India surges towards a digital economy

-By Yashvendra Singh, ETCIO.com

Authored by Rohit Mahajan (APAC Leader, Partner and Head – Forensic, Financial Advisory, Deloitte India) and Arjun Rajagopalan (Director and TMT Lead – Forensic, Financial Advisory, Deloitte India)

Demonetization led to the withdrawal of 86 percent of India's currency as well as facilitated a sudden increase of the adoption of/ dependence on digital payments. Prominent examples of this 'digital explosion' was the exponential rise in the download and use of electronic wallets as well as an unprecedented increase in digital transactions/ payments, witnessed within weeks of the move.

While moving towards a cashless economy is the eventual endeavor, it is important to understand that the sudden push to 'go-digital' may test the existing security and fraud controls extensively. India's status as a digital economy is at a very nascent stage and will evolve and innovate drastically in the coming years, especially with the increased convergence of sectors such as financial services, telecom, information technology, etc. This change will also come with its fair share of challenges, both in the short and long term.

In our view, some of the key concerns that may have an impact on security and governance (including fraud) and would require immediate attention are:

- **Absence of clearly defined security standards/ guidelines for digital payment instruments:** RBI's master circular governing Prepaid Payment Instruments[1] is vague with respect to guidelines on security. As per the circular, wallets are required to have 'adequate' data security infrastructure and systems for the prevention and detection of frauds. However, the circular does not prescribe any minimum standards of security to be followed (by wallets). Nor does it establish liability in case any fraud or loss occurs due to the lack of security measures.

While prepaid instruments operated by financial institutions adopt the security guidelines defined for core banking operations (for adequate data security), wallets operated by other FinTech companies rely on Section 43A of the Information Technology Act (IT Act), in the absence of any other security

standards available. While the IT Act requires documented evidence on compliance to security standards, there is no further liability stated. Further, the IT Act is not specific on the constant updation of security standards based on the changing environment and associated risks.

- **Contractual terms may leave the end customer helpless in case of a fraud incident:** All wallet providers while signing up a new user, get them to accept certain terms and conditions (T&C), which are largely one sided. Most contracts allow wallet operators to disclaim any form of liability for the security of data. While the IT Act covers certain requirements on adequate standards, it also allows private contracts to set the standards. In the case of a dispute where the contracted standards are inadequate, the disclaimer under those T&Cs signed, become binding, leaving the impacted customer with no alternative.

- **Limited data encryption:** A transaction typically allows a mobile phone to interact with servers of the wallet company, facilitating an exchange of data. If at this stage the data is not encrypted, it may be vulnerable to an external fraudster allowing them access to information/ wallets and subsequently their credentials. In case of a fraudulent incident, while technically the company may not take accountability since correct credentials have been used, such an incident may have a negative impact on the brand itself as well as future users. A fair number of organizations having realized these risks, have started encrypting data while transactions are carried out. These encryption algorithms may also need to undergo constant revisions depending on the volume and value of transactions carried out.

- **Convergence leading to confused accountability:** The rise of digital payments and the convergence of these technologies across sectors such as financial services, telecommunications etc., brings with it certain inherent gaps. Most sectors operate in and have different security/ fraud control measures within their eco-system. However to carry out transactions for the end customer, there are certain inter-dependencies between these eco systems, where possible controls gaps do exist. For example, OTP is a verification mechanism sent to a 'registered mobile number' for a transaction to be completed. However, currently wallets owned by FinTech and financial services organizations have no control on fraudulent SIM swap carried out at a telecom service provider's end, inevitably leading to fund embezzlement from the wallets. Similarly FinTech/ telecommunication organizations offering wallet services have no control on data thefts from banking organizations, which can be used to embezzle cash from the wallet. In such incidences, the accountability is not clearly attributable making it difficult for customers to get a fair resolution.

- **'Counterfeit' app leading to phishing fraud:** Apps not downloaded from known and secure sources like Android's "playstore" and Apple's "appstore" or the organizations' registered portal could make the end user vulnerable to fraud. Such apps tend to have the same user interface as the legitimate app and may induce the customer to enter login credentials and other essential information. Once the login details are provided, it may show an error

message or shut down. By the time the customer realizes and is able to make a complaint, funds would have been embezzled using legitimate credentials captured from the user.

- **Roll out pressure may deprioritize focus on fraud controls, SDLC governance:** The lack of focus on controls during the software development lifecycle (SDLC) stage of a product, has the potential to lead to multi-million dollar losses. In our experience, in most cases, perpetrators (mostly customers) have taken advantage of an existing loophole/ gap within the design of the product. In some cases, the design gap that would have been left open intentionally inadvertently has been taken advantage of at a later stage by a nexus of employees, partners, and customers. Wallets in India are at a similar stage, and pressure on acquisition may lead to focus shifting away from fraud controls and security measures. However any design failure at this stage may not only lead to financial losses but can also have a significant impact on the overall success of the digital payment instrument if the customer's faith is broken once.

- **Customer awareness, a critical challenge to curb security breaches and frauds:** While the government is encouraging and pushing people to embrace digital banking/ payment solutions, it is a reality that a large part of the demographic in India has limited awareness on the use of this technology, and to a large part, even banking as a concept. This therefore may pose challenges for organizations, financial institutions and the government to instill faith on opting for such a route. Fraudsters may also find this the most appropriate period to induce customers into sharing critical information and embezzle their money (cramming frauds). It is therefore important that customers not only understand the mechanism of transactions, but the security aspects related to it as well. This may be one of the most critical factors that has the potential to derail the adoption of digital payment instruments, if not addressed soon.

- **Intervention to instill community faith - critical success factor enabling the transition into a 'less cash' economy**
  While there is a clear push by the government and industry to 'go digital', for the community to embrace these alternative payment modes, the faith of customers and merchants on the systems and processes will prove to be the most critical. This faith can be easily shattered if there are frequent incidences of actual (or perceived) frauds, especially during this nascent stage. Some of the important aspects to be taken care of at this stage, to safeguard security and prevent fraud, are mentioned below:

Governing bodies need to come out with well-defined and consistent security standards for all digital payment instruments with each part of the value chain covered under it. We also need a strong monitoring mechanism to assess the

relevance of standards, effectiveness in implementation and compliance to it. Apart from security standards, governing bodies also need to define accountability in case of an incident and establish associated policies around it. The contractual terms and conditions also need to be scrutinized and governed by government bodies effectively.

There needs to be increased focus on governance during the design and development stage (SDLC), despite pressure to expedite roll out. The industry also needs to come out with common standards and framework on application and system development instead of relying on proprietary frameworks and architecture. This would enable consistent security and encryption measures across wallets.

Cross-industry solutions on control vulnerabilities (such as fund embezzlement through SIM SWAP) should be deployed. This may involve modification in systems, input parameters exchanged, as well as process and contracts between parties involved.

Adequate importance needs to be given to fraud management systems and anti-money laundering (AML) systems. While there could be pressure to roll out operations, manual fraud monitoring and AML monitoring interventions should be deployed till the time automated systems are implemented to manage any sudden upsurge in transactions with limited system capabilities.

Of late, the government has initiated customer awareness campaigns on digital payment instruments and the associated risks around duping and frauds. Organizations also need to invest to help educate customers at each stage across the life cycle on possible frauds that they should be careful about, their responsibilities/ ownership, and who they need to approach for consequence management in case of an incident. The organization should also invest on internal processes to deal with customers, address customer complaints and transfer ownership based on the nature of the complaint/ incident. Handholding the customer will help enhance their faith on the brand and in turn protect the reputation of the organization.

[1] Source: RBI Master Circular released on July 1, 2016 – 'Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India (https://rbidocs.rbi.org.in/rdocs/notification/PDFs/16MC9102DB7D5FE742CCB5D0715A77F6666E.PDF)