GGWG-Legal Issues

Banking Industry & IT Act ,2008

Naavi

Background

- Indian Banking has been using E-Banking since around 1997 when ICICI Bank started offering Internet banking
- At that time, there was no legal recognition for electronic documents.
  - Internet Banking was therefore lawless Banking!
- On 17th October 2000, ITA 2000 was notified
  - Provided Legal recognition for
    - electronic documents
    - Authentication
  - Defined some Cyber Crimes and penalties/punishments thereof
  - Defined responsibilities for Intermediaries and corporate officials

Background..2

- RBI constituted S R Mittal Working Group to develop guidelines for Internet Banking.
  - Based on the recommendations, RBI issued Internet banking guidelines on June 14, 2001 (IBG-2001)

Background..4

- 27th October 2009
  - Substantial amendments to ITA 2000 became effective
    - ITA 2008 came into being
    - Rules under Sections 69/69A/69B relesed
- RBI constituted GGWG in April 2010
  - Report released on January 14, 2011
  - RBI notified acceptance on April 29, 2011
- ITA 2008 rules on Sec 43A released on April 11, 2011

Status of Internet Banking Guidelines-2001

- GGWG-New Guidelines are an extension of the 2001 guidelines.
  - In the event of a direct conflict with an earlier guideline, the new guideline would be the basis for implementation by banks.
  - Else, the relevant guidelines prescribed earlier would be an adjunct to the present guidelines issued herewith.

Flexibility

- The guidelines are not “one-size-fits-all” and the implementation of these recommendations need to be
  - risk based and
  - commensurate with the nature and scope of activities engaged by banks and
  - the technology environment prevalent in the bank and
  - the support rendered by technology to the business processes
- Banks with extensive leverage of technology to support business processes would be expected to implement all the stipulations outlined in the circular

Legal Compulsion recognized

- It is clarified that
  - except where legally required,
    - banks may consider any other equivalent/better and robust technology/methodology based on new developments after carrying out a diligent evaluation exercise.

IBG-2001.. Five Guidelines

As accepted by RBI

Introduction for Account Opening

- (IBG-1) Considering the legal position prevalent,
  - there is an obligation on the part of banks not only to establish the identity
  - but also to make enquiries about integrity and reputation of the prospective customer.
  - Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer. (Para 7.2.1)

Digital Signature

- (IBG-2) From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature.
  - In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record.
    - Any other method used by banks for authentication should be recognized as a source of legal risk. (Para 7.3.1)

Risk Control Measures

- (IBG-3) Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers' accounts.
  - In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors.
  - Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures.
    - The banks should, therefore, institute adequate risk control measures to manage such risks. (Para 7.5.1-7.5.4)

Stop Payment

- (IBG-4) In Internet banking scenario there is very little scope for the banks to act on stop-payment instructions from the customers.
  - Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted. (Para 7.6.1)

Insurance

- (IBG-5) The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well.
  - Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers.
  - Considering the banking practice and rights enjoyed by customers in traditional banking,
    - banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks. (Para 7.11.1)

GGWG

Recommendations on Legal Issues

Final Circular highlights..

- Basel Committee definition of "Operational Risk" includes Legal Risk
  - Uncovered legal risk creates defaults in capital adequacy
- It is critical that the impact of Cyber Laws is taken into consideration by Banks to obviate any risk arising there from.

Final Circular highlights..2

- The Risk Management committee at the Board level (IT Strategy Committee) 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
  - Appoint an ITA 2008 compliance official
- Operational Risk Group needs to incorporate legal risks as part of operational risk framework and take steps to mitigate the risks involved in consultation with its legal functions within the bank
  - Initiate an audit

Final Circular highlights..3

- Legal Department within the bank needs to advise the business groups on the legal issues arising out of use of Information Technology with respect to the legal risk identified and referred to it by the Operational Risk Group.
  - Organize training programmes

Final Circular highlights..4

- The IT Act, 2000 as amended, exposes the banks to both civil and criminal liability.
- There could also be exposure to criminal liability to the top management of the banks given the provisions of Chapter XI of the amended IT Act
  - and the exposure to criminal liability could consist of imprisonment for a term which could extend from three years to life imprisonment as also fine.

Final Circular highlights..5

- Legal risk and operational risk are same.
  - Most risks are sought to be covered by documentation, particularly where the law is silent.
  - 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 do exist in documentation.

Final Circular highlights..6

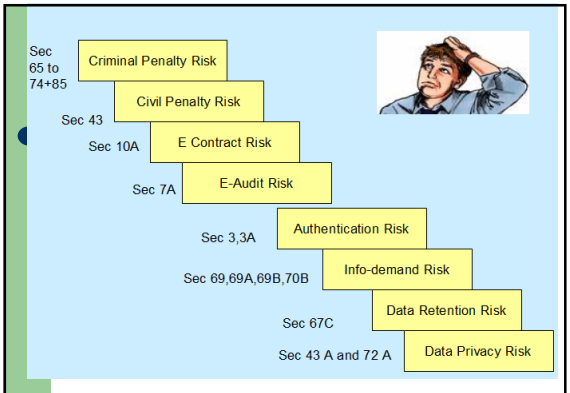
- Legal risks need to be incorporated as part of operational risks and
  - the position need to be periodically communicated to the top management and Board/Risk Management Committee of the Board.

Final Circular highlights..7

- As the law on data protection and privacy, in the Indian context are in an evolving stage,
  - banks have to keep in view the specific provisions of IT Act, 2000 (as amended in 2008), various judicial and quasi judicial pronouncements and related developments in the Cyber laws in India as part of legal risk mitigation measures.
  - Banks are also required to keep abreast of latest developments in the IT Act, 2000 and the rules, regulations, notifications and orders issued there under pertaining to bank transactions and
  - emerging legal standards on digital signature, electronic signature, data protection, cheque truncation, electronic fund transfer etc.
    - as part of overall operational risk management process.

Salient Compliance Requirements

In ITA 2008



ITA 2008...

- Data Privacy Risk
  - Requires Every Body Corporate handling Sensitive Personal Information to follow Reasonable Security Practices
    - Failing which
      - the body corporate would be liable to pay compensation (no upper limit)
      - Could also lead to 3 year's imprisonment to the corporate executives who were negligent

ITA 2008....

- Data Retention Risk
  - Section 67C
    - mandates specified data retention in specified formats
- Regulatory Agencies Information Demand Risk
  - Section 69, 69A and 69 B
    - empowers CERT IN with powers of interception, decryption, monitoring, blocking or demanding of data traffic information
    - Not assisting the CERT In when demanded can impose penalties on the company
    - To assist, companies need to put their compliance practices in place right now.
      - Designate a Compliance Officer whose name may have to be displayed on the website and in the annual report

ITA 2008...

- Authentication Risk
  - Sec 3 and 3A along with Sec 5
    - mandate technical requirements of authentication of electronic documents
- E-Audit Risk
  - Sec 7A
    - mandates auditing of e-documents
- E-Contract Risk
  - Sec 10A along with Sec 4
    - mandates contractual obligations

ITA 2008...

- Civil Penalty Risk
  - Sec 43
    - imposes civil penalties for different contraventions
- Criminal Penalty Risk
  - Sections 65, 66, 66A, 66B,66C,66D,66E,66F, 67, 67A,67B, 70,71,72,73, and 74
    - impose criminal penalties for various contraventions

ITA 2008…Employee Contraventions

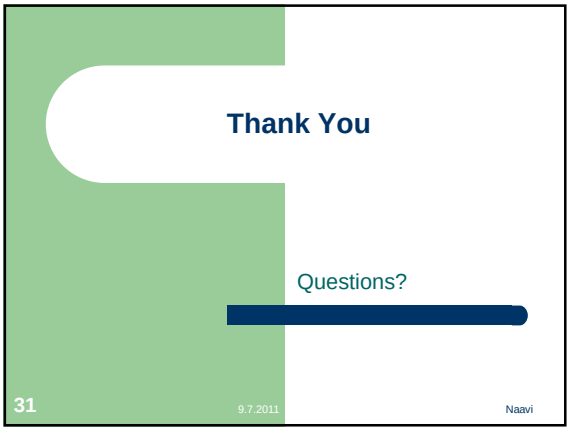
- Vicarious Liability Risk
  - Section 85 and Section 79
    - extend contravention of any of the provisions of ITA 2008
    - by the use of any of the facilities of an organization
      - To the Company and its executives

Concept of Due Diligence

- Sec 85 of ITA 2008
- (1)Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company,
  - every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:
    - **Provided** that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention

Sec 85..contd

- (2)Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place
- with the consent or connivance of, or
- is attributable to any neglect
- on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.
  - **Explanation**- For the purposes of this section
    (i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and
    (ii) "Director", in relation to a firm, means a partner in the firm


Thank You
Questions?
31
9.7.2011
Naavi