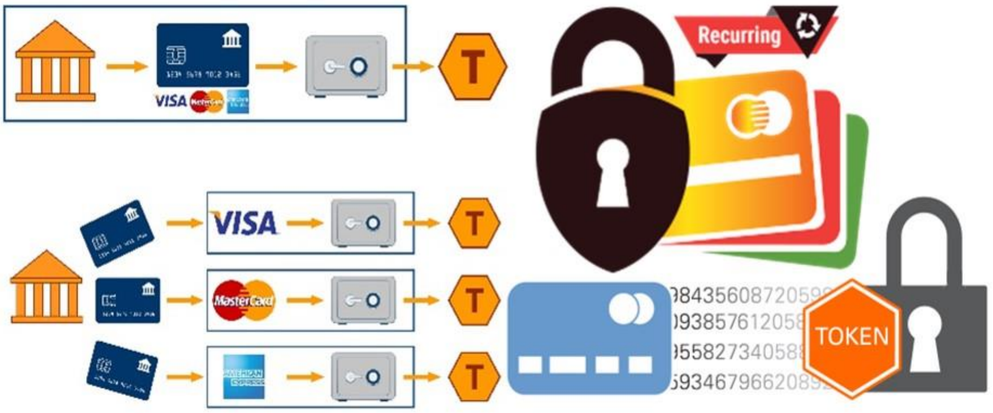
FASTag is a RFID passive tag used for making toll payments directly from the customers linked prepaid or savings/current account. It is affixed on the windscreen of the vehicle and enables the customer to drive through toll plazas, without stopping for any toll payments. The toll fare is directly deducted from the linked account of the customer. FASTag is also vehicle specific and once it is affixed to a vehicle, it cannot be transferred to another vehicle. FASTag can be purchased from any of the NETC Member Banks. If a FASTag is linked to the prepaid account, then it needs to be recharged/ topped-up as per the usage of the customer. If adequate balance is not maintained by the customer, the FASTag gets blacklisted at the toll plaza. In such a scenario if the customer travels through a toll plaza without recharging then he won't be able to avail the NETC services and would be required to pay the toll fare through cash.

Following are some of the key features and functionalities of National Electronic Toll Collection system-

Transaction Type.	Off-line; near real time transaction processing as the toll plazas send the transactions within 10 mins interval.
Interoperability.	NETC ecosystem supports multiple issuers and multiple acquirers' i.e. Tag issued by any member bank is accepted at all toll plaza (under NETC program) acquired by any member bank in a safe and secured manner.

Flexibility to choose the underlying payment instruments.	Customers can link their FASTag to their existing savings/current account or to a prepaid account basis the offering from the Issuer member banks. For opening a prepaid account it is not mandatory to have an existing relationship with the issuer bank.
Tag Issuance.	Can be issued by member banks, authorized for NETC Program.
Cashless Payment.	FASTag facilitates electronic payments at the toll plaza while the vehicle is in motion.
Save Time and Fuel.	Customer can travel without stopping at the toll plaza by using the FASTag thus reduce congestion at plazas and , saving fuel and reduce travel time.
Recharge FASTag account online.	Customer can recharge FASTag account online through issuing member banks portal using UPI/ Credit Card/ Debit Card/ NEFT/ RTGS /Net Banking.

Tokenization



A big step to enable Secured Payments: -

The Reserve Bank has today released guidelines on tokenisation for debit / credit / prepaid card transactions as a part of its continuous endeavour to enhance the safety and security of the payment systems in the country. Tokenisation involves a process in which a unique token masks sensitive card details. Thereafter, in lieu of actual card details, this token is used to perform card transactions in contactless mode at Point of Sale (POS) terminals, Quick Response (QR) code payments, etc. These guidelines permit authorized card payment networks to offer card tokenisation services to any token requestor (third party app provider), subject to conditions enumerated in these guidelines. A card holder may avail of these services by registering the card on the token requestor's app after giving explicit consent. No charges shall be recovered from the customer for availing this service.

All extant instructions of Reserve Bank on safety and security of card transactions, including mandate for Additional Factor of Authentication (AFA) / PIN entry shall be applicable for tokenised card transactions also.
Jose J. Kattoor
Chief General Manager
RBI
Press Release: 2018-2019/1597
****

Tokenisation – Card transactions

RBI/2018-19/103
DPSS.CO.PD No.1463/02.14.003/2018-19

January 08, 2019

The Chief Executive Officer / President
All authorised card payment networks

Madam / Dear Sir,

Tokenisation – Card transactions
Continuing the efforts to improve safety and security of card transactions, Reserve Bank of India had permitted card networks for tokenisation in card transactions for a specific use case.

2. It has now been decided to permit authorised card payment networks to offer card tokenisation services to any token requestor (i.e., third party app provider), subject to the conditions listed in Annex 1. This permission extends to all use cases / channels [e.g., Near Field Communication (NFC) / Magnetic Secure Transmission (MST) based contactless transactions, in-app payments, QR code-based payments, etc.] or token storage mechanisms (cloud, secure element, trusted execution environment, etc.). For the present, this facility shall be offered through mobile phones / tablets only. Its extension to other devices will be examined later based on experience gained.

3. All extant instructions of Reserve Bank on safety and security of card transactions, including the mandate for Additional Factor of Authentication (AFA) / PIN entry shall be applicable for tokenised card transactions also.

4. All other instructions related to card transactions shall be applicable for tokenised card transactions as well. The ultimate responsibility for the card tokenisation services rendered rests with the authorised card networks.
5. No charges should be recovered from the customer for availing this service.

6. Before providing card tokenisation services, authorised card payment networks shall put in place a mechanism for periodic system (including security) audit at frequent intervals, at least annually, of all entities involved in providing card tokenisation services to customers. This system audit shall be undertaken by empaneled auditors of Indian Computer Emergency Response Team (CERT-In) and all related instructions of Reserve Bank in respect of system audits shall also be adhered to. A copy of this audit report shall be furnished to the Reserve Bank, with comments of auditors on deviations, if any, from the conditions listed in Annex 1, along with the compliance thereto. Further, a report on the details provided in Annex 2 shall be submitted at monthly intervals to the Chief General Manager, Reserve Bank of India, Department of Payment and Settlement Systems, Central Office, Mumbai and by email.

7. This directive is issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

Yours faithfully,

(P Vasudevan)
Chief General Manager

Encl.: As above

Annex 1

(DPSS.CO. PD. No.1463/02.14.003/2018-19 dated January 08, 2019)

Card tokenisation services

Tokenisation refers to replacement of actual card details with a unique alternate code called the "token", which shall be unique for a combination of card, token requestor and device (referred hereafter as "identified device").

Conditions
Tokenisation – de-tokenisation service

i. Tokenisation and de-tokenisation shall be performed only by the authorised card network and recovery of original Primary Account Number (PAN) should be feasible for the authorised card network only. Adequate safeguards shall be put in place to ensure that PAN cannot be found out from the token and vice versa, by anyone except the card network. Integrity of token generation process shall be ensured at all times.

ii. Tokenisation and de-tokenisation requests should be logged by the card network and available for retrieval, if required.

iii. Actual card data, token and other relevant details shall be stored in a secure mode. Token requestors shall not store PAN or any other card detail.

Certification of systems of card issuers / acquirers, token requestors and their app, etc.

iv. Card network shall get the token requestor certified for (a) token requestor's systems, including hardware deployed for this purpose, (b) security of token requestor's application, (c) features for ensuring authorised access to token requestor's app on the identified device, and, (d) other functions performed by the token requestor, including customer on-boarding, token provisioning and storage, data storage, transaction processing, etc.

v. Card networks shall get the card issuers / acquirers, their service providers and any other entity involved in payment transaction chain, certified in respect of changes done for processing tokenised card transactions by them.

vi. All certification / security testing by the card network shall conform to international best practices / globally accepted standards.

Registration by customer

vii. Registration of card on token requestor's app shall be done only with explicit customer consent through Additional Factor of Authentication (AFA), and not by way of a forced / default / automatic selection of check box, radio button, etc.

viii. AFA validation during card registration, as well as, for authenticating any transaction, shall be as per extant Reserve Bank instructions for authentication of card transactions.

ix. Customers shall have option to register / de-register their card for a particular use case, i.e., contactless, QR code based, in-app payments, etc.

x. Customers shall be given option to set and modify per transaction and daily transaction limits for tokenised card transactions.
xi. Suitable velocity checks (i.e., how many such transactions will be allowed in a day / week / month) may be put in place by card issuers / card network as considered appropriate, for tokenised card transactions.

xii. For performing any transaction, the customer shall be free to use any of the cards registered with the token requestor app.

Secure storage of tokens

xiii. Secure storage of tokens and associated keys by token requestor on successful registration of card shall be ensured.

Customer service and dispute resolution

xiv. Card issuers shall ensure easy access to customers for reporting loss of "identified device" or any other such event which may expose tokens to unauthorised usage. Card network, along with card issuers and token requestors, shall put in place a system to immediately de-activate such tokens and associated keys.

xv. Dispute resolution process shall be put in place by card network for tokenised card transactions.

Safety and security of transactions

xvi. Card network shall put in place a mechanism to ensure that the transaction request has originated from an "identified device".

xvii. Card network shall ensure monitoring to detect any malfunction, anomaly, suspicious behavior or the presence of unauthorized activity within the tokenisation process, and implement a process to alert all stakeholders.

xviii. Based on risk perception, etc., card issuers may decide whether to allow cards issued by them to be registered by a token requestor.

Understanding Tokenization

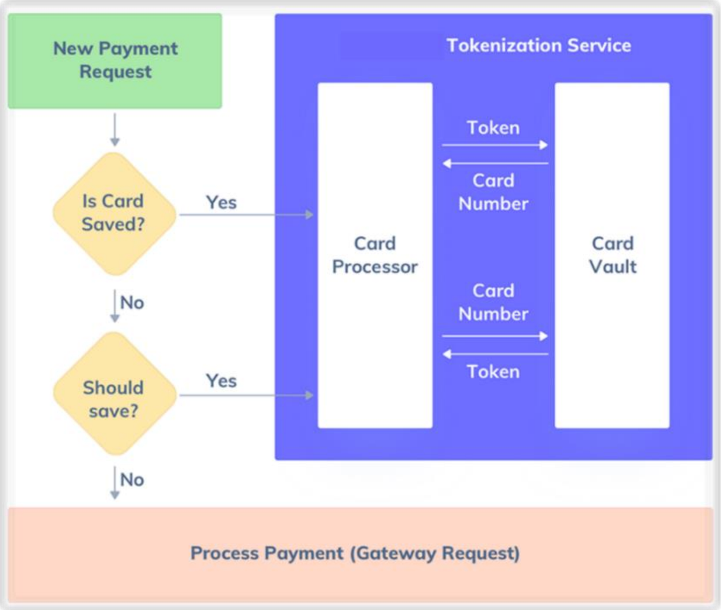
Tokenization is a process through which sensitive information or data is replaced with a unique set of characters that retain all the essential information without compromising the security of the sensitive information.

In the payments space, tokenization is the process of replacing the 16-digit payment card account number with a unique digital identifier known as a 'token' in mobile and online transactions. This token then allows payments to be processed without exposing sensitive account details that could breach security and privacy.

Substitution methods like tokenization have been around for a while as a way to separate data in ecosystems, and databases. Before tokenization was introduced, encryption with reversible cryptographic algorithms was the preferred method of protecting sensitive data. Unlike encryption, a process that encrypts cardholder data at the origin, and then decrypts it at the end destination, tokenization replaces sensitive cardholder detail with a stand-in token. Because of the random assignation of tokens, it's almost impossible to reverse-engineer or compromise a token.

Let's take a look at what happens from the time a customer uses his credit card to the time where the payment is processed, to better understand the process of tokenization.

- A credit card is swiped at a POS machine or is used for an online transaction
- The credit card number is passed to the tokenization system
- The tokenization system generates a string of 16 random characters to replace the original credit card number.
- The tokenization system returns the newly generated 16-digit random characters to the POS machine or e-commerce site to replace the customer's credit card number in the system.



<u>What a token looks like?</u>

There are two types of tokens, format preserving tokens and non-format preserving tokens.

Format preserving tokens maintain the appearance of the 16-digit credit card number.

Example:
Card number: 5945 8612 5953 6391

Format preserving token: 4111 8765 2345 1111

Non-format preserving tokens do not resemble the original credit card number and can include both alpha and numeric characters.

There are specific format-preserving tokenization schemes which maintain the IIN (first 6 digits) as well as the last 4 digits of the card number.

Example:
Card number: 5945 8612 5953 6391
Non-format preserving token: 25c92e17-80f6-415f-9d65-7395a32u0223

What is the impact of tokenization on online businesses?

Credit card tokenization helps online businesses improve their data security, from the point of data capture to storage as it eliminates the actual storage of credit card numbers in the POS machines and internal systems. But the greatest benefit of tokenization is that it minimizes the impact of security breaches for merchants.

Since merchants are storing tokens instead of credit card numbers in their systems, hackers will acquire tokens which are of no use to them. Breaches are expensive, and many retailers and banks have experienced huge losses as a result of data theft. Tokenization helps minimize this.

What is the impact of tokenization on customers?

Apart from the comfort that comes with knowing that your credit card is less likely to get hacked, there's also the fact that tokenization is very convenient for customers in the case of fraud or theft. This works because of the fact that multiple tokens are issued for the same card payment on different platforms that use tokenization.

So even if a website you use gets breached and the tokens are acquired by the hacker/miscreant, it's difficult to reverse engineer the actual card number from it as access to the tokenization logic will also be needed.

Does using tokenization make you PCI DSS compliant?

Storing tokens instead of credit card numbers is one alternative that can help to reduce the amount of cardholder data in the environment, potentially reducing the merchant's effort to implement PCI DSS (Payment Card Industry Data Security Standard) requirements.

The following key principles relate to the use of tokenization and its relationship to PCI DSS:

- Tokenization solutions do not eliminate the need to maintain and validate PCI DSS compliance, but they may simplify a merchant's validation efforts by reducing the number of system components for which PCI DSS requirements apply.
- Verifying the effectiveness of a tokenization implementation is necessary and includes confirming that a financial card number is not retrievable from any system component removed from the scope of PCI DSS.
- Tokenization systems and processes must be protected with strong security controls and monitoring to ensure the continued effectiveness of those controls.

- Tokenization solutions can vary greatly across different implementations, including differences in deployment models, tokenization and de-tokenization methods, technologies, and processes.

Both tokenization and encryption are widely used today to protect sensitive data stored in cloud services or internal applications. An organization can decide to use encryption, tokenization or a mix of both depending on their use case. This also depends on the different types of data that the organization wants to secure.

(Source – RBI & Razorpay)

BlockChain

First and foremost, Blockchain is a public electronic ledger - similar to a relational database - that can be openly shared among disparate users and that creates an unchangeable record of their transactions, each one time-stamped and linked to the previous one. Each digital record or transaction in the thread is called a block (hence the name), and it allows either an open or controlled set of users to participate in the electronic ledger. Each block is linked to a specific participant.

The block chain is seen as the main technical innovation of bitcoin, where it serves as the public ledger of all bitcoin transactions. Bitcoin is peer-to-peer, every user is allowed to connect to the network, send new transactions to it, verify transactions, and create new blocks, which is why it is called permissionless. This original design has been the inspiration for other cryptocurrencies and distributed databases."

Think of a situation where a bank's know-your-customer (KYC) check on a corporate customer fails to show up a suspicious transaction done by the company with another bank. What if banks could share and also monetise corporate KYCs, including investigation reports and cross-border wire transfer reports, on a real-time basis, on a secure, private, immutable and consensus-based shared digital ledger?

Similarly, how much simpler would life become for a manufacturing company mired in input credit claims under the goods and services tax (GST) if its system automatically generated and shared pre-reconciled invoices with all its suppliers over a seamless and secure cryptographic ledger that is replicated and synchronised? This could help the company save hundreds of crores of rupees stuck in working capital currently.

Thirty banks and non-banking finance companies (NBFCs) in India and the Middle East including State Bank of India, ICICI Bank, Axis Bank and Yes Bank, are set to share corporate KYCs and more through BankChain - a blockchain consortium set up by financial technology firm Primechain Technologies. BankChain, now rechristened Primechain Money, is going live with five blockchain platforms that include cross-border remittances and peer-to-peer money transfers, and the banks should start using them real-time from February 2018. Besides, IBM is working on an invoice management blockchain solution for manufacturing companies to tackle their GST woes.

Like their global counterparts, Indian companies and financial institutions are rapidly taking to blockchain - the indelible ledger technology that became popular for powering the digital cryptocurrency bitcoin. And, they're realising that there's more to it than bitcoin or the other cryptocurrencies of its ilk, because of its inherent advantages of privacy, security, consensus and transparency. The record created on the ledger cannot be tampered with. They are encrypted and decrypted using cryptographic public and private keys, and a member/ company can only access records relevant to it. If a record is changed in one place, it has to be changed everywhere.

APIs

Application programming interfaces (APIs) is relatively an old technical composition, which has been around for a long time. It is a structured and predetermined mechanism where two systems can exchange data with each other. Essentially APIs were internally focused and were exposed externally only in a very private manner or only to pre-identified partners. Open APIs is a combination of API technology and contemporary thinking about open collaboration. It refers to new dialogues, connections, and ways of working between participants in emerging business ecosystems.

This composition is used widely these days by a lot of organizations in different fields and one such looming field is financial services and the emerging trend in the financial ecosystem which uses APIs is open banking technology (FinTech). It is based on using application programming interfaces (APIs) that enable third-party developers to build applications and services around a financial institution (FI). It facilitates greater financial transparency and helps financial institutions to innovate and create new revenue models. With the changing regulatory mandates, open banking has been gaining significant momentum across the globe.

This shift towards open banking APIs is also driven by regulations like PSD2 in Europe, the Monetary Authority of Singapore and the CMA in the UK, and these aim at fostering greater collaboration among financial institutions. Regulations like PSD2 mandates banks to open themselves, and the accounts of their customers, to external parties creating different types of new market participants thereby providing customers with more services. Effectively, the open bank API will allow for unbundling as well as bundling of traditional banks' services by smart aggregators, be it non-bank competitors or other banks.

Today's banks traditionally own their products, distribution and customer base and have a monopoly on their customer's account information and services. While fintech's have been able to develop some innovative approaches that accesses the huge client base of the banks, but it has been a challenge, whilst getting access to a bank's data and functionality. The introduction of API in the banking service would give both customers and businesses the freedom to access all bank data in real-time, and basically providing them with more accurate and up to date information on their finances.

The new regulations like PSD2 will further spin the ball forward in terms of creating a more open banking environment. It will encourage competition and create an opportunity for new products and services in this domain and this could be one of the biggest and most transformational changes to hit banking since the advent of the Internet.

Currently, many small and medium-sized enterprises use commercial software for accounting purposes, but for the most part, these businesses have to add their daily transaction data manually. The introduction of API in the banking service would give both customers and businesses the freedom to access all bank data in real-time, and basically providing them with more accurate and up to date information on their finances. With this push, customers will be able to draw a clear comparison and save on their accounts and have access to more personalized resources for making sturdy banking decisions. In addition to this, customers will have access to better loan terms as lenders would then have access to historic transactional data to determine a borrower's risk level.

An open API ecosystem will have to function on more layers than a bank-to-consumer model and function as distributed economy, especially with scrunched up applications where data can move in any direction. While this open API ecosystem provides the required flexibility, it also increases the risk of cyberattacks. Cyber threats are more sophisticated today than ever and they are engineered to steal the data and assets from the organization or even cause a major business disruption. Two key things for enterprises opening their API to the internet to keep in mind are understanding the ecosystem and ensuring right levels of data encryption and access methodologies are used alongside providing only required control to the API consumers.

These new developments will further spin the ball forward in terms of creating a more open banking environment. It will encourage competition and create an opportunity for new products and services in this domain and this could be one of the biggest and most transformational changes to hit banking since the advent of the Internet.

As of now, we're still at the early stages of a new era in API-driven payments revolution. Banks, fintech companies, and merchants have so much to learn. This technology is not only a new way to meet compliance obligations, but it also represents a new way of doing business that must be embraced with open arms and put to work.

AI (Artificial Intelligence's)

Digital solution providers state that one robot can work 24/7 and replace up to eight employees, without asking for days off or a raise. This is the major reason why big global banks are increasingly turning toward Artificial Intelligence (AI) technologies to stay competitive in the digital era.

AI has huge benefits, for both banks and their customers. The implications of AI disruption in the financial sector is that the analysis of users' habits, activities, behavioral characteristics, and financial data products can be customized to meet and anticipate each user's unique and evolving needs. This makes it viable for each user to have his/her own digital personal financial assistant.

The banking and financial sectors are slowly moving from the first digital age to the second. AI, cloud computing, mobile-first and digital dashboards are already the norm, and new technologies are being adopted.

These are the most relevant application areas of Artificial Intelligence technology in banking and finance:

<u>Personalized Financial Services</u>

Automated financial advisors and planners assist users in taking financial decisions. They monitor events, stock and bond price trends against the user's financial goals and personal portfolio, and offer recommendations regarding stocks and bonds to buy or sell.

Smart Wallets

Digital wallets are billed in most tech circles as the future of real-world payment technologies. With major players like Google, Apple, PayPal and others jumping on the bandwagon and developing their own mobile-first payment technologies, it appears to be a safe bet.

Underwriting

The insurance sector is utilizing AI systems that automate the underwriting process and provide more granular information to take better decisions.

Voice Assisted Banking

This technology empowers customers to use banking services with voice commands rather than a touch screen. The natural language technology can process queries to answer questions, find information, and connect users with various banking services.

Data-driven AI applications for lending decisions

Applications embedded in end user devices, personal robots, and financial institution servers are capable of analyzing massive volumes of information, providing customized financial advice, calculations and forecasts. These applications can also develop financial plans and strategies, and track their progress. This includes research regarding various customized investment opportunities, loans, rates, fees, etc.

Customer support

As speech processing and natural language processing technologies mature, we are drawing closer to the day, when computers could handle most customer service queries. This would mark an end to waiting in line and hence result in happier customers.

New Management Decision-making

Data-driven management decisions at low cost could lead to a new style of management, where future banking and insurance leaders would ask right questions to machines, rather than to human experts, which would analyze data and come up with recommended decisions that leaders and their subordinates would use and motivate their workforce to execute.

Reducing Fraud and Fighting Crime

Most industries operating on the World Wide Web are susceptible to fraudulent users and the banking industry is no exception. This has led to an arms race between online security providers and fraudsters involved in everything from email scams to credit card frauds. As security providers improve, criminals change their ways. AI tools, which learn and monitor behavioral patterns of users to identify anomalies and warning signs of fraud attempts and occurrences, along with collection of evidence necessary for conviction, are also becoming more commonplace in fighting crime.

According to a Gartner study, by 2020, consumers will manage 85% of the total business associations with banks through chatbots. Banks can offer advice on a large scale and with better impact by using AI chatbots that can learn about customer's user habits. These engines can refer to the data from the past about user transactions, offerings, credit card usage, investment strategies, fund management pattern, etc., and make the recommendation to the user based on the same aligned with best banking practices.

Banks can benefit from artificial intelligence models which can be done by taking input from several financial market sources and offer trading platforms based on the automated artificial intelligence systems.

Cyber Security / Crime / Attack, Computer Virus – Info. Sec. etc...

In general cybercrime may be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime".

Below is a list for some of the cybercrimes along with their indicative explanation.

Cyber Bullying

A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc.

Cyber stalking

Cyber stalking is the use of electronic communication by a person to follow a person, or attempts to contact a person to foster personal interaction repeatedly despite a clear indication of disinterest by such person; or monitors the internet, email or any other form of electronic communication commits the offence of stalking.

Cyber Grooming

Cyber Grooming is when a person builds an online relationship with a young person and tricks or pressures him/ her into doing sexual act.

Online Job Fraud

Online Job Fraud is an attempt to defraud people who are in need of employment by giving them a false hope/ promise of better employment with higher wages.

Vishing

Vishing is an attempt where fraudsters try to seek personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

Smshing

Smishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

SIM Swap Scam

SIM Swap Scam occurs when fraudsters manage to get a new SIM card issued against a registered mobile number fraudulently through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through victim's bank account. Getting a new SIM card against a registered mobile number fraudulently is known as SIM Swap.

Debit/Credit Card Fraud

Credit card (or debit card) fraud involves an unauthorized use of another's credit or debit card information for the purpose of purchases or withdrawing funds from it.

Impersonation and Identity Theft

Impersonation and identity theft is an act of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person.

Phishing

Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source.

Spamming

Spamming occurs when someone receives an unsolicited commercial messages sent via email, SMS, MMS and any other similar electronic messaging media. They may try to persuade recepient to buy a product or service, or visit a website where he can make purchases; or they may attempt to trick him/ her into divulging bank account or credit card details.

Ransomware

Ransomware is a type of computer malware that encrypts the files, storage media on communication devices like desktops, Laptops, Mobile phones etc., holding data/information as a hostage. The victim is asked to pay the demanded ransom to get his device decrypts.

Virus, Worms & Trojans

Computer Virus is a program written to enter to your computer and damage/alter your files/data and replicate themselves.

Worms are malicious programs that make copies of themselves again and again on the local drive, network shares, etc.

A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.

Data Breach

A data breach is an incident in which information is accessed without authorization.

Denial Of Services /Distributed DoS

Denial of Services (DoS) attack is an attack intended for denying access to computer resource without permission of the owner or any other person who is in-charge of a computer, computer system or computer network.

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Website Defacement

Website Defacement is an attack intended to change visual appearance of a website and/ or make it dysfunctional. The attacker may post indecent, hostile and obscene images, messages, videos, etc.

Cyber-Squatting

Cyber-Squatting is an act of registering, trafficking in, or using a domain name with an intent to profit from the goodwill of a trademark belonging to someone else.

Pharming

Pharming is cyber-attack aiming to redirect a website's traffic to another, bogus website.

Cryptojacking

Cryptojacking is the unauthorized use of computing resources to mine cryptocurrencies.

Online Drug Trafficking

Online Drug Trafficking is a crime of selling, transporting, or illegally importing unlawful controlled substances, such as heroin, cocaine, marijuana, or other illegal drugs using electronic means.

Espionage

Espionage is the act or practice of obtaining data and information without the permission and knowledge of the owner.

BANK
1234 5678
Credit Card
CYBER DOST

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

SECURE ONLINE
Financial services!

Be Cautious...

With the growth of information and communication technology, the structure and nature of financial services delivery has also changed. Online banking or internet banking has emerged as a new and convenient way for using financial services like funds transfer, viewing account statement, bill payment, use of e-wallets etc.

An upsurge in the use of devices connected with the internet and the convenience of online financial services has increased the risk of our hard-earned money being duped by cybercriminals of our hard-earned money.

<u>Following tips may be adhered for safe online transactions:</u>

1. Never disclose your net banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number, expiry date to anyone, even if they claim to be from your bank. Also, never respond to mails asking for above details which seem to have received from your bank.

2. No bank or its employees will ever call or email you requesting for your net banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number, etc. Such cases should be immediately reported to your bank.

3. Always use strong passwords and prefer separate ID/password combinations for different accounts to prevent anyone from guessing them.

4. Periodically change passwords of your online banking accounts.

5. To make passwords strong, use alphabets in upper case and lower case, numbers and special characters. Do not use passwords such as Jan@2018, admin@123, password@123, your date of birth etc

6. Always use virtual keyboards while logging into online banking services. This is specially adhered in-case you need to access net banking facility from a public computer/ cyber café or a shared computer.

7. Do not make financial transaction over shared public computers or while using public Wi-Fi networks. These computers might have key loggers installed which are designed to capture input from keyboards and could enable fraudsters to steal your username and password.

8. Always remember to log off from your online banking portal/ website after completing an online transaction with your credit/ debit card.

9. Always delete the browsing data of your web browser (Internet Explorer, Chrome, Firefox etc.) after completing your online banking activity.

10. To make passwords strong, use alphabets in upper case and lower case, numbers and special characters. Do not use passwords such as Jan@2018, admin@123, password@123, your date of birth etc.

11. Always use virtual keyboards while logging into online banking services. This is specially adhered in-case you need to access net banking facility from a public computer/ cyber café or a shared computer.

12. Do not make financial transaction over shared public computers or while using public Wi-Fi networks. These computers might have key loggers installed which are designed to capture input from keyboards and could enable fraudsters to steal your username and password.

13. Always remember to log off from your online banking portal/ website after completing an online transaction with your credit/ debit card.

14. Always delete the browsing data of your web browser (Internet Explorer, Chrome, Firefox etc.) after completing your online banking activity.

15. Always be sure about the correct address of the bank website and look for the "lock" icon on the browser's status bar while visiting your bank's website or conducting an online transaction. Always be sure "https" appears in the website's address bar before making an online transaction. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted.

16. Login and view your bank account activity regularly to make sure that there are no unexpected transactions. Report any discrepancies in your account to your bank immediately.

17. Keep your bank's customer care number handy so that you can report any suspicious or unauthorized transactions on your account immediately.

18. It is easy for cyber criminals to send convincing emails which appear to be from your bank. Don't click on the links provided in such emails even if they look genuine. They could lead you to malicious websites.

19. Whenever you receive a credit/ debit card from the bank, make sure the letter is not damaged and it is sealed properly. In-case, there are any signs of tampering with the package, please notify your bank immediately.

20. Make sure to change the PIN of credit/ debit card after receiving a new card from your bank. The PIN can be changed online by visiting your bank's website or at your nearest ATM machine.

21. Always ensure that credit or debit card swipes at point of sale are done in your presence to avoid cloning/unauthorized copying of your card information. Do not let the sales person take your card away to swipe for the transaction.

22. Take extra precaution while typing your password/PIN so that no one sees it. Try to cover the key-pad with your other hand while you type your PIN to avoid the number being picked up by someone monitoring CCTV footage.

23. Register your personal phone number with your bank and subscribe to mobile notifications. These notifications will alert you quickly of any suspicious transaction and the unsuccessful login attempts to your netbanking account.

24. Always review transaction alert received on your registered mobile number and ensure that your transaction is billed according to your purchase.

25. Keep an eye on the people around you while transacting at an ATM. Make sure that no one is standing too close to you while you transact at an ATM.

26. It is necessary that you keep your PIN secret and close your transaction completely before walking away from the ATM machine. If there is anything suspicious, cancel your transaction and walk away immediately.
27. Enable international transaction option on your credit card only when you are travelling abroad. Always ensure to disable international transaction option on your card upon return to your country.

28. Fraudsters may call your family members posing as hospital staff and may request for money transfer saying that you have met an accident and you are in urgent need of money. This could be a spam. Before entertaining any such request, contact your family member to confirm their whereabouts and check authenticity of the phone call.

29. Check for latest updates of your Smartphones operating system if you are using your mobile phone for online banking. Do install an antivirus as well and keep it up-to date by enabling the automatic update feature.

30. Always ignore an advertisement if it claims that you can earn money with little or no work or you can make money on an investment with little or no

risk. It could be a scam. These offers seem, too good to be true, and you may end up losing money.

31. Always use familiar websites for online shopping rather than shopping by searching products on search engines. Search results can be misleading and may lead to malicious websites.

32. Avoid using third-party extensions, plugins or add-ons for your web browser as it may secretly track your activity and steal your personal details.

33. Always verify and install authentic e-wallet apps directly from the app store on your smartphone. Do not follow links shared over email, SMS or social media to install e-wallet apps.

34. Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.

35. Always type the information in online forms and not use the auto-fill option on your web-browser to fill your online forms they may store your personal information such as card number, CVV number, bank account number etc.

Source – National Cyber Crime Reporting Portal
To get cyber safety tips - Twitter Handle @CyberDost
National Cyber Crime Reporting Portal - www.cybercrime.gov.in

Importance Of Cyber Security

Why is Cyber Security Awareness Important?

Advanced technologies have changed the modern way of life. The internet provides us with many benefits. Be it communicating with friends, searching for information, doing banking transactions, availing online services, finding job, finding life partner or even running entire businesses. The internet touches almost all aspects of our lives. However, it also makes us vulnerable to a wide range of threats.

New and powerful cyber-attacks are striking the internet regularly. A minor lapse in managing our digital lives can open the door to cyber criminals. Cyber criminals can steal our money or damage our reputation. According to a study by a leading industry research organization, 90% of all cyber-attacks are caused by human negligence. Therefore, cyber security awareness is important for everyone today.

We must be vigilant while making use of technology to reduce the risk of cyber threats.

Types of Cybercrime

A cybercrime is a crime involving computers and networks. This includes a wide range of activities, from illegally downloading music files to stealing money from online bank accounts. Cyber criminals are not always financially motivated. Cybercrimes include non-monetary offenses as well. It can include frauds such as job related frauds, matrimonial frauds; stealing and misusing sensitive personal information (Aadhaar details, credit/debit card details, bank account credentials, etc.); defamation of an individual on social media; distribution of computer viruses etc. Cybercrimes can also lead to physical or sexual abuse.

IDENTITY THEFT

PSYCHOLOGICAL TRICKS

SOCIAL MEDIA FRAUDS

MOBILE APPLICATION FRAUDS

ONLINE BANKING FRAUDS

VIRUS ATTACK ON PERSONAL COMPUTER

IDENTITY THEFT

Identity theft is the act of wrongfully obtaining someone's personal information (that defines one's identity) without their permission. The personal information may include their name, phone number, address, bank account number, Aadhaar number or credit/debit card number etc.

Identity theft can have many adverse effects. The fraudster can use stolen personal information and identity proofs to:

- gain access to your bank accounts

- apply for loans and credit cards or open insurance accounts
- file a tax refund in your name and get your refund
- obtain a driver's license, passport or immigration papers
- create new utility accounts
- get medical treatment on your health insurance
- assume your identity on social media
- give your name to the police during an arrest etc.

Hence, everyone should be aware about identity theft and should know how to prevent it. Let us look at some examples of identity theft.

Hacking or gaining access to Social Media Accounts
The attacker hacks or gains access to the social media account of the victim. The attacker can then harm the victim by misusing their personal information and photographs. The attacker can also post offensive content on victim's profile or defame the victim.

Misuse of photo copies of identity proofs
The attacker misuses the photo copies of identity proofs of the victim. These can be PAN Card, Aadhaar Card or any other identity proof of the victim. The attacker can use these photo copies to steal money or cause harm to the victim.

Credit/Debit Card Skimming
Credit/Debit card skimming is done using a small device called skimmer. The magnetic stripe of the card stores details such as name, credit/debit card number and expiration date. First, the credit/debit card is swiped through a skimmer. Then, the skimmer captures all these details. Thieves use this stolen data to make online transactions. They also use this data to create duplicate credit/debit cards and withdraw money from ATM.

PSYCHOLOGICAL TRICKS

Psychological tricks are where attackers play with the minds of the user to trap them with lucrative offers. Once trapped, the attackers can exploit the victim by either stealing money or stealing sensitive personal information (name, Aadhaar details, bank account details etc.) or harm the victim in any other way. The entire basis of this kind of attack is to make the victim fall into their trap by sending fake e-mails, calls or SMSs.

Phishing is the act of sending fraudulent e-mail that appears to be from a legitimate source, for example, a bank, a recruiter or a credit card company etc. This is done in an attempt to gain sensitive personal information, bank account details etc. from the victim.

Vishing is similar to phishing. But, instead of e-mail, in this type of crime, the fraudster uses telephone to obtain sensitive personal and financial information.

Smishing is the SMS equivalent of phishing. It uses SMS to send fraudulent text messages. The SMS asks the recipient to visit a website/weblink or call a phone number. The victim is then tricked into providing sensitive personal information, debit/credit card details or passwords etc.

Phishing, Vishing and Smishing are done in an attempt to steal money from the victim or cause any other harm to the victim.

Let us look at some examples of psychological tricks.

Lottery Fraud

The fraudster congratulates the victim for winning a handsome lottery via e-mail/call/SMS. The victim is delighted and is eager to get the lottery money. The fraudster asks the victim to transfer a token amount and share vital personal information to get the lottery money. The victim loses his/her money and does not get anything in return.

Credit/Debit Card Fraud

The attacker tries to scare the victim by informing them that their credit/debit card has been blocked. The victim becomes worried and starts panicking. The attacker takes advantage of this situation and asks victim to provide sensitive personal information to re-activate the card. This information is then misused to steal money or cause harm to the victim.

Job Related Fraud

The attacker sends a fake e-mail to the victim offering a job with an attractive salary. The victim, unfortunately, believes it and follows the instructions. The attacker then steals the money or harms the victim physically.

SOCIAL MEDIA FRAUDS

Social Media has become an integral part of our lives. It is the new way of communicating, sharing and informing people about the events in our lives. We share our day to day lives on social media in the form of self and family photographs, updates on our locations/whereabouts, our views/thoughts on prevalent topics etc. One can understand the entire history of an individual through their social media profile and can even predict future events based on patterns in the past.

This poses a threat to an individual as unwanted access to social media profile can cause loss of information, defamation or even worse consequences such as physical/sexual assault, robbery etc. Hence, protection and appropriate use of social media profile is very important.

Let us look at some examples of social media frauds.

Sympathy Fraud

The attacker becomes friends with the victim on social media. The attacker gains trust by frequent interactions. The attacker later extracts money/harms the victim.

Romance Fraud

The attacker becomes friends with the victim on social media. Over a period, the attacker gains victim's affection. The attacker later exploits the victim physically, financially and/or emotionally.

Cyber Stalking

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail, instant messaging (IM), messages posted on a website or a discussion group.A cyber stalker relies upon the fact that his/her true identity is not known in the digital world. A cyber stalker targets the victim with threatening/abusive messages and follows them/their activities in the real world.

Cyber Bullying

Cyber bullying is bullying that takes place over digital devices. Cyber bullying can occur through SMS, social media, forums or gaming apps where people can view, participate or share content. Cyber bullying includes sending, posting or sharing negative, harmful, false content about someone else. The intention is to cause embarrassment or humiliation. At times, it can also cross the line into unlawful criminal behavior.

MOBILE APPLICATION FRAUDS

With the increase in the use of smartphones and the consequent rise in the use of mobile applications, associated security risks have also increased. The number of mobile transactions has increased four times in the last couple of years, and now, cyber criminals are targeting mobile users to extract data and money.

Mobile applications are widely used not only for entertainment but also for ease and convenience to perform day-to-day tasks such as bill payments, bank accounts management, service delivery etc. As a result, these applications are more prone to cyber-attacks. Users need to be aware of such attacks on commonly used mobile applications such as digital payment applications and gaming applications.

Let us look at some day to day example on how mobile applications can be used for cyber frauds.

Cyber-attacks using Infected Mobile Applications

People become habitual users of certain mobile applications. As a result, they ignore security warnings. Fraudsters use this to attack the victim by infiltrating through such popular mobile applications. They infect the applications with malicious software, called Trojan. This Trojan can get access to your messages, OTP, camera, contacts, e-mails, photos etc. for malicious activities. It can also show obscene advertisements, sign users up for paid subscriptions or steal personal sensitive information from the mobile etc.

ONLINE BANKING FRAUDS

Nowadays, all banking services are shifting online. Services like retrieving account statement, funds transfer to other accounts, requesting a cheque book, preparing demand draft etc. can all be done online. Most of these services can be done sitting at home without physically visiting the bank. As the services are shifting towards online platforms, cyber frauds related to banking are also increasing. Just like we protect our locker full of jewelry with a lock and key, we must protect our online bank accounts with strong passwords. If the key is stolen, then the jewelry will be stolen. Similarly, if the password is stolen, then the money in the bank accounts will be stolen. Hence, protection of bank accounts with strong passwords becomes highly essential.

Let us look at some examples of online banking fraud.

Digital Payments Applications related attacks
Digital payments have become very common in today's life. However, they do pose a threat if the account is hacked.

Hacking of Bank Account due to Weak Password
In this type of attack, the attacker hacks into the victim's account by using a program to guess commonly used passwords. Once the account is hacked, the attacker can steal money or perform an illegal transaction in order to defame or frame the victim.

Hacking of Multiple Accounts due to same password
If same password is used for multiple accounts, then hacking of one account may also lead to hacking of other accounts.

VIRUS ATTACK ON PERSONAL COMPUTER

Personal Computers or laptops play a very important role in our lives. We store our crucial information such as bank account numbers, business documents etc. in the computer. We also store personal files like photos, music, movies etc. in the computer. Therefore, protection of all this data is highly essential. Just as we keep a physical lock on our safe vaults, it is equally important to protect our valuable data from viruses/malicious applications that can damage it.

Let us look at some examples on how our personal computer can get affected by virus.

Virus Attack through external devices
A virus can enter the computer through external devices like pen drive or hard disk etc. This virus can spread across all the computer files.

Virus Attack by downloading files from un-trusted websites
The virus can enter the computer by download of files from un-trusted websites. The virus can be hidden in the form of music files, video files or any attractive advertisement. This virus can spread across all the computer files.

Virus Attack by installation of malicious software
The virus can enter into the computer by installing software from un-trusted sources. The virus can be an additional software hidden inside unknown game files or any unknown software. This virus can spread across all the computer files.

A Virus/Malicious application can cause various harms such as slowing down the computer, lead to data corruption/deletion or data loss.

Most Common Types of Cyber Attacks

(Source - netwrix.com)

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

Unlike attacks that are designed to enable the attacker to gain or increase access, denial-of-service doesn't provide direct benefits for attackers. For some of them, it's enough to have the satisfaction of service denial. However, if the attacked resource belongs to a business competitor, then the benefit to the attacker may be real enough. Another purpose of a DoS attack can be to take a system offline so that a different kind of attack can be launched. One common example is session hijacking, which I'll describe later.

There are different types of DoS and DDoS attacks; the most common are TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and botnets.

TCP SYN flood attack

In this attack, an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker's device floods the target system's small in-process queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to time out while waiting for the response from the attacker's device, which makes the system crash or become unusable when the connection queue fills up.

There are a few countermeasures to a TCP SYN flood attack:

- Place servers behind a firewall configured to stop inbound SYN packets.
- Increase the size of the connection queue and decrease the timeout on open connections.

Teardrop attack

This attack causes the length and fragmentation offset fields in sequential Internet Protocol (IP) packets to overlap one another on the attacked host; the attacked system attempts to reconstruct packets during the process but fails. The target system then becomes confused and crashes.

If users don’t have patches to protect against this DoS attack, disable SMBv2 and block ports 139 and 445.

Smurf attack

This attack involves using IP spoofing and the ICMP to saturate a target network with traffic. This attack method uses ICMP echo requests targeted at broadcast IP addresses. These ICMP requests originate from a spoofed “victim” address. For instance, if the intended victim address is 10.0.0.10, the attacker would spoof an ICMP echo request from 10.0.0.10 to the broadcast address 10.255.255.255. This request would go to all IPs in the range, with all the responses going back to 10.0.0.10, overwhelming the network. This process is repeatable, and can be automated to generate huge amounts of network congestion.

To protect your devices from this attack, you need to disable IP-directed broadcasts at the routers. This will prevent the ICMP echo broadcast request at the network devices. Another option would be to configure the end systems to keep them from responding to ICMP packets from broadcast addresses.

Ping of death attack

This type of attack uses IP packets to ‘ping a target system with an IP size over the maximum of 65,535 bytes. IP packets of this size are not allowed, so attacker fragments the IP packet. Once the target system reassembles the packet, it can experience buffer overflows and other crashes.

Ping of death attacks can be blocked by using a firewall that will check fragmented IP packets for maximum size.

Botnets

Botnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks. These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system’s bandwidth and processing capabilities. These DDoS attacks are difficult to trace because botnets are located in differing geographic locations.

Man-in-the-middle (MitM) attack

A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Here are some common types of man-in-the-middle attacks:

Session hijacking

In this type of MitM attack, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client. For instance, the attack might unfold like this:

- A client connects to a server.
- The attacker’s computer gains control of the client.
- The attacker’s computer disconnects the client from the server.
- The attacker’s computer replaces the client’s IP address with its own IP address and spoofs the client’s sequence numbers.
- The attacker’s computer continues dialog with the server and the server believes it is still communicating with the client.

IP Spoofing

IP spoofing is used by an attacker to convince a system that it is communicating with a known, trusted entity and provide the attacker with access to the system. The attacker sends a packet with the IP source address of a known, trusted host instead of its own IP source address to a target host. The target host might accept the packet and act upon it.

Replay

A replay attack occurs when an attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants. This type can be easily countered with session timestamps or nonce (a random number or a string that changes with time).

Currently, there is no single technology or configuration to prevent all MitM attacks. Generally, encryption and digital certificates provide an effective safeguard against MitM attacks, assuring both the confidentiality and integrity of communications. But a man-in-the-middle attack can be injected into the middle of communications in such a way that encryption will not help — for example, attacker "A" intercepts public key of person "P" and substitute it with his own public key. Then, anyone wanting to send an encrypted message to P using P's public key is unknowingly using A's public key. Therefore, A can read the message intended for P and then send the message to P, encrypted in P's real public key, and P will never notice that the message was compromised. In addition, A could also modify the message before resending it to P. As you can see, P is using encryption and thinks that his information is protected but it is not, because of the MitM attack.

So, how can you make sure that P's public key belongs to P and not to A? Certificate authorities and hash functions were created to solve this problem. When person 2 (P2) wants to send a message to P, and P wants to be sure that A will not read or modify the message and that the message actually came from P2, the following method must be used:

- P2 creates a symmetric key and encrypts it with P's public key.
- P2 sends the encrypted symmetric key to P.
- P2 computes a hash function of the message and digitally signs it.
- P2 encrypts his message and the message's signed hash using the symmetric key and sends the entire thing to P.
- P is able to receive the symmetric key from P2 because only he has the private key to decrypt the encryption.
- P, and only P, can decrypt the symmetrically encrypted message and signed hash because he has the symmetric key.
- He is able to verify that the message has not been altered because he can compute the hash of received message and compare it with digitally signed one.
- P is also able to prove to himself that P2 was the sender because only P2 can sign the hash so that it is verified with P2 public key.

Phishing and spear phishing attacks

Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.

Spear phishing is a very targeted type of phishing activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against. One of the simplest ways that a hacker can conduct a spear phishing attack is email spoofing, which is when the information in the "From" section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company. Another technique that scammers use to add credibility to their story is website cloning — they copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials.

To reduce the risk of being phished, you can use these techniques:

- **Critical thinking** — Do not accept that an email is the real deal just because you're busy or stressed or you have 150 other unread messages in your inbox. Stop for a minute and analyze the email.
- **Hovering over the links** — Move your mouse over the link, but do not click it! Just let your mouse cursor h over over the link and see where would actually take you. Apply critical thinking to decipher the URL.
- **Analyzing email headers** — Email headers define how an email got to your address. The "Reply-to" and "Return-Path" parameters should lead to the same domain as is stated in the email.
- **Sandboxing** — You can test email content in a sandbox environment, logging activity from opening the attachment or clicking the links inside the email.

Drive-by attack

Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike many other types of cyber security attacks, a drive-by doesn't rely on a user to do anything to actively enable the attack — you don't have to click a download button or open a malicious email attachment to become infected. A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack of updates.

To protect yourself from drive-by attacks, you need to keep your browsers and operating systems up to date and avoid websites that might contain malicious code. Stick to the sites you normally use — although keep in mind that even these sites can be hacked. Don't keep too many unnecessary programs and apps on your device. The more plug-ins you have, the more vulnerabilities there are that can be exploited by drive-by attacks.

Password attack

Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person’s password can be obtained by looking around the person’s desk, ‘‘sniffing’’ the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing. The last approach can be done in either a random or systematic manner:

- **Brute-force** password guessing means using a random approach by trying different passwords and hoping that one work Some logic can be applied by trying passwords related to the person’s name, job title, hobbies or similar items.
- In a **dictionary attack**, a dictionary of common passwords is used to attempt to gain access to a user’s computer and network. One approach is to copy an encrypted file that contains the passwords, apply the same encryption to a dictionary of commonly used passwords, and compare the results.

In order to protect yourself from dictionary or brute-force attacks, you need to implement an account lockout policy that will lock the account after a few invalid password attempts. You can follow these account lockout best practices in order to set it up correctly.

SQL injection attack

SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for example, instead of the login or password) in order to run predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system.

For example, a web form on a website might request a user’s account name and then send it to the database in order to pull up the associated account information using dynamic SQL like this:

“SELECT * FROM users WHERE account = ‘“ + userProvidedAccountNumber +”’;”

While this works for users who are properly entering their account number, it leaves a hole for attackers. For example, if someone decided to provide an account number of “‘ or ‘1’ = ‘1’”, that would result in a query string of:

“SELECT * FROM users WHERE account = ‘’ or ‘1’ = ‘1’;”

Because ‘1’ = ‘1’ always evaluates to TRUE, the database will return the data for all users instead of just a single user.
The vulnerability to this type of cyber security attack depends on the fact that SQL makes no real distinction between the control and data planes. Therefore, SQL injections work mostly if a website uses dynamic SQL. Additionally, SQL injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. J2EE and ASP.NET applications are less likely to have easily

exploited SQL injections because of the nature of the programmatic interfaces available.

In order to protect yourself from a SQL injection attacks, apply least0privilege model of permissions in your databases. Stick to stored procedures (make sure that these procedures don't include any dynamic SQL) and prepared statements (parameterized queries). The code that is executed against the database must be strong enough to prevent injection attacks. In addition, validate input data against a white list at the application level.

Cross-site scripting (XSS) attack

XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website's database. When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script. For example, it might send the victim's cookie to the attacker's server, and the attacker can extract it and use it for session hijacking. The most dangerous consequences occur when XSS is used to exploit additional vulnerabilities. These vulnerabilities can enable an attacker to not only steal cookies, but also log key strokes, capture screenshots, discover and collect network information, and remotely access and control the victim's machine.

Eavesdropping attack

Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network. Eavesdropping can be passive or active:

- Passive eavesdropping — A hacker detects the information by listening to the message transmission in the network.
- Active eavesdropping — A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.

Detecting passive eavesdropping attacks is often more important than spotting active ones, since active attacks requires the attacker to gain knowledge of the friendly units by conducting passive eavesdropping before.

Data encryption is the best countermeasure for eavesdropping.

Birthday attack

Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature. A message processed by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message; this MD uniquely characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user's message with his, and the receiver will not be able to detect the replacement even if he compares MDs.

Malware attack

Malicious software can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet. Here are some of the most common types of malware:

- **Macro viruses** — These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.
- **File infectors** — File infector viruses usually attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded. Another version of a file infector associates itself with a file by creating a virus file with the same name, but an .exe extension. Therefore, when the file is opened, the virus code will execute.
- **System or boot-record infectors** — A boot-record virus attaches to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.
- **Polymorphic viruses** — These viruses conceal themselves through varying cycles of encryption and decryption. The encrypted virus and an associated mutation engine are initially decrypted by a decryption program. The virus proceeds to infect an area of code. The mutation engine then develops a new decryption routine and the virus encrypts the mutation engine and a copy of the virus with an algorithm corresponding to the new decryption routine. The encrypted package of mutation engine and virus is attached to new code, and the process repeats. Such viruses are difficult to detect but have a high level of entropy because of the many modifications of their source code. Anti-virus software or free tools like Process Hacker can use this feature to detect them.
- **Stealth viruses** — Stealth viruses take over system functions to conceal themselves. They do this by compromising malware detection software so that the software will report an infected area as being uninfected. These viruses conceal any increase in the size of an infected file or changes to the file's date and time of last modification.
- **Trojans** — A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers. For example, a Trojan can be programmed to open a high-numbered port so the hacker can use it to listen and then perform an attack.
- **Logic bombs** — A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.
- **Worms** — Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. Worms are commonly spread through email attachments; opening the attachment activates the worm program. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address In addition to conducting malicious activities, a

worm spreading across the internet and overloading email servers can result in denial-of-service attacks against nodes on the network.

- **Droppers** — A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.
- **Ransomware** — Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.
- **Adware** — Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically.
- **Spyware** — Spyware is a type of program that is installed to collect information about users, their computers or their browsing habits. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.

Juice jacking

When your battery is dying and you're nowhere near a power outlet, would you connect your phone to any old USB port? Joyce did, and her mobile phone got infected. How? Through a type of cyberattack called "juice jacking." Don't be like Joyce.

The term juice jacking was first coined in 2011 after researchers created a compromised charging kiosk to bring awareness to the problem. When people plugged in their phones, they received a security warning and learned their phones had paired to the kiosk.

If you're stuck somewhere with a dying smartphone battery, you may not think twice about plugging in at the nearest USB charging station.

Not so fast. Warnings of juice jacking may cause to you to reconsider.

It could be that someone has loaded malware on the USB port or the USB cable attached to one of these public charging stations. While your phone is charging, the perpetrator might be able to infect your device with a virus or malware that could track your keystrokes or even steal your data. That's juice jacking.

Juice jacking does not yet appear to be widespread threat, but it's still a good idea to understand your risks and alternatives before giving your battery a boost at public charging stations like those at airports or hotels.

How juice jacking works

Whether you have an iPhone, BlackBerry, or an Android device, smartphones have one thing in common: The power supply and the data stream pass through the same cable.

This could spell trouble. When your phone connects to another device, it pairs to that device and establishes a trusted relationship. That means the devices can share information. So during the charging process, the USB cord opens a pathway into your device that a cybercriminal may be able to exploit.

On most phones, the data transfer is disabled by default (except on devices running older Android versions), and the connection is only visible on the end that provides the power.

For instance, when you plug your phone into your computer, a message on the computer may ask whether to trust the device.

In the case of juice jacking, the device owner won't see what the USB port connects to. So when you plug in the phone, if someone's checking on the other end, they may be able to move data between your device and theirs.

Types of juice jacking

There are two ways juice jacking could work:

- **Data theft**: During the charge, data is stolen from the connected device.

  When a device is plugged into the public USB port, a cybercriminal could have compromised that port and enabled malware to infect your plugged-in device. This could potentially allow someone to steal the data on your mobile device.

  Using a crawler program on your device, a cybercriminal could then search for personally identifiable information, account credentials, and financial information.

  If the perpetrator can transfer that data onto their device, it might be enough personal information to impersonate you or access your financial accounts.

- **Malware installation**: As soon as the connection is established, malware is dropped on the connected device. The malware remains on the device until it is detected and removed by the user.

  Cybercriminals may use a malware app to clone your phone data and transfer it back to their own device. Other malware may help them gather data such as your GPS location, purchases, social media interactions, photos, and call logs.

  Some types of malware include adware, cryptominers, spyware, Trojans, or ransomware. Once your device is frozen or encrypted with one of these types of malware, the cyber-thief may demand payment to restore the information.

GENERAL TIPS TO KEEP YOU SAFE

1. Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches.

2. Protect systems/devices through security software such as anti-virus with the latest version.

3. Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.

4. Ensure all devices/accounts are protected by a strong PIN or passcode. Never share your PIN or password with anyone.

5. Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.

6. Always change the default admin password on your Wi-Fi router to a strong password known only to you. In addition, always configure your wireless network to use the latest encryption (contact your network service provider, in case of any doubt).

7. Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.

8. Always use virtual keyboard to access net-banking facility from public computers; and logout from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Internet Explorer, Chrome, Firefox etc.) after completion of online banking activity.

9. Do scan all e-mail attachments for viruses before opening them. Avoid downloading e-mail attachments received in e-mails from unknown or un-trusted sources.

10. Be careful while sharing identity proof documents especially if you cannot verify the authenticity of the company/person with whom you are sharing information.

11. Note the IMEI code of your cell phone and keep it in a safe place. The operator can blacklist/block/trace a phone using the IMEI code, in case the cell phone is stolen.

12. Observe your surroundings for skimmers or people observing your PIN before using an ATM.

13. Discuss safe internet practices and netiquettes with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.

14. Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.

15. If you think you are compromised, inform authorities immediately.

INCIDENT REPORTING

1. Visit the nearest police station immediately.
2. To report cybercrime complaints online, visit the National Cyber Crime Reporting Portal. This portal can be accessed at https://cybercrime.gov.in/. In this portal, there are two sections. One section is to report crimes related to Women and Children (where reports can be filed anonymously as well). Another section is to report other types of cybercrimes. You can also file a complaint offline by dialing the helpline number 155260.
3. In case you receive or come across a fraud sms, e-mail, link, phone call asking for your sensitive personal information or bank details, please report it on Maharashtra Cyber'sweb portal by visiting www.reportphishing.in
4. Refer to the latest advisories which are issued by CERT-IN on https://www.cert-in.org.in/
5. Report any adverse activity or unwanted behavior to CERT-IN using following channels
   E-mail: incident@cert-in.org.in
   Helpdesk: +91 1800 11 4949
   Provide following information (as much as possible) while reporting an incident.
   - Time of occurrence of the incident
   - Information regarding affected system/network
   - Symptoms observed
6. To report lost or stolen mobile phones, file a First Information Report (**FIR**) with the police. Post filing the FIR, inform Department of Telecommunications (**DoT**) through the helpline number **14422** or file an online compliant on **Central Equipment Identity Register**(**CEIR**) portal by visiting https://ceir.gov.in. After verification, DoT will blacklist the phone, blocking it from further use. In addition to this, if anyone tries to use the device using a different SIM card, the service provider will identify the new user and inform the police.

(Source - https://cybercrime.gov.in)

Computer Virus

A computer virus is "malware attached to another program (such as a document), which can replicate and spread after an initial execution on a target system where human interaction is required. Many viruses are harmful and can destroy data, slow down system resources, and log keystrokes."

Most computer viruses target systems running Microsoft Windows. Macs, on the other hand, enjoy a reputation as virus-proof super machines. In reality, Macs are not inherently safer. There are more Windows users in the world than Mac users and cybercriminals simply choose to write viruses for the operating system (OS) with the largest amount of potential victims.

Whatever OS you choose, Windows or Mac, don't worry too much, because viruses just aren't a thing anymore. That may sound odd coming from a cybersecurity company but hear us out.

Cybercriminals aren't creating new viruses, instead they are focusing their efforts on more sophisticated and lucrative threats. When people talk about "getting a virus" on their computer, they usually mean some form of malware—often a computer worm.

The terms "virus" and "malware" are often used interchangeably, but they're not the same thing. While a computer virus is a type of malware, not all malware are computer viruses.

The easiest way to differentiate computer viruses from other forms of malware is to think about viruses in biological terms. Take the flu virus, for example. The flu requires some kind of interaction between two people—like a hand shake, a kiss, or touching something an infected person touched. Once the flu virus gets inside a person's system it attaches to healthy human cells, using those cells to create more viral cells.

A computer virus works in much the same way:

- A computer virus requires a host program.
- A computer virus requires user action to transmit from one system to another.
- A computer virus attaches bits of its own malicious code to other files or replaces files outright with copies of itself.

It's that second virus trait that tends to confuse people. Viruses can't spread without some sort of action from a user, like opening up an infected Word document. Worms, on the other hand, are able to spread across systems and networks on their own, making them much more prevalent and dangerous.

Famously, the 2017 WannaCry ransomware worm spread around the world, took down thousands of Windows systems, and raked in an appreciable amount of untraceable Bitcoin ransom payments for the alleged North Korean attackers.

Computer viruses don't capture headlines like that—at least not anymore.
To recap, the bad guys aren't focused on creating new viruses and most of the really bad stuff is actually malware. Should we still take computer viruses seriously? Definitely, yes.

Continuing the virus analogy, if a given population stops receiving vaccinations for diseases thought to be eradicated, like the measles and polio, those diseases can and do come back. Likewise, it's important to be proactive about cybersecurity and take some basic protective measures against computer viruses. Otherwise, computer viruses could make a comeback.

With that said, let's take a look at computer viruses under the microscope.

Computer virus examples

Sometimes to understand what something is, we have to examine what it isn't. Keeping that in mind, let's play: Is It a Virus?

In the Is It a Virus game we're going to take a look at examples of things people on the Internet commonly believe to be a virus and explain why it is or isn't. What fun!

Is a Trojan a virus?

Trojans can be viruses. A Trojan is a computer program pretending to be something it's not for the purposes of sneaking onto your computer and delivering some sort of malware. To put it another way, if a virus disguises itself then it's a Trojan. A Trojan could be a seemingly benign file downloaded off the web or a Word doc attached to an email. Think that movie you downloaded from your favorite P2P sharing site is safe? What about that "important" tax document from your accountant? Think twice, because they could contain a virus.

Is a worm a virus?

Worms are not viruses, though the terms are sometimes used interchangeably. Even worse, the terms are sometimes used together in a strange and contradictory word salad; i.e. a "worm virus malware." It's either a worm or a virus, but it can't be both, because worms and viruses refer to two similar but different threats. As mentioned earlier, a virus needs a host system to replicate and some sort of action from a user to spread from one system to the next. A worm, conversely, doesn't need a host system and is capable of spreading across a network and any systems connected to the network without user action. Once on a system, worms are known to drop malware (often ransomware) or open a backdoor.

Is ransomware a virus?

Ransomware can be a virus. Does the virus prevent victims from accessing their system or personal files and demands ransom payment in order to regain access à la ransomware? If so, then it's a ransomware virus. In fact, the very first ransomware was a virus (more on that later). Nowadays, most ransomware comes as a result of computer worm, capable of spreading from one system to the next and across networks without user action (e.g. WannaCry).

Is a rootkit a virus?

Rootkits are not viruses. A rootkit is a software package designed to give attackers "root" access or admin access to a given system. Crucially, rootkits cannot self-replicate and don't spread across systems.

Is a software bug a virus?

Software bugs are not viruses. Even though we sometimes refer to a biological virus as a "bug" (e.g. "I caught a stomach bug"), software bugs and viruses are not the same thing. A software bug refers to a flaw or mistake in the computer code that a given software program is made up of. Software bugs can cause programs to behave in ways the software manufacturer never intended. The Y2K bug famously caused programs to display the wrong date, because the programs could only manage dates through the year 1999. After 1999 the year rolled over like the odometer on an old car to 1900. While the Y2K bug was relatively harmless, some software bugs can pose a serious threat to consumers. Cybercriminals can take advantage of bugs in order to gain unauthorized access to a system for the purposes of dropping malware, stealing private information, or opening up a backdoor. This is known as an exploit.

How do I prevent computer viruses?

Preventing computer viruses from infecting your computer starts with situational awareness.

"Situational awareness is something law enforcement and militaries have practiced for decades. It refers to a police officer or a soldier's ability to perceive threats and make the best decision possible in a potentially stressful situation," said Malwarebytes Head of Security, John Donovan.

"As it applies to cybersecurity, situational awareness is your first line of defence against cyber threats. By staying on the lookout for phishing attacks and avoiding suspicious links and attachments, consumers can largely avoid most malware threats."

Regarding email attachments and embedded links, even if the sender is someone you know: viruses have been known to hijack Outlook contact lists on infected computers and send virus laden attachments to friends, family and coworkers, the Melissa virus being a perfect example.

If an email reads oddly, it's probably a phishing scam or malspam. When in doubt about the authenticity of an email, don't be afraid to reach out to the sender. A simple call or text message can save you a lot of trouble.

Next, invest in good cybersecurity software. We've made a distinction between computer viruses and malware, which now begs the question, "Do I need antivirus software or anti-malware software?" We've covered this topic before in great detail so checkout our article on antivirus vs. anti-malware. For now, though, here's a quick gloss on the subject.

Antivirus (AV) refers to early forms of cybersecurity software focused on stopping computer viruses. Just viruses. Anti-malware refers to all-encompassing threat protection designed to stop old-fashioned viruses as well as today's malware threats. Given a choice between traditional AV with limited threat detection technology and modern anti-malware with all the bells and whistles, invest in anti-malware and rest easy at night.

As mentioned previously in this piece, traditional AV solutions rely on signature-based detection. AV scans your computer and compares each and every file against a database of known viruses that functions a lot like a criminal database. If there's a signature match, the malicious file is thrown into virus jail before it can cause any damage.

The problem with signature-based detection is that it can't stop what's known as a zero-day virus; that is, a virus that cybersecurity researchers have never seen before and for which there is no criminal profile. Until the zero-day virus is added to the database, traditional AV can't detect it.

How do I remove computer viruses?
Going back to our virus analogy one final time—removing a virus from your body requires a healthy immune system. Same for your computer. A good anti-malware program is like having a healthy immune system. As your immune system moves through your body looking for and killing off invading viral cells, anti-malware scans for files and malicious code that don't belong on your system and gets rid of them.

Malware

Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems.

Hostile, intrusive, and intentionally nasty, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations. Like the human flu, it interferes with normal functioning.

Malware is all about making money off you illicitly. Although malware cannot damage the physical hardware of systems or network equipment, it can steal, encrypt, or delete your data, alter or hijack core computer functions, and spy on your computer activity without your knowledge or permission.

Most common offenders in the rogues' gallery of malware:

- **Adware** is unwanted software designed to throw advertisements up on your screen, most often within a web browser. Typically, it uses an underhanded method to either disguise itself as legitimate, or piggyback on another program to trick you into installing it on your PC, tablet, or mobile device.
- **Spyware** is malware that secretly observes the computer user's activities without permission and reports it to the software's author.
- A **virus** is malware that attaches to another program and, when executed—usually inadvertently by the user—replicates itself by modifying other computer programs and infecting them with its own bits of code.
- **Worms** are a type of malware similar to viruses, self-replicating in order to spread to other computers over a network, usually causing harm by destroying data and files.
- A **Trojan**, or Trojan horse, is one of the most dangerous malware types. It usually represents itself as something useful in order to trick you. Once it's on your system, the attackers behind the Trojan gain unauthorized access to the affected computer. From there, Trojans can be used to steal financial information or install threats like viruses and ransomware.
- **Ransomware** is a form of malware that locks you out of your device and/or encrypts your files, then forces you to pay a ransom to get them back. Ransomware has been called the cyber criminal's weapon of choice because it demands a quick, profitable payment in hard-to-trace cryptocurrency. The

code behind ransomware is easy to obtain through online criminal marketplaces and defending against it is very difficult.

- **Rootkit** is a form of malware that provides the attacker with administrator privileges on the infected system. Typically, it is also designed to stay hidden from the user, other software on the system, and the operating system itself.
- A **Keylogger** is malware that records all the user's keystrokes on the keyboard, typically storing the gathered information and sending it to the attacker, who is seeking sensitive information like usernames, passwords, or credit card details.
- **Malicious cryptomining**, also sometimes called drive-by mining or cryptojacking, is an increasingly prevalent malware usually installed by a Trojan. It allows someone else to use your computer to mine cryptocurrency like Bitcoin or Monero. So instead of letting you cash in on your own computer's horsepower, the cryptominers send the collected coins into their own account and not yours. Essentially, a malicious cryptominer is stealing your resources to make money.
- **Exploits** are a type of malware that takes advantage of bugs and vulnerabilities in a system in order to allow the exploit's creator to take control. Among other threats, exploits are linked to malvertising, which attacks through a legitimate site that unknowingly pulls in malicious content from a bad site. Then the bad content tries to install itself on your computer in a drive-by download. No clicking is necessary. All you have to do is visit a good site on the wrong day.

<u>How to get rid of a computer virus</u>

In this section, we explore how to get rid of a computer virus from a PC and from a Mac.

Removing a computer virus from a PC

Computer viruses are almost always invisible. Without anti-virus protection, you may not know you have one. This is why it is vital to install anti-virus protection on all your devices.

If your PC has a virus, following these ten simple steps will help you to get rid of it:

Step 1: **Download and install a virus scanner**

Step 2: Disconnect from internet

When you are removing a virus from your PC, it is a good idea to disconnect from the internet to prevent further damage: some computer viruses use the internet connection to spread.

Step 3: **Reboot your computer into safe mode**

To protect your computer while you remove the virus, reboot it in 'Safe Mode'. Are you unsure of how to do this?

Here is a simple guide:

- Turn your computer off and on again

- When the screen lights, press F8 to bring up the 'Advanced boot options' menu
- Click 'Safe Mode with Networking'
- Remain disconnected from the internet

Step 4: Delete any temporary files
Next, you need to delete any temporary files using 'Disk Clean Up'.

Here's how to do this:

- Click the Windows logo on the right bottom
- Type "Temporary Files"
- Choose "Free up disk space by deleting unnecessary files"
- Find and select "Temporary Internet Files" in the 'Files to delete' Disk Cleanup list and click OK
- Confirm "Delete Files" selection

Some viruses are programmed to initiate when your computer boots up. Deleting temporary files may delete the virus. However, it is not safe to rely on this. To ensure you rid your computer of viruses, it is wise to complete the following steps.

Step 5: **Run a virus scan**
Now it is time to run a virus scan using your chosen anti-virus or internet security software.

Step 6: Delete or quarantine the virus
If a virus is found, it may affect multiple files. Select 'Delete' or 'Quarantine' to remove the file(s) and get rid of the virus. Rescan your computer to check there's no further threats. If threats are found, quarantine or delete the files.

Step 7: Reboot your computer
Now that the virus is removed, you can reboot your computer. Simply turn it on as you would normally. It no longer needs to be in 'Safe Mode'.

Step 8: Change all your passwords
To protect your computer from further attack, change all your passwords in case they were compromised. This is only strictly necessary if you have reason to believe your passwords have been captured by malware, but it is better to be safe than sorry.

You can always check the virus's functionality on your anti-virus vendor's website or with their technical support team if unsure.
Step 9: Update your software, browser and operating system
Updating your software, browser and operating system will reduce the risk of flaws in old code being exploited by criminals to install malware on your computer.

Antivirus and Firewall

Key Difference: Antivirus or anti-virus software is a software that is used to prevent viruses from entering the computer system and infecting files. Many antivirus programs these days also eliminate different kinds of malware in addition to viruses. Firewall software is a software that controls the incoming and outgoing network traffic by analyzing the number of data packets that is sent. Firewall is a hardware based network security system that works based on a rule set. It works to protect between private and public networks

Antivirus and Firewall software are two different methods of protecting the computer from infectious malicious software. Antivirus works by scanning the computer to detect and remove already infected files and also prevents from viruses from affecting any files. Firewall software comes built in but can also be added separately works to make making networks secure to keep malicious software to enter into the computer using a network connection.

Just as it has become quite easy to find everything online, it has also become the best place to target people for personal information. There are many different malware that are looking out to harm the computer system or collect private data about the user. Fear not, there are companies that have built software and programs that can protect the user’s system. These are known as Antivirus and Antimalware software.

Antivirus or anti-virus software is a software that is used to prevent viruses from entering the computer system and infecting files. Many antivirus programs these days also eliminate different kinds of malware in addition to viruses. The main purpose of an antivirus software is to scan, detect, prevent and remove many different kinds of software. The software employs a variety of strategies to detect viruses including searching for known patterns of data within executable code. However, the computer is still vulnerable against new types of viruses that may use different codes.

In order to counter this, many antivirus programs use heuristics, which is a technique that is designed to solve a problem more quickly than a classic method. This is done by creating an approximate solution when the classical solution fails. Initially, only executable files were corrupted or infected with viruses but with the new viruses, many files could also become infected requiring antivirus programs to manually search all files and folders that are available in the system. There are also drawbacks to having antivirus programs such as false-positive. This is when the antivirus program detects a non-malicious file as a virus and deletes it from the system. If the file is an important file, it could cause the operating system to stop working or certain applications to crash. Hence, files should be reviewed before they are deleted from the system.

Firewall software is a software that controls the incoming and outgoing network traffic by analyzing the number of data packets that is sent. Firewall is a hardware based network security system that works based on a rule set. According to "internet Security: FIREWALLS and BEYOND, “A network's firewall builds a bridge between the internal network or computer it protects, upon securing that the other network is secure and trusted, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.” These days, many computers and routers come with built in firewalls that protect the computer from treats on the internet.

The term firewall was originally used to describe a wall that is responsible for confining a fire to one particular room or building. This terminology was later adapted to refer to the current firewall technology that we have. The firewall technology emerged in the late 1980s, with the first paper on firewalls being published in 1988. Firewalls were developed in three generations: packet filters, ‘stateful’ filters and application layer. The first generation worked by examining packets and if a packet does not match the packet filter’s rules, it would automatically drop the packet or reject it and send error notifications. The ‘stateful’ filters performs the function of a first-generation processor and retains the packet until enough information is available to make a judgment about its state. The application layer filter can also understand certain applications and protocols to detect and reject connection from certain applications.

There are various different types of firewalls depending on where the communication is taking place, where it is intercepted and the state that is being traced. These include Network layer or packets filter, Application-layer, proxies and network address translation. The packet layer operates at a low level of the TCP/IP protocol stack and monitors incoming and outgoing packets. The application layer works on the application level of the TCP/IP layer monitors packets transference between applications or application and the internet. A proxy server acts as a firewall by allowing certain packets in the manner of an application and rejecting all other packets. Network address translation is more of a functionality of many firewalls that hides the true address of the protected hosts.

IT Security

Information security: sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. it is a general term that can be used regardless of the form the data may take (e.g. electronic, physical)

Information security:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
- Unintentional errors and omissions
- IT disruptions due to natural or man-made disasters
- Failure to exercise due care and diligence in the implementation and operation of the IT system.

Internet security, Computer security, Mobile security, Network security

Cybercrime:

- Identity theft
- Cyberterrorism
- Online harassment

Virus Protection

- The Active directory components shall have antivirus/anti-malware software installed.
- The Virus/Malware signature on Active directory shall be updated regularly.
- The Active Directory Components shall be hardened as per the secure configuration documents approved by the bank.
- The Active directory components shall be updated periodically with necessary system patches.

Do’s and Don’ts

Risk	DOs	DON'Ts
1. Computer/Data Usage		
• Loss of data • Compromise security policies • Misuse of data	• Be accountable for your IT assets and data • Adhere to Policy on Use of IT Services and Facilities. • Use good judgment to protect your data • Protect your laptop during trip • Ensure sensitive information on the computer screen is not visible to others • Protect your user ID and password	• Don’t store sensitive information in portable device without strong encryption • Don’t leave your computer / sensitive documents unlocked • Don’t discuss something sensitive in public place. People around you may be listening to your conversation
2. Surfing Web		
• Virus • Worms • Trojan • Spyware • Malware	• Validate the website you are accessing • Install personal Firewall • Be cautious if you are asked for personal information • Use encryption to protect sensitive data transmitted over public networks and the Internet • Install anti-virus, perform scheduled virus scanning and keep virus signature up-to-date • Apply security patching timely • Backup your system and data, and store it securely	• Don't download data from doubtful sources • Don't visit untrustworthy sites out of curiosity, or access the URLs provided in those websites • Don't use illegal software and programs • Don't download programs without permission of the copyright owner or licensee (e.g. the use of BT software)
3. Email		
• Junk mail • Spam mail • Virus	• Do scan all email attachments for viruses before opening them • Use email filtering software • Only give your email address to people you know • Use digital signature to send emails for proving who you are	• Don’t open email attachments from unknown sources • Don't send mail bomb, forward or reply to junk email or hoax message • Don’t click on links embedded in spam mails • Don’t buy things or make charity donations in

• Identity theft	• Check the terms and disclaimers of an e-shopping site before acquiring its service • Choose well-known or trustworthy e-shopping sites • Check the trustworthiness of the e-commerce website (e.g. checking the SSL certificate) • Use strong password, and change your password on a regular basis • Logout immediately after you finished your e-shopping activities • Retain and review your transaction records • Use different passwords for bank accounts, university accounts and external accounts	• Don't make any e-shopping transactions using computers in Internet cafe • Don't visit untrustworthy sites out of curiosity • Don't use easily-guessed password, such as HKID card number, phone number, date of birth • Don't share your IDs with others

5. Public Terminals		
• Account Access • Information Loss	• Always reboot when starting to use the public PCs • Clean up cache files after use	• Don't leave without closing all browsers and logging out from the public PCs • Don't let others watch over your shoulder while logging in or doing online transactions

USB Storage Device Security

Do's

- Always do low format for first time usage.
- Always delete the drive securely to clear the contents.
- Always scan USB disk with latest Antivirus before accessing.
- Protect your USB device with a password.
- Encrypt the files / folders on the device.
- Use USB security products to access or copy data in your USB.
- Always protect your documents with strong password.

Don'ts

- Do not accept any promotional USB device from unknown members.
- Never keep sensitive information like username/passwords on USB disk.

The 10 Most Dangerous Things You should avoid doing Online

1. Opening attachments from unknown senders.
2. To open any unsolicited/suspicious mail.
3. Installing unauthorized applications
4. Disabling security tools like anti-virus and/or firewall.
5. Leaving computer in an unsecured or unattended area.
6. Sharing of passwords
7. Wireless networks without password.

8. Filling in web forms and registration pages from Cyber café
9. Posting of information on social networking sites.
10. Surfing unsure sites is always dangerous and you may be a Victim of Identity Theft.

To prevent **identity theft** avoid disclosing any information pertaining to oneself to unknown party's.

Always **avoid sending any photograph online** particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

Always keep **back up volumes** so that one may not suffer data loss in case of virus contamination

Never send your credit card number to any **site that is not secured**, to guard against frauds.

Mobile Security

- Wi – Fi Practices
- Apps
- Browsing
- Root Access
- Anti Virus

Branch Manager

Branch manager is responsible for maintaining security of information systems located in the branch. Manager also supervises security responsibilities of personnel working in the Bank including branch administrator and system users.

Responsibilities

- Promote acceptable system usage amongst the end users in the branch as per the acceptable usage policy.

- Direct and control activities of branch administrator to ensure security responsibilities are fulfilled.

- Nominate a user control officer for overseeing user creation and privileges for applications in use in the branch.

- Approve Internet access and email access for users in the Bank.

Branch System Administrator

Branch system administrator is responsible for security of IT infrastructure in the branch and provides security services related to desktops, Internet access and antivirus to branch users.

Responsibilities

- Ensuring that anti-virus software is applied to all the machines in the branch and antivirus signature updates are regularly occurring.

- Submitting anti-virus status report to the central antivirus team on a monthly basis, if the branch is not on network.

- Applying security patches and hot fixes on user machines and branch server as provided by central antivirus team and application owners.

- Maintain detailed documentation of branch network and IT asset inventory.

- Allocate / Modify privileges for new users in branch applications based on approval.

- Perform backup operations of branch servers as per schedule determined by application owner and labelling and securing backup media.

- Identifying and reporting security incidents to ISO and assisting in any preliminary analysis of incidents.

- Ensure only authorized software and licensed copy is installed on all machines in the branch.

ASSISTANCE MAY BE TAKEN FROM ZONAL IT DEPT. TO UNDERTAKE THE JOBS

- Users of IT systems All users of IT system in the Bank are required to use the systems in responsible manner.

- These responsibilities are outlined in "Acceptable Usage" policy of the Bank.

5P MANTRA

1. PRECAUTION
2. PREVENTION
3. PROTECTION
4. PRESERVATION
5. PERSEVERANCE (Do not give up)

Do's and Don'ts while browsing

Do's

- Install and use a firewall, pop-up blocker and spyware detector. Maintain the logs.
- Ensure that Anti-Virus is up to date.
- Run anti-virus and spyware detectors/cleaners regularly.
- Habitually download security protection update patches & Keep your browser and operating system up to date
- Make Backups of Important Files and Folders.
- Use strong passwords (alphanumeric and special characters) - Easy to remember and difficult to guess. Change administrator's password from the default password.
- Use a variety of passwords, not same for all of your account.
- Disconnect internet connection when not in use
- Make the wireless network invisible by disabling identifier broadcasting. If the wireless network does not have a default password, create one and use it to protect the network.
- Disable file sharing on computers.

- Avoid online banking, shopping, entering credit card details, etc if the network is not properly secured.
- Check your online account frequently and make sure all listed transactions are valid.
- Be extremely wary of spam legitimate looking email asking for confidential information. Never ever click on the link given in the spam email.
- Always delete spam emails immediately and empty the trash box to prevent accidental clicking on the same link.
- Be wary of websites that require your card details up front before you actually place an order.
- Never respond to text messages from someone you don't know.
- Open email attachment carefully.
- Be careful while downloading any free software or screensaver etc.
- Not delete email in question, save the email and take out the full header of the such email and report the crime.
- Be cautious when dealing with individuals not known to you or outside of your own country.
- Be cautious of unsolicited offers. Never purchase anything advertised through an unsolicited email.
- Beware of promises to make fast profits. Be cautious of exaggerated claims of possible earnings or profits.
- Beware of lotteries that charge a fee prior to delivery of your prize .
- Always type website addresses yourself rather than clicking on a link provided.

Don’t

- Expose yourself that you are not available in town or give your details about location and itinerary when email auto responder enabled.
- Hand over your credit card to any person.
- Auto-connect to open Wi-Fi (wireless fidelity) networks
- Get confused, frightened or pressured into divulging information if you receive an e-mail purporting to be from your bank or credit card provider as criminal use scare tactics.
- Keep passwords stored on your computer.
- To go online without virus protection and a firewall in place.
- Open email attachment if you are not sure about it.
- Provide any information like Your real name, home address, your phone number, your friends' or family members' private information, your passwords to anonymous chat friend

Do’s and Don’ts for Credit / ATM cum Debit card

DO’s

- Always keep your cards in safe and secured place.
- Always make sure contact numbers of your bank is readily available with you. Take diary note of your card numbers for any time reference.
- Always keep the card’s PIN safe by Memorizing. Choose a strong PIN code (alfa numeric) , which is not easy to guess. Change the PIN number frequently.
- If anything makes you uncomfortable during the ATM transaction, hit the cancel button.
- Always request for a receipt of a transaction.

- Be especially cautious using ATMs at night. If the machine is poorly lit avoid it.
- Observe the ATM site and make sure no one is lingering nearby. Cover the keypad while keying in your PIN.
- Always leave the ATM only after the transaction is fully completed.
- Always ensure the card is swiped in front of you at all times.
- Always register your mobile number at the branch to get SMS alerts.
- Always inform for change of address to the Bank promptly.
- Always follow the guidelines which are issued by Bank.

DON'Ts

- Don't accept the card if it is damaged or seal is broken.
- Don't expose the card to excessive heat or keep close to a magnetic field.
- Don't list the PIN on your Debit or Credit card.
- Don't disclose your Card PIN to anyone.
- Don't carry around extra credit cards that you rarely use.
- Don't hand over the card to anyone, even if he/she claims to represent the Bank.
- Don't take help from strangers while using ATM machine.
- Don't provide your card information on a website that is not a secured site.
- Don't access net banking for payment using your credit/debit card from shared or unprotected computers in public places.
- Don't share credit and debit card details on social networking sites or blogs.
- Do not reveal personal details and card numbers in response to attractive-sounding schemes from suspicious callers.
- Don't share your PIN, card number, Date of birth and CVV2 to anyone.

Do's and Don'ts for Internet Banking

DO's

- Always keep your Internet banking password and transaction password secret.
- Always keep a unique password and keep changing it regularly.
- Always set password that is easy to remember but difficult to guess.
- Ensure that no one is watching you when you are entering password.
- Always use Virtual keyboard for typing user id and password.
- Always check website address of your bank before login.
- Always click the padlock on the status bar and ensure that it has valid certificate pertaining to your bank.
- Check your account statement regularly.
- Refrain from accessing your bank account at public places like cyber café.
- Always update your web browser and enable phishing filter.
- Always ensure that your computer has Antivirus and Anti Spyware installed and it is updated.
- Log off completely from your on-line banking website, close the browser and log off your PC, when not in use.
- Follow our advice and guidelines given on our website

DON'Ts

- Never disclose internet banking username, password, on phone call or email.
- Never leave the PC unattended while using internet banking.

- Don't open multiple tabs in your browser windows and keep them inactive for long time.
- Don't reply to an email or pop-up message that asks for personal information like password, login to Internet Banking or PIN. Bank will never demand such sensitive information. You may call the bank to know the factual position.
- Never download/install/run programs/files from untrusted sources.
- Don't click on any link which has come through unknown sources.
- Don't access the Internet Banking website through a link from another website or a link in an e-mail.
- In case you smell anything fishy, call and confirm from our Bank before you act as requested.

Do's and Don'ts for Mobile Banking

DO's

- Set up a strong Pin/password to access the handset menu on your mobile phone.
- Change Mobile banking Pin/password periodically.
- Register for SMS alerts to keep track of your banking transactions.
- Install an effective mobile anti-malware/anti-virus software on your smartphone and keep it updated
- Keep your mobile's operating system and applications, including the browser, updated with the latest security patches and upgrades.
- Clear temporary files stored in the memory as they may contain your sensitive information when you send your mobile for repair/maintenance.
- Turn off wireless device services such as Wi-Fi and Bluetooth, when they are not being used.
- Log out from online mobile banking or application as soon as you have completed your transactions. Also make sure you close that window.
- Contact Bank in case of loss/theft of mobile device for blocking the mobile banking services.

DON'Ts

- Don't open every SMS / MMS as it may contain viruses, especially from unknown sources.
- Do not save confidential information such as your debit/credit card numbers, CVV2 numbers or PINs on your mobile phone.
- Never accept offers such as caller tunes or dialer tunes from unknown sources.
- Be careful about the websites you are browsing. If it does not sound authentic, do not download anything from it.
- Never connect your mobile phone through an unsecured Wi-Fi connection available in public places such as airports etc.

DO's AND DON'Ts FOR EMPLOYEES OF BANK WHILE USING SOCIAL MEDIA

DON'Ts OF SOCIAL MEDIA:

1. No employee shall write/express anything in any internet site or social media that may damage the reputation of the Bank or any of its employees.
2. No employee shall post/express any remarks/views in any internet site or social media which may be defamatory to the Bank or officials or its employees.

3. No employee shall disclose any information about any employee or customer of the Bank including their personal details on any internet site or social media.
4. No employee should criticize the management of the Bank or the business processes or strategies of the Bank or policies of the Bank on any internet site or social media.
5. No employee shall, without express authority, use the name Bank of India or BOI while expressing any views in any of the internet sites/social media.
6. No employees of the Bank are supposed to respond/comment on social media channel through internet, smart phone during office hours.
7. If any employee of the Bank is creating any social network profile he/she should create such profile in his/her real name and shall not create any profile by using any ID otherwise than his real name.
8. No employee of the Bank shall establish I form I promote I become a member of any group I community on any internet site including social networking sites which uses the name and logo of the Bank, unless such is expressly created or permitted by the Bank.
9. DON'T be disrespectful: - Don't insult the thoughts and opinions of others.
10. DO NOT SPAM: - Do not post random comment online in large numbers.
11. DO NOT turn into a Social Media stalker:-Take time and weigh each word before posting online.
12. DO NOT Speak on behalf of your bank: - Staff should speak for themselves and not for the brand as a whole. This can lead to confusion and a skewed image of the Bank.
13. No employee shall canvass for any donation, lottery or third party marketing promotional activities/affairs on any internet site or social media.
14. No employee shall engage in collusive behavior on any internet site or social media, with Bank's competitors or employees.
15. No sensitive data be shared in any WhatsApp Group even in personal capacity. All the members are required to meticulously follow this.
16. No employee must share any image or record including the photograph, signature, account number or any other sensitive information related to the customers' account, on any group in WhatsApp, even in personal capacity.
17. No post should be irrelevant to the objective I subject of the Social Media or misleading or a spam.
18. No sensitive or confidential information, pertaining to bank that has the potential to affect adversely market sentiment or bank's position, is to be posted on any Social media platforms or shared or forwarded outside the Bank.
19. No posting of official communication like circular, memo, official emails, sensitive business information of the bank etc. to be posted on any Social media platforms.

DOs OF SOCIAL MEDIA

1. Staff are required to maintain Confidentiality I Secrecy, Integrity and Availability of bank's Information Assets I Computing Resources.
2. Engage and create positive content: When publishing commenting in personal capacity, make sure it adds value to any conversation where staff participate in, as staff represents bank.
3. Think before posting and commenting: Always review the content you post on social media networks. When reciprocating, leave quality comments related to the post, which adds to the conversation.

However, staff can be part of any Social Media platform in their personal capacity only as an individual or part of a group and sometimes at the choice or request of the customers for faster communication to provide better customer service subject to strictly complying with above Do's and Don'ts of Social Media Policy without any liability and responsibility of the Bank.

(This book is not for sale and is strictly for internal use only)
(Sources: RBI/NPCI/PwC/Internal Communications/mygov.in)

🙏 **Abhay**

उत्कृष्टता की दिशा में एक कदम आगे ...

Management Development Institute
Plot No.–30, Sector–11
CBD Belapur,
Navi Mumbai - 400614