BNA International Financial Regulation Review™

Source: International Financial Regulation Review: News Archive > 2011 > 08/31/2011 > New Developments > India: Indian Data Protection Rules and The BFSI Sector

India

Indian Data Protection Rules and The BFSI Sector

By Kartik Maheshwari, Huzefa Tavawalla and Gowree Gokhale, Nishith Desai, India

According to a report by global management consultancy McKinsey & Company[1], as many as 7% of account holders in India are conducting banking transactions online, which is a seven-fold jump since 2007, whereas branch banking has fallen by 15 %. Furthermore, it is envisaged that non-traditional forms of banking are going to rise with an increasing number of banks introducing novel platforms such as tele-banking, mobile banking etc to provide ease and convenience to their customers.

Usage of the internet and electronic mediums for doing business, especially financial transactions, prompted the Government of India to enact the Information Technology Act, 2000 (the "Act"). The Act provides for recognition of electronic signatures, e-documents and e–transactions; and seeks to control offences conducted over the internet. Also, post 2001, the Reserve Bank of India ("RBI") introduced guidelines governing internet banking, confidentiality, anti-money laundering and Know- Your-Customer ("KYC") norms, which may have prompted customers to move towards the e-platform, albeit a few concerns with respect to privacy and security of their banking transactions.

In view of the growing outsourcing industry and e-commerce environment, the Government attempted to introduce a separate bill called "Personal Data Protection Bill 2006" to protect privacy of individuals, but the same was not passed into a law. In the meantime, the Act was amended in 2008 to include Section 43A and Section 72A, to protect Personal Data ("PI") and Sensitive Personal Data or Information ("SPDI"). Recently, effective April 11, 2011 the government has also brought into effect certain rules to support the said provisions (the "Rules").

The Rules have defined SPDI to mean –

Whereas any information, not freely available relating to a person's password, financial information, health condition, sexual orientation, medical records and history, biometric information or any detail relating to the above clauses as provided to body corporate for providing service or for processing, stored or processed under lawful contract or otherwise is defined as SPDI.

These Rules apply to body corporates or persons located within India and relate to information of natural persons.

Since banks collect SPDI, they need to comply with the Rules which lay down certain procedures to be followed at the time of collection of data, transfer of data, disposal of data and maintain relevant security practices and procedures. In the event the bank is negligent in implementing and maintaining 'reasonable security practices and procedures' in relation to SPDI and which causes 'wrongful loss or wrongful gain' to any person, then the bank is liable to pay compensation to the affected person, whose SPDI was compromised. The aggrieved person for claiming compensation may approach adjudicating officer appointed under the Act in case of damages up to Rs. 5 crores (approximately 100,000 USD) or before the civil court in case damages claimed are above Rs. 5 crores (approximately 100,000 USD).

The Rules lay down different level of compliances that are required to be adhered to:

(i) Privacy Policy – The bank or a person who on behalf of the bank, collects, store, deals, or handles SPDI, is required to have a privacy policy in place with the prescribed details. Such privacy policy should be available for review on the website, by the provider of the information. This may in some cases even apply when the information belongs to a person located in India and is collected by a bank outside India using an Indian computer resource.

(ii) Consent – While collecting SPDI, the bank must seek express written consent from the provider of information via a letter/fax/e-mail or consent given by any mode of electronic communication in relation to the purpose for which SPDI may be used. The provider of information

must also be given an option to withdraw such consent and must have knowledge of and/or be provided information as to (a) the fact that information is being collected; (b) purpose for which it is being collected; (c) intended recipients of the information; and (d) name and address of the agency that is collecting and/or retaining the information. This provision is likely to create practical difficulty, as at the time of collection of information banks may not have finalized third party vendors with whom the information may be shared or when the bank changes its vendor(s).

(iii) Transfer & Disclosure - Disclosure of SPDI to a third party requires prior written approval of the provider unless such disclosure has been agreed to in the contract between the bank and the provider of information. The exception(s) being –

a. Where the disclosure is necessary to be in compliance with law; or

b. Where the disclosure is necessary for government agencies mandated under law to procure such information.

Further, banks may transfer SPDI to any third party that ensures the same level of data protection that is adhered to by the bank as provided for under the Rules. Also, the transfer may be allowed only if it is necessary for the performance of a lawful contract between the bank and the provider of information or where the provider of information has consented to such transfer. Therefore, banks will have to ensure through audit process or otherwise that the transferee of information is also adhering to the Rules.

(iv) Reasonable Security Practices - The banks needs to comply with 'reasonable security practices and procedures' designed to protect SPDI from unauthorized access, damage, use, modification, disclosure or impairment. In case there is an agreement between the parties in relation to practices and procedures or there is an applicable law, then the same would govern. In the absence of either, International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" would apply. Best code practices other than IS/ISO/IEC 27001, as approved by the Government of India through any industry body may also be adopted in the absence of the agreement or law.

In light of the above, a few basic issues with respect to data privacy that may arise in relation to BFSI sector are as follows:

- Opening of a Bank Account: At the time of opening of the bank account, customer shares his/her information as per prevalent KYC norms (name, address, pan number etc) with the bank. At that stage the bank in addition to the prescribed RBI regulations will also have to comply with provisions relating to privacy policy and consents under the Rules.

- Sharing of information with third parties: Throughout the conduct of banking activities, the banks share SPDI with third parties, requiring compliance with the transfer and disclosure provisions stated in the Rules. Some of the instances where SPDI is shared with third parties are:

o Bank Account: Upon allotment of a bank account, credit/debit cards, cheque book, ATM pin etc are printed and dispatched to the Customer. This activity in most cases would be outsourced by the banks.

o ATMs: To increase operations and expand consumer reach, banks avail of services of third party for access to a shared ATM network. While conducting such activities SPDI is also shared with third parties by the bank.

o Co-branded Cards: When marketers tie-up with banks to issue co-branded cards which enable accruing of reward points on the basis of usage of such cards, information such as name, address, spending pattern etc. may be shared between the bank, the marketers and merchants.

o Internet Banking: When e-banking facility is outsourced customer information (SPDI) may be saved / stored or retained by third parties.

o Business Correspondents: With the objective of ensuring greater financial inclusion and increasing the outreach of the banking sector, the RBI had decided[2] to enable banks to use the services of Non-Governmental Organisations/ Self Help Groups (NGOs/ SHGs), Micro Finance Institutions (MFIs) and other Civil Society Organisations (CSOs) as intermediaries in providing financial and banking services through the use of Business Correspondent ("BC") model. Rather simply put, a BC is an affiliate of the bank, providing certain approved services on behalf of the parent bank in areas where no branch or ATM of the bank exists. These BCs are allowed to perform a number of functions including, disbursal of small value credit, collection of small value

deposits, sale of mutual fund products and receipt/delivery of small value remittances. Therefore these BCs are intermediary of banks and would need to adhere to the Rules if any information is transmitted / processed in a non-physical format.

- Payment Gateways: Payment gateways facilitate the transfer of information between a payment portal (such as a website, mobile phone etc) and the bank. Since the payment gateway operators on the basis of the information provided by the customer (cvv number, credit card number, date of expiry etc) will be validating such transactions, they would need to have in place mechanisms to ensure data security protection as per the Rules.

- Tele/Mobile Banking: Whenever a customer calls the tele banking number or undertakes banking activities through his/her mobile phone, they must share unique identifiable information like their account number (SPDI), without which they do not gain access to these services. As per the Act 'Communication Device' includes Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate. Thus, 2 Vide DBOD.No.BL.BC. 58/22.01.001/2005-2006 Circular on Financial Inclusion by Extension of Banking Services - Use of Business Facilitators and Correspondents RBI/2005-06/288 tele/mobile banking may also fall within the ambit of the Rules, and would therefore require specific compliances as soon as the customer, avails of such services.

Apart from the Rules in relation to SPDI, the government has also issued rules in relation to intermediaries. In the event any BFSI entity acts as an intermediary, then the said Rules would also be required to be adhered to by such intermediary.

Way Forward

Though these Rules are being applauded by civil rights activists who appreciate the move to protect privacy of individuals, industry players on the other hand, are arguing that such onerous compliances would be an additional burden on them. Section 43A does not lay down a maximum cap in relation to the compensation which would be required to be paid, this essentially is "unlimited liability" for companies.

The Government of India on August 24, 2011 has issued a clarification[3] that reflects that these Rules would apply only to body corporates or persons located within India. However, there still exists concerns with the possible extra territorial ramifications that these Rules may have, for e.g.: In case the bank is located abroad but is collecting information of customers located in India via a computer resource located in India, then would the provisions of the Act apply? It will be interesting to see how the regulators / judiciary interpret the Rules so as to make a bank located outside India liable for contravention of the Act, when the Rules per se are not applicable to such banks.

Lastly, since these Rules are fairly new, there is no established jurisprudence on this subject. Thus, it would be recommended that the banking industry treads carefully and revisits its existing business models to determine various levels at which data is collected, received, possessed, stored, dealt or handled, so as to ensure relevant compliances as specified in the Rules.

1 http://www.rediff.com/business/slide-show/slide-show-1-seven-fold-rise-in-net-banking-in-india-since-2007/20110721.htm

2 Vide DBOD.No.BL.BC. 58/22.01.001/2005-2006 Circular on Financial Inclusion by Extension of Banking Services - Use of Business Facilitators and Correspondents RBI/2005-06/288

3 http://www.mit.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf

Kartik Maheshwari, (Associate), Huzefa Tavawalla (Senior Associate) and Gowree Gokhale (Partner)

The Authors are members of the TMT practice group at Nishith Desai Associates and may be reached at gowree@nishithdesai.com

Nishith Desai Associates is a research based international law firm with offices in Mumbai, Bangalore, Silicon Valley, Singapore and Basel. The firm specializes in strategic legal, regulatory and tax advice coupled with industry expertise in an integrated manner.

ISSN 2047-4733