Business Standard

More steps needed to make e-transactions safer

Absence of comprehensive data protection and privacy laws will be barriers in the govt's digitalisation drive

Sayan Ghosal | New Delhi November 27, 2016 Last Updated at 23:12 IST

The government's recent demonetisation scheme has given a fillip to digital transactions in the traditionally cash-based economy. Amid the changing times and the plethora of conveniences associated with e-payments, experts have again highlighted the lack of a comprehensive data protection and privacy framework.

The Nilson Report, a trade newsletter covering the card and mobile payment segments, estimates fraud losses incurred by banks and merchants in electronic transactions reached the equivalent of $21.8 billion in 2015. This figure is expected to grow as more and more transactions go cashless. India's recent brush with transactional fraud, involving 3.2 million debit cards, have highlighted the growing necessity of ensuring safety and security in the digital payment space. Advent of an e-payment regime now places a greater responsibility on the government, corporate entities and

citizens alike to spread awareness about the associated risks, to ensure a well-protected financial environment.

India's data protection scenario is highly decentralised. It is governed primarily through a series of sector-specific laws in individual regulatory spaces. Introduction of a comprehensive law on data protection has been in the pipeline since 2010, without much progress on the ground. A glimpse of a generic data security scheme can be found in certain provisions of the Information Technology Act. Sections 43 and 66C outline criminal provisions dealing with cases of extraction of data without permission and identity theft. Sections 43A and 72A provide for compensation and punishment for disclosures in breach of lawful contracts.

According to Stephen Mathias, partner, Kochhar & Co, though the amount of compensation payable under Section 43A is unlimited, it fails to cover cases involving the government. As a large majority of banking institutions are part of the public sector, the provision seems feeble in protecting the rapidly evolving transactional space.

Section 72A makes the disclosure culpable only when there is an intention to cause wrongful loss or gain. However, such intent is hard to prove, often allowing companies to escape prosecution.

To modernise the regulatory framework in the transactional space, the government introduced the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, laying down guidelines for the collection, possession, storage and dissemination of personal data.

These Rules also promote reasonable security practices and require annual due-diligence and audit exercises to ensure conformity. Additionally, the Banking Codes and Standards Board of India lays down further safeguards on handling of personal data in financial transactions.

However, many of these requirements are optional in nature. One may contractually opt out of these, undermining the effectiveness.

"Till the Reserve Bank of India (RBI) starts penalising banks for non-adherence, its efforts are sure to be lacklustre. Some banks are yet to comply with even the old guidelines and the whole of the cooperative sector is outside the clutches of the regulator," says Prashant Mali, president, Cyber Law Consulting.

He says RBI should also have separate guidelines for mobile payments. At present, the regulation of these platforms is weak. India's tryst with encryption standards has further complicated the issue of data security. According to Salman Waris, founder partner, TechLegis, there exists a practical dichotomy between the RBI-mandated minimum standards (128-bit) and the maximum permissible encryption levels (40-bit), allowed by the department of telecommunications (DoT).

“This often requires banks to obtain permissions and provide encryption keys to DoT, creating a hurdle in Ease of Doing Business for these entities," he says.

LAWS APPLICABLE TO E-TRANSACTIONS

- Information Technology (IT) Act, 2000
- IT (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
- Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983
- Banking Regulation Act, 1949
- Credit Information Companies (Regulation) Act, 2005

Introduction of a two-factor authentication for online transactions does go a long way in securing digital payments. However, further guidelines on protecting original data sources in banking databases is a must for smooth transition into a cashless system.

“The government may consider protecting personally identifiable information such as spending patterns, in addition to the current protection awarded to sensitive data. And, an enhanced security framework should always be promoted," says Vaibhav Parikh, partner, Nishith Desai Associates.

According to Sunil Abraham, executive director, Centre for Internet and Society, apart from legislating on an omnibus data protection law, introduction of data protection officers to regulate the market and respond to changes will build confidence and promote a culture of digital payment.

Consolidating the multi-layered Know Your Customer (KYC) requirements and proper implementation of the e-KYC system, alongside the development of a secured central digital database, such as Aadhaar, will also give a boost to e-transactions.

“The lack of adoption of electronic payments by merchants is another hurdle to achieving a digital payment regime,” says Rahul Matthan, partner, Trilegal. Under the present system, sellers have to bear several associated costs. These are disincentives for transitioning into a cashless economy. “The government must come up with innovative solutions to encourage vendors to adopt these alternative modes of payment," says Matthan.