BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 11, Number 9 September 2011

India's Data Protection Rules And Their Impact On The Banking And Financial Services Industry

By Kartik Maheshwari, Huzefa Tavawalla, and Gowree Gokhale, of Nishith Desai Associates.

According to a report by global management consultancy McKinsey & Co., as many as 7 percent of bank account holders in India conduct banking transactions online, which represents a sevenfold jump since 2007, whereas branch banking has fallen by 15 percent. 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 media for conducting business, especially financial transactions, prompted the Government of India to enact the Information Technology Act, 2000 ("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 introduced guidelines governing internet banking, confidentiality, anti-money laundering and know-your-customer norms, which may have prompted customers to move towards the e-platform, albeit with some concerns with respect to the 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 the "Personal Data Protection Bill 2006" to protect the privacy of individuals, but the bill was not passed into 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 and information ("SPDI").

Recently, effective April 11, 2011, the Government also brought into effect certain rules to support the said provisions ("Rules") (*see analysis at WDPR, May 2011, page 11*).

The Rules define SPDI:

> **Sensitive Personal Data or Information (SPDI)** — 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 bodies corporate 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, and disposal of data, and to maintain relevant security practices and procedures. In the event a bank is negligent in implementing and maintaining "reasonable security practices and procedures" in relation to SPDI, 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 claiming compensation may approach an adjudicating officer appointed under the

Act in the case of damages of up to Rs. 5 crores (approximately U.S.$100,000) or before the civil court in case the damages claimed are above Rs. 5 crores (approximately U.S.$100,000).

The Rules lay down different levels of compliance required to be adhered to:

Privacy Policy

The bank, or a person on behalf of the bank, that 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 on its website for review by the provider of the information. This may in some cases apply even when the information belongs to a person located in India and is collected by a bank outside India using an Indian computer resource.

Consent

While collecting SPDI, the bank must seek express written consent from the provider of information via a letter, fax or 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 and/or be provided information as to 1) the fact that information is being collected; 2) the purpose for which it is being collected; 3) intended recipients of the information; and 4) the name and address of the agency that is collecting and/or retaining the information.

This provision is likely to create practical difficulties, as at the time of collection of information banks may not have finalized arrangements with third party vendors with whom the information may be shared or when the bank changes its vendor(s).

Transfer and 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 exceptions are:

- where the disclosure is necessary to be in compliance with law, or
- 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. Such 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 an audit process or otherwise that the transferee of the information also adheres to the Rules.

Reasonable Security Practices

Banks need 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 an agreement or law.

In light of the above, a few basic issues with respect to data privacy that may arise in relation to the banking and financial services industry are as follows:

Opening of a Bank Account

At the time of opening of the bank account, the customer shares his or her information as per the prevalent know-your-customer norms (name, address, PIN number, *etc.*) with the bank. At that stage the bank, in addition to complying with the prescribed Reserve Bank of India 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, 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:

- Bank Accounts: Upon allotment of a bank account, credit or debit cards, a cheque book, an ATM PIN, *etc.*, are printed and dispatched to the customer. This activity in most cases would be outsourced by the banks.
- ATMs: To increase operations and expand consumer reach, banks avail of services of third parties for access to a shared ATM network. While conducting such activities, SPDI is also shared with third parties by the bank.
- Co-Branded Cards: When marketers tie up with banks to issue co-branded cards which enable the 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.
- Internet Banking: When an e-banking facility is outsourced, customer information (SPDI) may be saved, stored or retained by third parties.
- Business Correspondents: With the objective of ensuring greater financial inclusion and increasing the outreach of the banking sector, the Reserve Bank of India decided (see Circular on Financial Inclusion by

   ISSN 1473-3579

Extension of Banking Services Use of Business Facilitators and Correspondents [RBI/2005-06/288]) 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 the 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 and delivery of small value remittances. Therefore, these BCs are intermediaries of banks and would need to adhere to the Rules if any information is transmitted or 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 will be validating payment transactions on the basis of information provided by the customer (CVV number, credit card number, date of expiry, *etc.*), they would need to have in place mechanisms to ensure data security protection as per the Rules.

Tele-Banking/Mobile Banking

Whenever a customer calls a tele-banking number or undertakes banking activities through his or her mobile phone, he or she must share unique identifiable information like his or her account number (SPDI), without which he or she does not gain access to these services. As per the Act, "Communication Device" includes cell phones, personal digital assistants, or a combination of both, or any other device used to communicate. Thus, tele/mobile banking may also fall within the ambit of the Rules, and would therefore require specific compliance 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 banking and financial services industry entity acts as an intermediary, the Rules would 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 the privacy of individuals, industry players, on the other hand, argue that such onerous compliance requirements would be an additional burden on them. Section 43A does not set a maximum cap in relation to the compensation which would be required to be paid, and essentially represents "unlimited liability" for companies.

The Government of India on August 24, 2011, issued a clarification that these Rules would apply only to bodies corporate or persons located within India (see *http://www.mit.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf*). However, there still exist concerns over the possible extraterritorial ramifications that these Rules may have. For example, if a bank is located abroad but is collecting information from customers located in India via a computer resource located in India, would the provisions of the Act apply? It will be interesting to see if the regulators or the 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 is recommended that the banking and financial services industry tread carefully and revisit its existing business models to determine various levels at which data is collected, received, possessed, stored, dealt or handled, so as to ensure relevant compliance as specified in the Rules.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 are available at http://op.bna.com/pl.nsf/r?Open=byul-8gypzn.

Kartik Maheshwari is an Associate, Huzefa Tavawalla is a Senior Associate, and Gowree Gokhale is a Partner in the TMT practice group at Nishith Desai Associates. The authors may be contacted at gowree@nishithdesai.com.