ELECTRONIC PAYMENTS IN INDIA

Isha Sidana & Ajit Brar

Amity Law School, Noida

INTRODUCTION

Government of India's recent war against cash economy coupled with demonetisation and the *'Digital India'* initiative portrays its aim to build a conducive ecosystem for '*cashless economy'*. Supplementing it with television channels such as '*DigiShala*', the government is aggressively promoting digital payments and fin-tech players and mobile wallet companies are riding this massive business opportunity that has emerged due to the state-sponsored '*war on cash*'.Recent reports justify it further by claiming that the total transaction volumes of Paytm (7 million transactions of Rs 140 crore a day) have exceeded that of all the plastic cards issued in the country.[1]With these substantial developments in the past few months we may well be riding the next wave of transformation in digital payments in India but there arises an issue of cybersecurity which our government has time and again failed to address.

Today, with more and more users preferring digital payments, the chances of getting exposed to cybersecurity risks such as online fraud, information theft, and malware or virus attacks are also increasing.[2]The existing laws are incompetent to address the cyber- crimes related to electronic payments. Our country doesn't have a root server of its own making it almost impossible to collect evidence on crimes that are initiated from outside India, thus rendering a victim in India without any immediate remedy. This paper studies the regulatory framework, the redressal framework, security measures and the extent to which these regulations protect the data of an individual.

PRE-PAID PAYMENT INSTRUMENTS

"*Prepaid payment instruments are those which facilitate purchase of goods and services against the value stored on such instruments. The value stored on such instruments*

[1]Sharanya G. Ranga, The legal framework for e-payments in India and the challenges it faces, TECHCIRCLE (May. 25, 2016, 12:16 PM), http://techcircle.vccircle.com/2016/12/01/the-legal-framework-for-e-payments-in-india-and-the-challenges-it-faces/.

[2]Mritunjay Kapur, Digital Payments-Analyzing the Cyber Landscape, KPMG (May. 25, 2017, 10:04 AM), https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Digital_payments_Analysing_the_cyber_landscape.pdf.

represents the value paid for by the holder, by cash, by debit to a bank account, or by credit card. These instruments can be issued as smart cards, magnetic stripe cards, internet accounts, internet wallets, mobile accounts, mobile wallets, paper vouchers. The prepaid payment instruments that can be issued in our country are classified under three categories viz. (i) Closed system payment instruments (ii) Semi-Closed system payment instruments (iii) Open system payment instruments." [3]

Semi-Closed System Payment Instrument

A semi-closed wallet is used to make payments at clearly identified merchant locations or even for the wallets' own digital goods and services.The ease of using electronic wallets as a substitute to physical wallets have made electronic wallets as one of the most convenient ways of making payment through the use of mobile phones.[4] Paytm, Free Charge and Mobi Kwik fall under this category. One can use these semi-closed wallets to pay for recharges as well as to pay for a ride on Uber. Most of the transaction that fall under this wallet are done through smart phones. Smartphone penetration in India was estimated to be at 239 million in 2015 and is expected to grow to 702 million by 2020.[5] Therefore in a short span of five years there is expected a threefold growth in smartphone users which will ultimately increase the users of semi-closed wallets.

REGULATORY FRAMEWORK

Currently there are two legislations that are applicable to the digital wallet security landscape. The first is the "*Information Technology Act, 2000"* (last amended in 2008) and the other is the "*Payments and Settlements Act, 2007"* under which RBI circulars and guidelines relevant to online security are released.

Information Technology Act, 2000[6]

The first relevant portion of this statute is Section 43A which states that *"body corporates"* handling sensitive personal data or information must provide reasonable security measures. These measures must be "*….designed to protect such information from unauthorised access, damage, use modification, disclosure or impairment, as may be specified in an*

[3] Master Circular-Policy Guidelines on Issuance and Operation of Pre-paid payment instruments in India, 2015, https://rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9872

[4]Anita Baid, Overview of the Regulatory Framework of Payment Systems in India, VINOD KOTHARI CONSULTANTS (May. 26, 2017, 02:15 PM), http://india-financing.com/overview-of-regulatory-framework-of-payment-and-settlement-systems-in-india-by-anita-baid/.

[5]Ovum Knowledge Center- Smartphone Connections Forecast 2015-20

[6] The Information Technology (Amendment)Act,2008, No.10, Acts of Parliament, 2009 (India).

agreement between the parties or as may be specified in any law…".[7] Failure to do the same would result in liability to pay the affected party damages.

However digital wallet companies can contract out of these data security obligations via their terms of service agreements. It should be noted that services which are provided by entities which are not corporate bodies such as BHIM, offered by the can be exempted from the obligations under this section.[8] Thus making them not liable for any loss, data failure, claim or damage suffered by the user or any other third party. It further goes on to state in its terms and conditions that it is not able for any electronic or mechanical defect or virus or bugs or related problems.

The second relevant portion are the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011[9]. These rules were notified under the IT Act, 2000. Rule 3 characterises "*sensitive personal data or information as Password;Financial information such as Bank account or credit card or debit card or other payment instrument details;Physical, physiological and mental health condition;Sexual orientation;Medical records and history;Biometric information;Any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise…"*[10]

However this rule circumscribes what may be categorised as *"sensitive data or information" and* is not exhaustive in nature. It restricts to such data and information which fits in one of the above mentioned categories. Such restrictiveness, has the capacity to exclude information or data which is stored, handled and processed by modern day online platforms. This indicates the rule's limited applicability in today's internet landscape.

Payment and Settlements Act, 2007[11] and role of Reserve Bank of India

Section 18 of this statute gives RBI the power to determine appropriate policy for the regulation of electronic payment systems which affect domestic transactions.[12] Section 10(2) gives the RBI the power to determine standards for the management of specific

[7] *Id.*, at s. 43A.
[8]Sidhart Deb, Digital Wallet Security, Centre for Communication Governance (Jun. 1, 2017, 05:28 PM), https://ccgnludelhi.wordpress.com/2017/01/30/digital-wallet-security-is-there-a-framework/.
[9] IT (Reasonable Security practices and procedures are sensitive personal data or information) Rules, 2011, Vol No. 2, C. O. P. (India)
[10] *Id.,* at r. 3.
[11]The Payment and Settlement Systems Act, 2007, No. 51, Acts of Parliament, 2007 (India).
[12] *Id.*, at s. 18.

payment systems.[13] Deriving authority from this, the RBI has been releasing annual circulars detailing the issuance and operation procedures for prepaid instruments. The latest one was release in July 2016. This circular while addressing *"Fraud protection and security standards"*, orders such companies to *"…put in place adequate information and data security infrastructure and systems for prevention and detection of frauds."*[14] No specific guidance is provided to determine what *"adequate information and data security infrastructure"* entails. There are no hard and fast instructions as to what is the required security standard. Moreover, it has no reference to any penal measures should a company fail to adhere to these requirements.

The RBI in December 2016 released a new notification addressing *"Security and Risk Mitigation Measures"* for prepaid instrument issuers. In this notification, the RBI acknowledges that without adequate cyber security their push for widespread adoption of digital payments will suffer huge setbacks. To enable a robust and secure digital ecosystem, this notification orders prepaid instrument issuers to undergo annual system audit reports from qualified auditors. The scope of these system audits includes *"hardware structure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing the systems and applications, documentation, etc."*[15]

Moreover, they have also been advised by the RBI's notification to take *"appropriate measures to mitigate phishing attacks and to disseminate best security practices to their customers periodically. Prepaid instrument issuers have also been asked to take dynamic security measures as per emerging threats and general threat perception."*[16] The question arises weather RBI should be providing for these *"appropriate measures for emerging threats" or* should these be left to the discretion of the prepaid instrument issuers.

INTERMEDIARIES AND THEIR LIABILITY

E- commerce intermediaries connect buyers and suppliers and enable internet transactions between them. Paytm is one such intermediary. It is the largest wallet player in Indian

[13] *Id.*, at s. 10(2).

[14] Master Circular- Policy Guidelines on Issuance and Operation of Pre-Paid Payment Instruments in India,2016, art. 13, https//rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=10510

[15] Security and Risk Mitigation Measure- Technical Audit of Prepaid Payment Instrument issuers, 2016 (India) ,http://cashlessindia.gov.in/files/rbi-notification-security-and-risk-mitigation-measure-technical-audit-of-prepaid-payment-instrument-issuers.pdf

[16]Sidhart Deb, Digital Wallet Security, CENTRE FOR COMMUNICATION GOVERNANCE (Jun. 1, 2017, 05:28 PM), https://ccgnludelhi.wordpress.com/2017/01/30/digital-wallet-security-is-there-a-framework/.

market with 89% of the market share, increased its subscriber base from 122 million in January 2016 to 147 million in December 2016, and further to 200 million by end of February 2017. About 1 billion transactions were conducted on this platform, contributing 26% of all digital transactions. The total balance in its wallets at the end of February 2017 was Rs. 89.91 billion.[17]

Section 2(1) (w) of the IT Act, as amended in 2008, defines '*intermediary' "with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes."*

Liability of such online intermediaries is limited in India. It is governed primarily by the *Information Technology Act, 2000*, supplemented by the *IT Amendment Acts of 2006 and 2008* and the *IT (Intermediaries Guidelines) Rules, 2011*. The RBI has also given directions in 2009 for electronic payments through intermediaries.[18]

Section 79 of the IT Act, as it stands today, debars an intermediary from being held liable for any third party information, data or communication link hosted by him/her in certain cases. If an intermediary is a mere conduit to information by *"providing access to a communication system over which information made available by third parties is transmitted or temporarily stored"*[19], or merely hosts the content without initiating, or modifying the content in, the transmission, or without selecting the receiver[20], and the intermediary generally observes due diligence while discharging his duties[21],such an intermediary cannot be held liable. However even when an intermediary acts as a mere conduit in an e-transaction, it should be liable for any data breach or fraud happening in that particular time frame in which its server is used. Any contentions by the intermediary regarding the knowledge of such breach or non- participation in such breach is immaterial. A strict liability should be imposed on intermediaries.

[17]Nidhi Prabhu, New PPI Draft Guidelines-Shift in Approach, LETS TALK PAYMENTS (Jun. 3, 2017, 01:22 PM), https://letstalkpayments.com/new-ppi-draft-guidelines-shift-in-approach/.
[18]Reserve Bank of India, Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries, RBI/2009-10/231 (May. 22, 2009, 10:42 AM), https://www.rbi.org.in/scripts/Notification User.aspx?Mode=0&Id=5379#M
[19]The Information Technology Act, No. 21 of 2000, India , s. 79(2)(a).
[20]*Id.*, at s. 79(2)(b).
[21]*Id.*, at s. 79(2)(c).

NEW PPI's DRAFT GUIDELINES — *A Comprehensive Approach*

As PPI's become systemically important, the new latest draft guidelines on PPIs, released by RBI in February 2017 seek to place a higher emphasis on safety and security of transactions. Weeding out inactive accounts goes in the same direction. This intention is also reflected in the prescribed security, fraud prevention and risk management framework. Some of the important requirements are a separate login required for the wallet, inactivity timeout feature, cooling period on addition of a beneficiary, restriction on multiple attempts, etc. Making a customer liability framework compulsory is also a step in the direction of enhanced customer protection.In addition, SFA (second-factor authentication) is going to be compulsory even for small-value transactions.

SAFETY MEASURES & RECOMMENDATIONS

With demonetisation, millions of Indians have enrolled for digital payments with mobile payments being the most preferred mode. With such surge in the volume and number of transactions, it is unlikely that the cybercriminals would not be interested. Further, India was recently ranked as one of the five most vulnerable nations to cyber security threats. This was highlighted by the recent debit and credit card hack which adversely compromised over 3 million accounts. The presence of a trust deficit seems justified when one looks at concerns expressed by both the National Crime Records Bureau ('NCRB') in its 2015 Report and the Reserve Bank of India ('RBI'). Both institutions have stressed numerous instances where people have been vulnerable to data theft. Further, it has been suggested that mobile wallets are not developed with hardware level security. Such industry practices leave sensitive information more susceptible to cyber threats. There is also a limited legal framework for the use of online payments.

Hence, securing digital payments infrastructure becomes one of the most important concerns for banks and payment service providers such as digital wallet providers. Organizations should understand the potential threats of cyberattacks and install leading security architecture to ensure that the transactions are seamless and secure. An effective cyber policy with special focus on digital payments should be formulated. A strong cyber protection culture needs to be developed in our country by conducting cyber awareness and trainings. Further, the government should perform periodic cyber risk assessments and an yearly report should be compiled. It should also perform periodic cyber audits and health checks.

People are the weakest link in the security architecture, hence the end users should also proactively ensure that they use strong and unique passwords and should keep their operating systems, applications and antivirus up to date.They should also enable 2FA, wherever available. Further one should avoid opening links or attachments sent from

unidentified sources and also ensure that the connection used during transacting is secure. Users should necessarily monitor their accounts on regular basis to track for unauthorised transactions and avoid sharing any personal information over e-mail or call. One should definitely avoid entering personal information on pop-up windows.

CONCLUSION

Therefore it is concluded that, the government should focus more on educating the customers as well as enforcing basic security standards for organisations. Also all the breaches should be mandatorily reported. The digital payment ecosystem needs to be strengthened, with organisations, users as well as government equally sharing the responsibility of securing the digital payment ecosystem.