CHAPTER 9 :LEGAL ISSUES

Introduction

Basel Committee on Banking Supervision, in its "Consultative Document on Operational Risk", defines "operational risk" as the risk of direct, or indirect, loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk[2].

The IT Act-2000 was enacted to handle issues relating to Information Technology. The IT Amendment Act-2008 had made further modifications to address more issues such as cyber crimes. It is critical that impact of cyber laws are taken into consideration by banks to obviate any risks arising therefrom.

Further, there is also a need to examine other issues relating to the need for data protection and privacy laws in India. It needs to be examined whether there is an Indian equivalent of "Electronic Fund Transfer Act (US)" that specifies rights and liabilities of banks and consumers in respect to various e-banking systems.

SCOPE OF THE STUDY

i) Roles, responsibilities and organizational structure

ii) Sources of legal risk to banks due to various cyber laws and other laws like AML

iii) Impact of important provisions of IT Act-2000 and IT Amendment Act-2008, for banks and customers

iv) Experience drawn from judicial pronouncements and related developments due to cyber laws in India

v) Need for any specific provision for data protection and privacy in Indian context

vi) Examining whether there is an Indian equivalent of "Electronic Fund Transfer Act in US", specifying rights and liabilities of banks and consumers in respect to various e-banking systems

A. Guidance for Banks

Roles and Responsibilities and Organizational Structure

Board: The Risk Management Committee at the Board-level needs to put in processes to ensure that legal risks arising from cyber laws are identified and addressed. It also needs to ensure that the concerned functions are adequately staffed and that the human resources are trained to carry out the relevant tasks in this regard

Operational Risk Group: This group needs to incorporate legal risks as part of operational risk framework and take steps to mitigate the risks involved.

Legal Department: The legal function within the bank needs to advise the business groups on the legal issues arising out of use of Information Technology.

Critical issues

(a) Sources of legal risk to banks due to various cyber laws and other laws like AML

Legal risk and operational risk are same. Most risks are sought to be covered by documentation, particularly where the law is silent. The Basel-II accord covers "legal

[2] http://www.bis.org/publ/bcbsca07.pdf

risk" under "operational risk." Documentation forms an important part of the banking and financial sector. For many, documentation is a panacea to the legal risks that may arise in banking activities. But then it has also been realized and widely acknowledged that loopholes exist in these documentations[3].

Documentation

The working group (WG) on Internet Banking[4] had noticed[5] that banks providing internet banking service, and customers availing the same, are currently entering into agreements defining respective rights and liabilities in respect of Internet banking transactions.

The said WG recommended, "A standard format or minimum consent requirement to be adopted by banks may be designed by the Indian Banks' Association, which should capture all essential conditions to be fulfilled by the banks, the customers and relative rights and liabilities arising there from. This will help in standardising documentation as also develop standard practice among bankers offering Internet banking facility."[6]

While addressing legal risks, it is also necessary to address risks arising out of non-compliance with the statutory requirements that involve reputational risks also. Such risks are also legal risks. Legal Risks arise from the ambiguity in the statutes also, particularly when the law is in a state of evolution. The legal risks arising out of the ambiguities in some of the statutes and statutory rules are discussed below.

1. Information Technology Act, 2000[7] (IT Act 2000)

IT Act, 2000 has been amended in 2008[8] and sweeping amendments have been carried out right from enlarging definitions, introducing the concept of electronic signature, creating new offences etc. However there are certain ambiguities which are discussed later in the chapter.

2. Prevention of Money Laundering Act, 2002 (PMLA) & PMLR[9]

Under Section 12[10] of PMLA, every banking company, financial institution and intermediary,

3 Inaugural address by Ms Shyamala Gopinath, Deputy Governor, at the Symposium on "Changing Dynamics of Legal Risks in the Financial Sector", Kochi, 30 October 2009. full text is available at http://www.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=443

4 http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/21595.pdf

5 in Para 9.2.8

6 *Ibid*

6 (21 of 2000)

7 7 Information Technology (Amendment) Act, 2008 (10 of 2009)

8

9 Prevention Of Money-Laundering (Maintenance Of Records Of The Nature And Value Of Transactions, The Procedure And Manner Of Maintaining And Time For Furnishing Information And Verification And Maintenance Of Records Of The Identity Of The Clients Of The Banking Companies, Financial Institutions And Intermediaries) Rules, 2005 (PMLA Rules)

10 12(1) Every banking company, financial institution and intermediary shall--

(a) maintain a record of all transactions, the nature and value of which may be prescribed, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month;

as the case may be (hereinafter referred to as such entities) is required to maintain a record of transactions as may be prescribed by rules and furnish information to the Director within such time as may be prescribed. The records to be maintained by such entities are set forth in rule 3 of PMLR. Such records include record of cash transactions of value more than ₹ 10 lakhs or its equivalent in foreign currency, integrally connected cash transactions taking place within a month, cash transactions where forged or counterfeit notes are involved and suspicious transactions of the nature described therein. Under rule 6 of PMLR, such records are to be maintained for a period of ten years from the date of transaction.

The period before which the transactions have to be reported to the Director are set forth in rule 8 of PMLR. With respect to the transactions of ₹10 lakhs and more and the integrally connected transactions referred to above, the information has to be submitted every month before the 15th day of the succeeding month. The information relating to forged or counterfeit notes is required to be submitted within seven days of the date of occurrence of the transaction. As regards suspicious transactions, principal officer of such entities is required to furnish the information in writing or fax or email to the Director within a period of seven working days on being satisfied that the transaction is suspicious.

The requirement of maintaining the records by such entities regarding the identity of their clients is prescribed in rule 9 of PMLR. The documents that need to be obtained with respect to different kinds of clients such as individual, company, partnership, trust and other unincorporated association have been listed therein. Such entities are required to formulate and implement a client identification programme which incorporates the requirements of the said rule. They may have their own additional requirements as they may feel appropriate to determine the identity of the clients. A copy of the said identification programme is required to be forwarded to Director.

Though the above requirements under PMLA and PMLR appear to be procedural in nature, it needs to be appreciated that the maintenance of records and reporting of transactions help in tracking transactions involving money laundering or the persons involved in such transactions. Under section 13 of PMLA, the Director is empowered (without prejudice to any other action that may be taken under PMLA) to impose a fine which shall not be less than ₹ 10 thousand but which may extend to ₹1 lakh for each failure. Since the imposition of fine by the Director is without prejudice to any other action that may be taken under PMLA it is possible that such entities may be exposed to penalty also under Section 63. In terms of Section 70 if the contravention is committed by such entities the officers in charge of and responsible to the conduct of the business of such entity at the relevant time are also liable to be proceeded with and punished.

It is therefore clear that such entities should have a robust system of keeping track of the transactions of the nature referred to in PMLA and PMLR and report the same within the prescribed period as aforesaid. Apart from the risk of penalty, this involves reputational risk for such entities.

3. *Negotiable Instruments Act-1881 (NI Act)*

Under NI Act, Cheque includes electronic image of truncated cheque and a cheque in the electronic form. The truncation of cheques in clearing has been given effect to and

(b) furnish information of transactions referred to in clause (a) to the Director within such time as may be prescribed;

(c) verify and maintain the records of the identity of all its clients, in such manner as may be prescribed:

appropriate safeguards in this regard have been set forth in the guidelines issued[11] by RBI from time to time.

A cheque in the electronic form has been defined as "a mirror image" of a paper cheque. The expression 'mirror image' is not appropriate. It is perhaps not even the intention that a cheque in the electronic form should look like a paper cheque as seen in the mirror. Further, requiring a paper cheque being written first and then its mirror image or electronic image being generated does not appear to have been contemplated as the definition requires generation, writing and signature in a secure system etc. The expression, "mirror image of" may be substituted by the expression, "electronic graphic which looks like" or any other expression that captures the intention adequately.

The definition of a cheque in electronic form contemplates digital signature with or without biometric signature and asymmetric crypto system. Since the definition was inserted in the year 2002, it is understandable that it has captured only digital signature and asymmetric crypto system dealt with under Section 3 of IT Act, 2000. Since IT Act,2000 has been amended in the year 2008 to make provision for electronic signature also, suitable amendment in this regard may be required in NI Act so that electronic signature may be used on cheques in electronic form.

(b) Impact of various important provisions of IT Act, 2000 and IT Amendment Act 2008 for banks and customers

Prior to the 2008 Amendment Act, IT Act, 2000 had only 2 sections[12] which dealt with computer related offences generally. The Amendment Act provides stronger data protection measures as well as strengthening the general framework against cyber crimes[13]. There are certain issues or lacunae which are inherent in the very nature of crimes involving information technology (and are not specific to banks and customers only) like (a) anonymity

[11] DIT.CO.No. 1/09.63.36/2004-05 dated July1, 2004 on Cheque Truncation - Pilot Implementation; http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=1756&Mode=0 ; New Delhi Bankers' Clearing House, Procedural Guidelines for Cheque Truncation System (CTS) (Version 2.0); Para 4.10 Use of PKI http://rbidocs.rbi.org.in/rdocs/content/pdfs/PRGUVE020910

[12] Sections 43 and 66

[13] By insertion of section 43A and section 72A and amending sections 66 and 67

in cyberspace[14]; (b) the issue of jurisdiction[15]; (c) the question of evidence[16] and (d) the issue of non-reporting of cyber crimes to authorities due to the bad publicity it can have for businesses operating online[17]. Apart from these issues, there are certain specific areas of concern to banks and customers or the banking sector as a whole, which are enlisted below.

(i) Intermediary

The definition[18] of the expression 'intermediary' has been amended in the year 2008. Prior to the said amendment, the definition of the expression 'intermediary' read as under.

" 'intermediary', with respect to any particular message, means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message"

Though banks are not directly referred to in the definition, the definition of the term is so wide that receiving payments on behalf of customers by receiving electronic message sent by other entities in this regard and transmitting electronic messages on behalf of their customers while making payments on their behalf which are normal activities carried on by banks may render them intermediaries. Further the definition also covers any person who provides any service with respect to such messages/records, in which case it is possible that banks may fall within the definition of the term 'intermediary'. In a few cases pending before the Delhi High Court, the court is seized of the question whether banks are intermediaries. The amended definition of the expression 'intermediary' reads as under.

" '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

[14] This conceals the identity of the cyber criminal due to which a criminal can carry out a crime secretly against innocent third parties and by the time the third party realises they have been victim of a crime; it may be too late for the authorities to identify the criminal responsible

[15] The international scope of cyberspace makes it hard to determine which countries courts have jurisdiction on a matter. It is true that there are principles in place for determining jurisdiction, however, a problem may arise if the jurisdiction that is decided upon does not recognise the act as a crime under there national laws. A smart criminal would then knowing this to be the case be able to plan his criminal endeavours ensuring that his actions are only caught by the jurisdiction of the country where his actions are not criminal. Though section 75 of the IT Act, 2000 makes the Act applicable to an offence or contravention committed outside India, a plain reading of the section reveals that its application is limited, in the sense that it applies to an offence committed outside India by any person if the act involves a computer, computer system or computer network located in India. Further, since internet is not restricted by geographical boundaries, it may not be possible for the aggrieved party in a number of cases to know where the crime has been committed and it may many a times lead to great difficulties in even filing a police complaint. It is therefore suggested that an exception ought to be made for any crime committed on the internet so that police stations may acknowledge any complaint made by the aggrieved party. The matter may then be transferred to the local police station in whose jurisdiction the complainant ordinarily resides and legal proceedings should also be taken up accordingly.

[16] Whether it is possible to procure sufficient evidence given the nature of the crime

[17] Journal of Financial Crime: 2007-Challenges for regulating financial fraud in cyberspace by Nigel Fletcher- http://login.westlawindia.com/maf/wlin/app/delivery?&docguid=1797A1090237911DCB5

[18] Section 2(1)(w) of IT Act, 2000

providers, internet service providers, webhosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes."

The changes brought about by the amendment do not really change the position with respect to banks. It is however possible to take a view that banks are not covered by the words, "and includes telecom service providers, network service providers, internet service providers, webhosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes", added by the amendments. The position cannot, however, be regarded as free from doubts. IT Act, 2000 places some responsibilities on intermediaries, which may not be relevant or applicable to banks. To make banks governed by all the provisions applicable to intermediaries would result in unintended consequences and may even expose banks to penal action under IT Act, 2000.

Uncertainty with respect to the meaning of a crucial expression such as, 'intermediary, is not in the interest of any party. As such, it is necessary, that clarity is brought about by statutory amendment with respect to the meaning of the expression 'intermediary' in so far as banks and financial institutions are concerned.

(ii) Encryption

Any data which is transferred online is subject to the risk of being intercepted and misused. Encrypting data before transferring it over the internet will go a long way in safeguarding against such interception. Even though the data may be intercepted it would be of no use unless it is decrypted. If encryption of data is adopted by all entities providing services through the internet then it would extremely helpful in protecting the customers' privacy and also in protection of all other data. At present, the data encryption standards imposed on different categories of online service providers are not uniform.

ISP license restricts the level of encryption for individuals, groups or organisations to a key length of only 40 bits in symmetric key algorithms or equivalents[19]. RBI has stipulated[20] SSL / 128 bit encryption as minimum level of security. SEBI has stipulated 64/128 bit encryption[21] for Internet Based Trading and Services. These encryption standards do not seem to be of international standards. Information Technology (Certifying Authorities) Rules, 2000 requires[22] 'internationally proven encryption techniques' to be used for storing passwords. An Encryption Committee constituted by the Central Government under Section 84A of the IT Act, 2000 is in the process of formulating Rules with respect to encryption. A minimum and reasonable level of encryption may be suggested for the banking sector.

(iii) Data Protection

Section 43A of IT Act[23] deals with the aspect of compensation for failure to protect data. The Central Government has not prescribed the term "sensitive personal data," nor has it

[19] www.dot.gov.in/isp/landing_station.doc; http://www.dot.gov.in/isp/guide_international_gateway.htm

[20] http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0 i

[21] Circular SMDRP/POLICY/CIR-06 /2000 dated January 31, 2000- http://www.sebi.gov.in/Index.jsp?contentDisp=Search

[22] The Information Technology (Certifying Authorities) Rules, 2000- Schedule II, Para 6.1(7)

[23] Please refer to footnote 33 above

prescribed a "standard and reasonable security practice". Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law[24]. However, Explanation (ii) to Section 43A is worded in such a way that there is lack of clarity whether it would be possible for banks, (or any body corporate) to enter into agreement which stipulate standards lesser than those prescribed by Central Government and in the event of the contradiction (between the standards prescribed by the Central Government and those in the agreement) which would prevail. Whether a negligence or mala fide on the part of the customer would make the financial institution liable for no fault of it or whether by affording too much protection to banks, a customer is made to suffer are the two extremes of the situation.[25] The need is for striking a balance between consumer protection and protection of the banks from liability due to no fault of theirs. Apart from affording protection to personal data ("sensitive personal data'- 43A), the IT Act, 2000 also prescribes civil and criminal liabilities (Section 43 and Section 66 respectively) to any person who without the permission of the owner or any other person who is in charge of a computer, computer system etc., *inter alia*, downloads, copies or extracts any data or damages or causes to be damaged any computer data base etc. In this context Section 72 and 72A of the amended IT Act, 2000 are also of relevance. Section 72 of the Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act, 2000, has secured access to any electronic record, information etc and without the consent of the person concerned discloses such information to any other person then he shall be punished with imprisonment upto two years or with fine upto one lakh or with both. Section 72A on the other hand provides the punishment for disclosure by any person, including an intermediary, in breach of lawful contract. The purview of Section 72A is wider than section 72 and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract and not merely disclosure of information obtained by virtue of 'powers granted under IT Act, 2000'.

Further relevant issues on the matter have also been been dealt with later in the chapter.

(iv) Computer related offences and Penalty/Punishment

The IT Act, 2000 as amended, exposes the banks to both civil[26] and criminal[27] liability. The civil liability could consist of exposure to pay damages by way of compensation upto ₹ 5 crore under the amended Information Technology Act before the Adjudicating Officer and beyond ₹ five crore in a court of competent jurisdiction. There could also be exposure to criminal liability to the top management of the banks given the provisions of Chapter XI of

[24] IPC- Sections 406, 420. Indian Copyright Act 1957- Sections 16, 63B. The Indian Contract Act, 1872 – breach of contract- specific performance of the contract. Credit Information Companies (Regulation), Act, 2005- etc.

[25] See also the case of Umashankar Sivasubramaniian v. ICICI Bank (Before the Adjudicating Authority under Information Technology Act, 2000 at Chennai. In this case ICICI contended that the case refers to a phishing case and the blame of negligence lies with the customer who would need to file an FIR and also raised a preliminary objection that the matter cannot be brought under the purview of IT Act, 2000. The Adjudicating Authority however vide its decision dated 12.04.2010 found ICICI Bank guilty of the offences made out in Section 85 read with relevant clauses of Section 43 of the Information Technology Act, 2000 and directed the ICICI to pay a total sum of Rs 12,85,000/-. It is understood that ICICI bank has obtained a stay on the judgment (upon depositing Rs 50,000/-) in an appeal filed by them before the Cyber Appellate Authority.

[26] Sections 43-45

[27] Sections 65-74

the amended Information Technology Act[28] and the exposure to criminal liability could consist of imprisonment for a term which would extend from three years to life imprisonment as also fine. Further, various computer related offences are enumerated in the aforesaid provisions. In case banks are of the view that, with the advancement in technology and information systems there are certain kinds of offences which are not adequately covered by the existing provisions and which would require separate treatment, the same could be indicated to Government.

Of late there have been many instances of 'phishing' in the banking industry whereby posing a major threat to customers availing internet banking facilities. Though Section 66D of the amended IT Act could broadly be said to cover the offence of phishing, attempt to commit the act of phishing is not made punishable. It is suggested that there is a need to specifically provide for punishment for attempt to phish as well in order to deter persons from attempting it.

(v) Bank's to be Licensed as Certifying Authority

The Working Group on Internet Banking had recommended[29] that banks may be allowed to apply for a license to issue digital signature certificate under Section 21 of the Information Technology Act, 2000 and function as certifying authority for facilitating Internet banking and that Reserve Bank of India may recommend to Central Government for notifying the business of certifying authority as an approved activity under clause (o) of Section 6(1) of the Banking Regulations Act, 1949.

It is for consideration whether banks are to be licensed to issue 'digital/electronic signature certificates' under Section 21 of IT Act, 2000.

(vi) Provision for online nomination facility

Though not explicitly dealing with a provision of the IT Act, an issue of relevance is being highlighted here. At present though it is possible to create a new fixed deposit through internet banking, it is not possible to submit a nomination request for it without walking into the branch of a bank. The Banking Companies (Nomination) Rules, 1985 ("Nomination Rules") requires a physical copy of the nomination forms to be submitted by the customer and further requires that the form should be signed in the presence of two witnesses. It is suggested that the Nomination Rules be modified to provide for a mechanism based on the existing platform used by banks so that customers may be able to place a request for nomination and variation or cancellation thereof without having to physically walk into a branch. Nomination which takes effect after the death of the person is on par with a will. Banks get valid discharge by paying to nominee even if there is a valid will in favour of some other party. Attestation of nomination by witnesses is apparently meant for facilitating proof of nomination in the event of dispute. The challenge appears to be to find a robust technological solution for proving that the nomination made on line is a genuine nomination, voluntarily made by the party.

(c) Experience drawn from various judicial pronouncements and other related developments due to cyber laws in India

A few relevant decisions and cases

1. Under IT Act, 2000

Umashankar Sivasubramaniian v. ICICI Bank (Before the Adjudicating Authority under Information Technology Act, 2000 at Chennai) - The complainant alleged that his account was wrongfully debited due to negligence on the part of the bank. ICICI contended that the

[28] Section 85

[29] In Para 9.2.4 http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/21595.pdf

case refers to phishing and the blame of negligence lies with the customer who would need to file an FIR and also raised a preliminary objection that the matter cannot be brought under the purview of IT Act. The Adjudicating Authority however vide its decision dated 12.04.2010 holding that ICICI bank had failed to establish that due diligence were exercised to prevent the contravention found ICICI Bank guilty of the offences made out in Section 85 read with relevant clauses of Section 43 of the Information Technology Act, 2000 and directed the ICICI to pay a total sum of ₹ 12,85,000/- (which includes an amount of ₹ 6,00,000/- towards expenses). ICICI bank has obtained a stay on the judgment (upon depositing ₹ 50,000/-) in an appeal filed by them before the Cyber Appellate Authority.

Avnish Bajaj v. State[30] decided by the Delhi High Court in Criminal Miscellaneous Case No. 3066 of 2006 which discussed amongst others the criminal liability of a network service provider being Baazee.com for third party data or information made available by them on their site. Delhi High court has held that "on a conjoint reading of Section 67 and 85 of the Information Technology Act, 2000, it may be concluded that on the basis of the principle of deemed criminal liability, a case may be made out against any director of a company even though the company may not be arrayed as an accused provided the ingredients laid down in the section are satisfied". It is understood that the decision of the Delhi High Court has been appealed against in the Supreme Court and that the Supreme Court has been pleased to stay the proceedings in the said matter and matter is subjudice.

National Association of Software and Services Companies v. Ajay Sood[31] - This was a reasoned order approving a settlement agreement between the plaintiff and the defendants in a case which dealt with the issue of 'phishing', wherein a decree of ₹16 lakhs was passed in favour of the plaintiffs. It is the contention of the plaintiff that the defendants were masquerading as NASSCOM, and were sending emails, in order to obtain personal data from various addresses, which they could then use for head-hunting, and they went on the website as if they were a premiere selection and recruitment firm. The suit was filed praying for a decree of permanent injunction restraining the defendants or any person acting under their authority from circulating fraudulent e-mails purportedly originating from the plaintiff of using the trade mark 'NASSCOM' or any other mark confusingly similar in relation to goods or services. A compromise application was filed before the court and the court while approving the settlement agreement observed that " in US an Act is proposed which, if passed, will add two crimes to the current federal law; It would criminalize the act of sending a phishing email regardless of whether any recipients of the email suffered any actual damages. It would criminalize the act of creating a phishing website regardless of whether any visitors to the website suffered any actual damages." The Hon'ble Judge further observed that "I find no legislation in India on 'phishing'. An act which amounts to phishing, under the Indian law would be a mis-representation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even the person whose name, identity or password is misused. It would also be an act of passing off as is affecting or tarnishing the image of the plaintiff, if an action is brought by the aggrieved party. Whether law should develop on the lines suggested by Robert Louis B Stevenson in his article noted above is left by this Court for future development in an appropriate case."

2. Under Consumer Laws

State Consumer Disputes Redressal Commission, Raipur- (Appeal No. 435/2009)- ICICI Bank v. Ashish Agrawal – This appeal was filed against the order dated 27.07.2009 of the District Consumer Disputes Redressal Forum, Raigarh directing the appellant bank to pay ₹ 49,912.36/-, which was allegedly not withdrawn by him from his account and also ₹ 5,000/-

[30] 150(2008)DLT769, 2008(105)DRJ721

[31] 119(2005)DLT596, 2005(30)PTC437(Del)

as compensation for mental agony and ₹3,000/- as litigation cost to the respondent/complainant on account of deficiency in service, regarding maintenance of his bank account. The complaint was filed alleging deficiency of service on the part of the appellant bank as ₹49,912.36/- was withdrawn from his bank account, without his knowledge, using internet banking. The State Commission vide its order dated 26.03.2010 allowed the appeal. The Commission observed that the respondent was negligent in giving information regarding password to a third person and hence deficiency of service could not be attributed on the part of the appellant bank, who had taken all precaution to give every instruction to the customer and also authorized him to change his password as and when desired.

Before the Consumer disputes Redressal Forum, Bangalore-(CC No. 514 of 2010) - Rishi Gupta v. ICICI Bank Ltd. - The complaint sought an order directing opposite party bank to refund ₹ 2,30,000/- along with interest @ 24% per annum which was lost by the complainant on account of alleged negligence of the opposite party and for an order directing the bank to pay ₹ 1,00,000/- as damages for negligence of service. The complainant alleges that an amount of ₹ 3,00,000/- was transferred from the account of the complainant, fraudulently, through 15 transactions of ₹ 20,000/- each. The District Forum vide order dated 21.06.2010 dismissed the complaint. The Hon'ble member in the order dated 21.06.2010 observed that in providing confidential details of his online banking such as corporate ID, password etc, to a third party in response to an email purported to be issued by the opposite party bank, without verifying with the opposite party bank, the complainant had acted negligently and he cannot put the blame on the bank.

Before the Consumer Disputes Redressal Forum, Bangalore- (CC No. 1059/2008)- M/s Pachisia Plastics v. ICICI Bank Ltd.- The complaint was filed alleging deficiency of service on the part of opposite party bank on the ground that an amount of ₹1,18,000/- was unauthorisedly debited from the account of the complainant through net banking. The Forum vide order dated 11.07.2009 dismissed the complaint on the ground that there was no deficiency of service on the part of the bank. In the order dated 11.07.2009, it was observed that the burden lies on the complainant to establish that he has kept the code number (password for net banking) secret and that there appeared to be a carelessness and negligence on the part of the complainant.

Before the Consumer Disputes Redressal Forum, Bangalore- (CC No. 2969 of 2009)- K Thagyarajan v. ICICI Bank- The complainant alleged that his internet bank account was breached and an amount of ₹ 77,000/- was unlawfully transferred to another account by some unknown persons. The complainant has alleged deficiency of service on the part of the opposite party bank and prayed for refund of the amount with interest and ₹ 3,00,000/- to be awarded as compensation. The complaint was dismissed vide order dated 20.05.2010 on the ground that there was no deficiency of service on the part of opposite party bank as the complainant had himself delivered the password and user id (for internet banking) to others.

Before the Consumer Disputes Redressal Forum, Bangalore- (CC No. 197 of 2008) Smt. Vimala Varkey & Others v. HDFC Bank Ltd & Another- In this case the complainant was aggrieved that money was fraudulently transferred from his account maintained with opposite party No. 1 bank to an account maintained with opposite party No.2 bank (ICICI bank). The complainant alleged deficiency of service by opposite party No.1 bank and had prayed for reimbursement of the amount with interest. It was observed that the complainant had, admittedly, himself disclosed his customer ID & IPIN to a third party, in reply to a phishing mail and on the basis of such information the third party might have managed to transfer the amount. The terms and conditions, of opposite party No.1 bank, governing operation of Net Banking, stipulated that opposite party cannot be held responsible for the loss sustained by the complainant in such transactions. The Forum therefore dismissed the complaint vide its order dated 2.09.2008 on the ground that there was no deficiency of service on the part of the opposite party bank.

It is necessary to balance the interests of customers and that of banks and provide protection to banks against any fraudulent or negligent act of customer. It is not appropriate to leave such an important issue to be dealt with in documentation. Appropriate statutory provision needs to be enacted in this regard.

(3) An international perspective

The case of TJX Inc's (which is the parent company to discount retailers Marshalls and T.J Maxx) was one which involved massive security breach. It highlighted the issue that financial institutions have been forced to shoulder the majority of the liability to consumers whose identities have been stolen. Unfortunately, in situations such as TJX, financial institutions that were not responsible for the security breach were made to bear the burden. The facts of the case are as follows: In January 2007, after auditors expressed concern over the adequacy of its data security, TJX discovered a massive security breach resulting in more than 45.7 million debit and credit card numbers being stolen. Investigators discovered that the security breach had been on-going since 2005 and that the 'intruders' had decoded the encryption keys TJX used to store customer information. The hackers also obtained customers' drivers license numbers, names, addresses and phone numbers. Investigators believe that the hackers obtained the information by aiming an antenna inside the store and decoding the data streaming between TJX's cash registers, hand-held scanning devices and TJX's computers. TJX's wireless computer system was said to be less secure than a personal home computer. Customers affected (and those even possibly affected) by the security breach instituted a class action suit against TJX on January 29, 2007. TJX also faced lawsuits by financial institutions that incurred losses as a result of the breach. A major concern over identity theft legislation involves whether the entity responsible for the security breach, such as TJX, should bear the cost of such breach or whether the financial institutions should continue to bear the ultimate burden. In *In re TJX Companies Retail Security Breach Litigation,* a federal court in Massachusetts allowed the financial institutions to continue their action against TJX on a negligent misrepresentation theory, but dismissed the banks' negligence and breach of contract claims'. The financial institutions' action against TJX was allowed to survive summary judgment and TJX recently agreed to settle with the financial institutions.[32]

Yet another instance of relevance was the dispute between Yahoo and the family of a marine named Justin Ellsworth killed in Iraq over the young man's e-mail account. The family of Justin Ellsworth sought access to his e-mail account after his death, but Yahoo refused to give his password or access to his correspondence citing the terms of service he had agreed to. A court ordered Yahoo to hand over the documents in 2005, which it did, but no definitive ruling on the status of such digital assets was made[33].

The case reflects the changing scenario of accumulation of 'virtual assets' of various kinds by the users of Information and Communication Technology and also brings in the concept of 'digital inheritance' and 'digital estate'. Issues arise on whom the digital assets of a user (deceased) of ICT would devolve. In India there is no clarity on the subject. It is suggested that there is scope for a separate legislation on 'Inheritance of Virtual Assets' on the lines of Transfer of Property Act or Indian Succession Act or a combination of both. [34]

---

32 DEVELOPMENTS IN BANKING AND FINANCIAL LAW: 2007-2008: XII. The Role of Banking Regulation in Data Theft and Security by Rebecca Dent [Review of Banking & Financial Law (2008) 27 Rev. Banking & Fin. L. 381]

33 http://www.financialexpress.com/news/death-in-an-online-age-raises-issues-of-ownership/537275/

34 http://dqindia.ciol.com/content/top_stories/2010/110041601.asp

B. INDUSTRY-WIDE CONSIDERATIONS

(a) Authentication of electronic records/transactions – Digital/Electronic signatures

Digital Signatures

Section 2(p) of the Information Technology Act, 2000 (Act) defines the term, 'Digital Signature' as "... ... ... authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3". Under sub-Section (1) of Section 3 of the Act, "Subject to the provisions of this section any subscriber[35] may authenticate an electronic record by affixing his digital signature." Sub-Section (2) of Section 3 of the Act reads as under.

"The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record."

A combined reading of Section 2(p) and sub-sections (1) and (2) of Section 3 makes it clear that in terms of the Act an electronic record **may** be authenticated by affixing 'digital signature' and if a party wants to authenticate the electronic record by affixing digital signature, the electronic method or procedure for affixing digital signature **shall** be asymmetric crypto system and hash function. While authentication of an electronic record by affixing digital signature is optional, the procedure for affixing digital signature, namely, use of asymmetric crypto system and hash function, is mandatory.

Electronic Signature

Information Technology (Amendment) Act, 2008 has brought in the concept of 'electronic signature' and has defined it as under:

"electronic signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second Schedule and includes digital signature."

Section 3A of the Act further provides as under:

"3A. Electronic signature.--(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which--

(a) is considered reliable; and

(b) may be specified in the Second Schedule."

Section 3A thus provides for an additional method of authenticating an electronic record by using 'electronic signature'. However, till the Central Government specifies any electronic authentication technique by notification in the Official Gazette and populates the Second Schedule of the Act, authentication of electronic record can be done only by using digital signature.

Proof of Digital Signature: Under section 36 of the Act, a Certifying Authority while issuing a Digital Signature Certificate shall certify, *inter alia*, that,-

" ... ...(ca) the subscriber holds a private key which is capable of creating a digital signature;

---

[35] **Section 2 (1) (zg) of the Act, '... ... ... a person in whose name the Electronic Signature Certificate is issued.'**

(cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber;

... ..."

Section 42 of the Act requires every subscriber to exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure. Further, if the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber is required to communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations. It has been clearly laid down in the explanation to section 42(2) of the Act that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Under Section 67A of Indian Evidence Act, the Court shall presume, unless contrary is proved, that the information listed in an Electronic Signature Certificate (which includes digital signature certificate) is correct. A combined reading of the above provisions makes it clear that the court shall presume that the subscriber has the private key and that the public key listed in the digital signature certificate may be used to verify the digital signature affixed by using that private key. Though this is a rebuttable presumption, it may reasonably be concluded that the subscriber has little chance of successfully challenging the contents of an electronic record authenticated by using digital signature. Under section 73A of the Indian Evidence Act, in order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct--

"(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person."

This makes proof of digital signature easy.

Proposal with respect to Electronic Signature

Electronic signature is also expected to produce the same result after the second schedule is populated by appropriate Notification in the Official Gazette. Since all the above provisions do not refer to electronic signature but refer only to digital signature, the possibility of the parties facing difficulties in proving electronic signature cannot be ruled out. It is therefore recommended that necessary amendments may be carried out in the Act and Indian Evidence Act on the same lines (as the provisions relating to digital signature) to facilitate proof of electronic signature also.

Binding nature of other Electronic Records

The question that arises for consideration is whether a party may be bound by the transactions entered into through electronic means (whether through ATMs, Internet or otherwise) though the electronic records in question are not authenticated by using digital/electronic signature.

Section 65B (1) of Indian Evidence Act reads as under:

"1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible."

It is thus clear that electronic records may be proved in courts even though they are not authenticated by using digital or electronic signature if the conditions mentioned therein are satisfied. The difficulty in proving the various conditions[36] set forth in sub-sections (2) and (3) of section 65B of Indian Evidence Act is ameliorated to a great extent by sub-section (4)[37] thereof under which the certificate of a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities

---

[36] Sub-section (2) of Section 65B of Indian Evidence Act- "(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: -

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in me electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) 'throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether--

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in the section to a computer shall be construed accordingly."

[37] Section 65B(4) of Indian Evidence Act - "(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,--

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a mailer to be stated to the best of the knowledge and belief of the person stating it."

(whichever is appropriate) shall be evidence of any matter stated in the certificate. The information stored in the central computer systems of a departmental store was relied on to hold a person guilty of theft[38]. The evidence of store detective that there was no evidence of malfunctioning of central computer was accepted. It may therefore be concluded[39] that it is possible to prove electronic records in courts even if the electronic records are not authenticated by digital or electronic signatures.

Examiners of Electronic Evidence

A reference may also be made to Section 79A of the Act which reads as under.

"**79A. Central Government to notify Examiner of Electronic Evidence.--** The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation.-For the purposes of this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines."

As the courts are not equipped to deal with the technological issues that may arise in evaluating the evidentiary value of electronic records, it is recommended that Central Government should specify sufficient number of agencies under section 79A of the Act to assist courts in arriving at a decision on the evidentiary value of electronic records irrespective of whether digital or electronic signature is affixed or not.

Bank Transactions

Financial transactions such as, operation of bank accounts and credit card operations are being carried on by banks in a big way by using cards, pin numbers and passwords, etc. Banks are using many security features to prevent frauds to the extent possible. The proposed 'two factor authentication method' (2F method) is also a step in the same direction. It may not be feasible and appropriate to insist on use of a specific technology (digital or electronic signatures) for all retail transactions of the customers.

Proposals

As a short term measure it is recommended that Rules may be framed by the Central Government under Section 5 of the Act, to the effect that, with respect to internet or e-banking transactions, 2F method or any other technique of authentication provided by banks and used by the customers shall be valid and binding with respect to such transactions, though 'digital signature' or 'electronic signature' is not affixed. Finally, it is submitted that provisions similar to the provisions dealing with 'unauthorised electronic fund transfers', consumers liability for unauthorised transfers etc., in the Electronic Fund Transfer Act, USA, (as pointed out later in the report), would be useful in India.

(b) Need for any specific provision for data protection and privacy in Indian context.

The law laid down in Tournier's case[40] is followed in India[41] also and banks are required to maintain secrecy of the accounts of their customer's. The exceptions to the rule are as under:

---

[38] **R v. Shepherd, [1993] 1 All E R 225.**

[39] For analysis of the case law in UK and the position in US, please see 'Computer Out-Puts – Whether valid inputs in Courts?' By G. S. Hegde, Joint Legal Adviser, 2003 Vol 8 RBI Legal News and Views page 55.

[40] Tournier v. National Provincial and Union Bank of England, (1924) 1 K.B. 461

[41] Shankarlal Agarwalla v. State Bank of India and Anr. AIR 1987 Cal 29.

(a) where the disclosure was under compulsion by law, (b) where there was a duty to the public to disclose, (c) where the interest of the bank require disclosure and (d) where the disclosure was made by express or implied consent of the customer

The use of technology in the field of banking appears to have thrown up fresh challenges to banks in effectively fulfilling their obligation to maintain secrecy of the accounts of their customers flowing from the relationship of banker and customer as recognized by the courts.

A reference may be made to 'The Personal data Protection Bill, 2006[42] which was introduced in the Rajya Sabha to provide for protection of personal data and information of an individual collected for a particular purpose, though the Bill has not been passed at all. However, section 43A[43] of IT Act, 2000 inserted in the year 2008 addresses some of the concerns regarding protection of personal data. To make the said provisions effective, Central Government has to frame rules and specify what are "sensitive personal data or information" and what are "reasonable security practices and procedures".

In this connection, a reference may be made to the provisions of Data Protection Act, 1998 (DPA)[44] of United Kingdom which provides for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. Important expressions defined under DPA include, *inter alia*, 'data controller'[45] and 'personal data'[46]. Some of the prominent provisions contained in the DPA are briefly captured as

---

[42] (Bill No. XCI of 2006)

[43] Section 43A. Compensation for failure to protect data.- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected

Explanation.--For the purposes of this section,--

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit

[44] http://www.legislation.gov.uk/ukpga/1998/29

[45] "data controller" means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

[46] "personal data" means data which relate to a living individual who can be identified—

under-

– Section 4 of DPA lays down data protection principles and the same have been set out in Part I of Schedule I[47] to the DPA. Anyone who holds personal information must comply with those principles.

– Section 11 of DPA empowers data subject (the person in respect of whom data is collected) to prevent processing of his personal data by data controller for purposes of direct marketing.

– Under Section 13 of DPA, an individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

– In terms of Section 17 of DPA, data controller cannot process personal data unless he/it has an entry in register maintained by the Commissioner.

– Commissioner is responsible for administering the provisions of DPA. In terms of Section 19 of DPA, Commissioner shall provide facilities for making the information contained in the entries in the register available for inspection by the members of public free of cost (the information is also available online[48]), supply any member of the public with a duly certified copy in writing of the particulars contained in any entry made in the register on payment of

---

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

47 Schdule1, The Data Protection Principles, Part I

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

48 http://www.ico.gov.uk/

fees.

– In terms of Section 24 of DPA, the data controller must, within twenty-one days of receiving a written request from any person, make the relevant particulars available to that person in writing free of charge.

– Part IV of DPA contains a number of exemptions from data protection principles, *inter alia*, for the purpose of national security, crime and taxation, health, education and social work, regulatory activities, manual data held by public authorities and Information available to the public by or under enactment. Miscellaneous exemptions have been captured in Schedule 7 to DP Act. In terms of Section 38 of DP Act, Secretary of State can make further exemptions by order.

– Commissioner under DPA is empowered to impose monetary penalty on the data controller for contravention of the provisions of an amount determined by him and specified in the notice.

– Section 61 of DPA provides for liability of directors etc. When an offence under DPA has been committed by body corporate.

Data Protection with respect to banking sector: In view of the nature and sensitivity of financial transactions, data protection is an important aspect in the banking sector. Further, since data which may have facets of sensitive personal information, is being sent from one jurisdiction to another (eg BPO operations of banks), its protection is all the more relevant. However, a perusal of the relevant positions on data protection under various jurisdictions across the globe clearly demonstrates that there is no unanimity on how data is to be protected. The EU and the United States present opposite extremes in the argument for data protection. While the EU system of data protection affords a standard across the EU[49] (thereby making the flow of data easier and more hassle-free), it adds a rung to the ladder of bureaucracy. In the contrast there is no single law in the United States that provides a comprehensive treatment of data protection or privacy issues. In addition to the constitutional interpretations provided by the courts and international agreements, there have been a number of laws and executive orders dealing specifically with the concept of data protection.[50] The amendments made to the IT Act, 2000 by the Amendment Act, 2008 (when compared to the EU Directive and the position in US) seems to be mid way between the two as far as norms guiding the protection of personal data exported to India are concerned. Section 43A of IT Act [51] deals with the aspect of compensation for failure to protect data. The Central Government has not prescribed the term "sensitive personal data," nor has it prescribed a “standard and reasonable security practice”. Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law[52]. However, Explanation (ii) to Section

[49] Please refer Directive 95/46/EC or the Data Protection Directive implemented by European Commission to ensure a high level of protection and free movement of data within the European Union (EU Directive) and OECD (Organisation for Economic and Cooperation and Development) Guidelines

[50] Journal of Internet Law, New York: Nov 2009, Vol 13- The Securtiy of Data Export to India by Shri Sajai Singh- http://proquest.umi.com/pqdweb?did=1897918491&Fmt=3&clientId=47637&RQT=309&VName=PQD

[51] http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapilcelexplus!DocNumber& lg=en&type doc=Directives&andoc=1995&nu doc=46

[52] IPC- Sections 406, 420. Indian Copyright Act 1957- Sections 16, 63B. The Indian Contract Act, 1872 – breach of contract- specific performance of the contract. Credit Information Companies (Regulation), Act, 2005- etc.

43A is worded in such a way that there is lack of clarity whether it would be possible for banks, (or any body corporate) to enter into agreement which stipulate standards lesser than those prescribed by Central Government and in the event of the contradiction (between the standards prescribed by the Central Government and those in the agreement) which would prevail. Whether a negligence or mala fide on the part of the customer would make the financial institution liable for no fault of it or whether by affording too much protection to banks, a customer is made to suffer are the two extremes of the situation.[53] The need is for striking a balance between consumer protection and protection of the banks from liability due to no fault of theirs.

Whether Section 43A read with Section 72 and 72A of the IT Act, 2000 present address the issue of data protection adequately or they need to be duly supplemented by long-term provisions which can help facilitate effective and efficient protection and preservation of data would depend on the prescriptions of the Central Government. It is felt that the prescriptions of the Central Government may address the following issues:

- Minimum parameters / standards of what constitutes 'reasonable security practices and procedures and needs to be ensured by the body corporate. It is suggested that the parameters / standards should not be uniform to be applicable across all body corporates, rather should be customized to suit the size and type of body corporate.
- Body corporates may be free to deploy their own security procedures to suit their needs which would be in addition to the prescribed minimum standards.
- Adequate safeguards for sharing information: Financial Institutions not only possess / deal / store and handle customers' information, but are also required to share the same with statutory / regulatory authorities and third parties due to several reasons. The rules should provide the minimum safeguards to be ensured and adhered while financial institutions share customer information with statutory / regulatory authorities and third parties due to several reasons.
- Workable definitions of data security practices, covering both a threshold for the sensitivity of the data lost, and criteria for the accessibility of that data.
- Mandatory and uniform central reporting system: agencies/ officers should be notified of the data lost.
- Clear rules on form and content of notification letters, which must state clearly the nature of the breach and provide advice on the steps that the individual should take to deal with it.
- Data Security Council of India have recommended [54]the following nine privacy principles in the context of Indian Industry: (a) Notice[55]; (b) Choice and consent[56] (c)

[53] See also the case of Umashankar Sivasubramanian v. ICICI Bank (Before the Adjudicating Authority under Information Technology Act, 2000 at Chennai. In this case ICICI contended that the case refers to a phishing case and the blame of negligence lies with the customer who would need to file an FIR and also raised a preliminary objection that the matter cannot be brought under the purview of IT Act, 2000. The Adjudicating Authority however vide its decision dated 12.04.2010 found ICICI Bank guilty of the offences made out in Section 85 read with relevant clauses of Section 43 of the Information Technology Act, 2000 and directed the ICICI to pay a total sum of ₹ 12,85,000/-. It is understood that ICICI bank has obtained a stay on the judgment (upon depositing ₹ 50,000/-) in an appeal filed by them before the Cyber Appellate Authority.

[54] DSCI Privacy Framework Best Practices, page 14.

[55] Providing a complete idea to an 'end customer' of how the organization concerned will use the information provided by the customer, its privacy policy etc.

Collection Limitation[57]; (d)Use Limitation[58]; (e) Access and Correction[59]; (f) Security[60]; (g) Disclosure to third party[61]; (h) Openness[62]; (i) Accountability[63]. The recommendations of DSCI are relevant and may be considered.

The Gramm-Leach-Bliley Act

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC.

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions "such as credit reporting agencies" that receive customer information from other financial institutions.

The Pretexting provisions of the GLB Act protect consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as "pretexting."[64]

---

[56] **Customers to be provided 'choices' for trading off their personal information to avail of the services and their consent to be proactively obtained, stored and preserved for any future use.**

[57] **Organization should only collect the required data and that too through fair and lawful means.**

[58] **Personal data should not be made available or used for any purpose other than what it was stated to be collected for.**

[59] **The end user (data subject) should be given access to the information and has to be provided with an opportunity to correct his/her data.**

[60] **The technical and organizational measures for securing the data.**

[61] **Disclosure to third party should be when it is necessary and should be subject to the same principles of data protection as adopted by the organization concerned.**

[62] **An organization should have openness/transparency with respect to the development, practices and policies with respect to personal data.**

[63] **Data controller accountable for complying with the measures that give effect to the aforesaid principles.**

[64] http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Right to Financial Privacy Act of 1978(USA)

Similarly, the above Act restricts access to personal data in the custody of financial institutions by the Government Authority[65].

(c) Whether there is an Indian equivalent of Electronic Fund Transfer Act in US specifying rights and liabilities of banks and consumers in respect to various e-banking systems.

Electronic Funds Transfer Act (USA)

In the US the Electronic Funds Transfer Act (EFTA) read with the Electronic Fund Transfers Regulation (Regulation E) provide the basic framework establishing the rights, liabilities and responsibilities of participants in electronic fund transfer systems. The Electronic Fund Transfer Act, 1978 is basically a consumer protection measure and is codified as title IX of the Consumer Protection Act[66]. This Act apart from defining certain basic concepts, lays down the disclosure norms in regard to terms, pricing etc. it also requires the service providers to supply transaction record. This Act defines the term unauthorised electronic fund transfer[67] and prescribes (limits) the consumers liability for unauthorised electronic transfers. The Act also prescribes the liability of the financial institutions in the situations enumerated therein. It also requires service providers to supply transaction record. This Act, however, applies mostly to consumer activated consumer payment systems and other consumer related Electronic funds transfer (EFT) like Electronic funds transfer at Point of Sale and ATMs. Inter-bank and intra-bank fund transfers are not covered by EFT Act.

Position in India

In India prior to 2007, there was no enactment which dealt with the issue of EFT. Payment and Settlement Systems Act, 2007 (PSS Act) and the directions and guidelines issued thereunder deal, to a certain extent, with the issue. Section 2(1)(c) of PSS Act[68] is more wide

---

[65] http://www.fdic.gov/regulations/laws/rules/6500-2550.html

[66] ***Codified to 15 U.S.C. 1693a-1693;*** **http://www.fdic.gov/regulations/laws/rules/6500-1350.html#fdic6500904**

[67] Section 903 (11)- " the term 'unauthorised electronic fund transfer' means an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit, but the term does not include any electronic fund transfer

- initiated by a person other than the consumer who was furnished with the card, code, or means of access to such consumer's account by such consumer, unless the consumer has notified the financial institution involved that transfers by such other person are no longer authorized,
- initiated with fraudulent intent by the consumer or any person acting in concert with the consumer, or which constitutes an error committed by a financial institution."

[68] Section 2(1)(c) "electronic funds transfer" means any transfer of funds which is initiated by a person by way of instruction, authorisation or order to a bank to debit or credit an account maintained with that bank through

in its coverage than the EFT Act in that it does not restrict itself to transfer of funds initiated through electronic means but deals with transfer initiated by a person by other means and is settled electronically, thereby bringing within its ambit Electronic Clearing system (ECS), auto-debit instructions etc. Section 18 of the PSS act empowers the Reserve Bank to issue directions and such directions issued by the Reserve Bank to be complied with. The Act also prescribes the penalties/punishments for failure to comply with the provisions of the Act and the rules, regulations, orders, directions etc issued thereunder. Section 25 of the Act deal with the issue of dishonour of Electronic Funds Transfer for insufficiency etc., of funds and make it an offence punishable with imprisonment for a term which may extend to two years or with fine or with fine which may extend to twice the amount of the electronic fund transfer, or with both.

So as to make the process of electronic fund transfer more smooth and effective, the Reserve Bank has been issuing a number of guidelines to deal with the various aspects of and procedures for electronic fund transfer[69].

Further, so as to help banks to identify and control fraudulent alterations in cheques, the Reserve Bank has issued instructions that no changes / corrections should be carried out on the cheques (other than for date validation purposes, if required). For any change in the payee's name, courtesy amount (amount in figures) or legal amount (amount in words), etc., fresh cheque forms should be used by customers.[70]

As regards various aspects of customer service, the Reserve Bank has been issuing directions/guidelines from time to time to deal with certain aspects like reconciliation of transactions at ATMs failure[71]; enhance security measures for online card transactions[72] etc In addition to these measures a customer also has the recourse to general law[73]. Thus in India though there is no specific legislation which deals only with 'electronic fund transfer' and which is as consumer protection driven certain concerns have been dealt with in the Payment and Settlement Systems Act, Rules, Regulations, directions etc issued thereunder as well as the provisions of general law. However, it may be apposite to have some provisions similar to those in EFT Act which exempts the bank from liability in the event of fraud by the customer or a technical failure etc.

---

electronic means and includes point of sale transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfers initiated by telephone, internet and card payment;

[69] Electronic Fund Transfer System-Procedural Guidelines; special Electronic Funds Transfer System-Procedural Guidelines; Electronic Clearing Service (Debit Clearing)- Procedural Guidelines; Electronic Clearing Service (Credit Clearing)- Procedural Guidelines; National Electronic Funds Transfer System-Procedural Guidelines etc

[70] Paragraph 1.8 of Annexure (CTS-2010 Standard) to Circular DPSS.CO.CHD.No.1832/04.07.05/2009-2010 dated February 22, 2010

http://rbi.org.in/scripts/NotificationUser.aspx?Id=5741&Mode=0

[71] Reconciliation of Transactions at ATMs Failure-Time Limit [RBI/2009-10/100; DPSS No. 101/02.10.02/2009-10 dated 17.07.2009]

[72] Credit/Debit card Transactions- Security Issues and Risk Mitigation Measures-[DPAA No. 1501/02.14.003/2008-09 dated 18.02.2009]

[73] Clause 8 of Banking Ombudsman Scheme; Consumer Protection Act etc.

KEY RECOMMENDATIONS

1. The Risk Management Committee at the Board level needs to put in place processes to ensure that legal risks arising from cyber laws are identified and adequately addressed. It also needs to ensure that the concerned functions are adequate staffed and the human resources are trained sufficiently to carry out the above. The Operational Risk Group need to incorporate legal risks as part of operational risk framework and take steps to mitigate the risks involved. The legal function within the bank needs to advise the business groups on the legal issues arising out of use of Information Technology.
2. It is necessary that banks have a robust system of keeping track of the transactions of the nature referred to in PMLA and PMLR and report the same within the prescribed period. Apart from the risk of penalty, this involves reputational risk for such entities.
3. A cheque in the electronic form has been defined as “a mirror image” of a paper cheque. The expression ‘mirror image’ is not appropriate. The expression, “mirror image of” may be substituted by the expression, “electronic graphic which looks like” or any other expression that captures the intention adequately.
4. The definition of a cheque in electronic form contemplates digital signature with or without biometric signature and asymmetric crypto system. Since the definition was inserted in the year 2002, it is understandable that it has captured only digital signature and asymmetric crypto system dealt with under Section 3 of IT Act, 2000. Since IT Act,2000 has been amended in the year 2008 to make provision for electronic signature also, suitable amendment in this regard may be required in NI Act so that electronic signature may be used on cheques in electronic form.
5. There is uncertainty with respect to the meaning of a crucial expression such as, ‘intermediary” as per IT Act 2000 and as amended by IT Amendment Act, 2008. As such, it is necessary, that clarity is brought about by statutory amendment with respect to the meaning of the expression ‘intermediary’ in so far as banks and financial institutions are concerned.
6. A combined reading of Section 2(p) and sub-sections (1) and (2) of Section 3 of IT Act makes it clear that in terms of the Act an electronic record may be authenticated by affixing ‘digital signature’ and if a party wants to authenticate the electronic record by affixing digital signature, the electronic method or procedure for affixing digital signature shall be asymmetric crypto system and hash function. While authentication of an electronic record by affixing digital signature is optional, the procedure for affixing digital signature, namely, use of asymmetric crypto system and hash function, is mandatory.
7. The question that arises for consideration is whether a party may be bound by the transactions entered into through electronic means (whether through ATMs, Internet or otherwise) though the electronic records in question are not authenticated by using digital/electronic signature. On a reading of Section 65B (1) of Indian Evidence Act, it is clear that electronic records may be proved in courts even though they are not authenticated by using digital or electronic signature if the conditions mentioned therein are satisfied. The difficulty in proving the various conditions set forth in sub-sections (2) and (3) of section 65B of Indian Evidence Act is ameliorated to a great extent by sub-section (4) thereof under which the certificate of a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate.

8. Government should specify sufficient number of agencies under section 79A of the Indian Evidence Act to assist courts in arriving at a decision on the evidentiary value of electronic records irrespective of whether digital or electronic signature is affixed or not.

9. Financial transactions such as, operation of bank accounts and credit card operations are being carried on by banks in a big way by using cards, pin numbers and passwords, etc. Banks are using many security features to prevent frauds to the extent possible. The proposed 'two factor authentication method' (2F method) is also a step in the same direction. It may not be ideal and practically feasible to insist on using a particular technology for all retail transactions of the customers with their banks.

10. As a short term measure it is recommended that Rules may be framed by the Central Government under Section 5 of the Act, to the effect that, with respect to internet or e- banking transactions, 2F method or any other technique of authentication provided by banks and used by the customers shall be valid and binding with respect to such transactions, though 'digital signature' or 'electronic signature' is not affixed.

11. ISP license restricts the level of encryption for individuals, groups or organisations to a key length of only 40 bits in symmetric key algorithms or equivalents. RBI has stipulated SSL / 128 bit encryption as minimum level of security. SEBI has stipulated 64/128 bit encryption for Internet Based Trading and Services. Information Technology (Certifying Authorities) Rules, 2000 requires 'internationally proven encryption techniques' to be used for storing passwords. An Encryption Committee constituted by the Central Government under Section 84A of the IT Act, 2000 is in the process of formulating Rules with respect to encryption. Allowance for higher encryption strength may be allowed for banks based on recommendations of RBI.

12. Section 43A of IT Act deals with the aspect of compensation for failure to protect data. The Central Government has not prescribed the term "sensitive personal data," nor has it prescribed a "standard and reasonable security practice". Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law.

13. Apart from affording protection to personal data ("sensitive personal data'- 43A), The IT Act, 2000 also prescribes civil and criminal liabilities (Section 43 and Section 66 respectively) to any person who without the permission of the owner or any other person who is in charge of a computer, computer system etc., inter alia, downloads, copies or extracts any data or damages or causes to be damaged any computer data base etc. In this context Section 72 and 72A of the amended IT Act, 2000 are also of relevance. Section 72 of the Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act, 2000, has secured access to any electronic record, information etc and without the consent of the person concerned discloses such information to any other person then he shall be punished with imprisonment upto two years or with fine upto one lakh or with both. Section 72A on the other hand provides the punishment for disclosure by any person, including an intermediary, in breach of lawful contract. The purview of Section 72A is wider than section 72 and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract and not merely disclosure of information obtained by virtue of 'powers granted under IT Act, 2000'.

14. The IT Act, 2000 as amended, exposes the banks to both civil and criminal liability. The civil liability could consist of exposure to pay damages by way of compensation upto ₹ 5 crore under the amended Information Technology Act before the Adjudicating Officer and beyond ₹ five crore in a court of competent jurisdiction. There could also be exposure to criminal liability to the top management of the banks given the provisions of Chapter XI of the amended Information Technology Act.

Further, various computer related offences are enumerated in the various provisions.

15. Of late there have been many instances of 'phishing' in the banking industry whereby posing a major threat to customers availing internet banking facilities. Though Section 66D of the amended IT Act could broadly be said to cover the offence of phishing, attempt to commit the act of phishing is not made punishable. It is suggested that there is a need to specifically provide for punishment for attempt to phish as well in order to deter persons from attempting it.

16. It is necessary to balance the interests of customers and that of banks and provide protection to banks against any fraudulent or negligent act of customer. It is not appropriate to leave such an important issue to be dealt with in documentation. Appropriate statutory provision needs to be enacted in this regard.

17. Whether Section 43A read with Section 72 and 72A of the IT Act, 2000 presently address the issue of data protection adequately or they need to be duly supplemented by long-term provisions which can help facilitate effective and efficient protection and preservation of data would depend on the prescriptions of the Central Government. Various suggestions have been offered in this report to address issues in this regard.

18. In India though there is no specific legislation which deals only with 'electronic fund transfer' and which is consumer protection driven, certain concerns have been dealt with in the Payment and Settlement Systems Act, Rules, Regulations, directions etc issued thereunder as well as the provisions of general law. However, it may be apposite to have some provisions similar to those in EFT Act which exempts the bank from liability in the event of fraud by the customer or a technical failure etc (for example, provisions dealing with 'unauthorized electronic fund transfers' and consumers liability for unauthorized transfers).