LEGAL FRAMEWORK OF E-BANKING SERVICES

4.1 INTRODUCTION

The legal framework for banking in India is provided by a set of enactments, viz., the Banking (Regulation) Act, 1949, the Reserve Bank of India Act, 1934, and the Foreign Exchange Management Act, 1999. Broadly, no entity can function as a bank in India without obtaining a license from Reserve Bank of India under Banking (Regulations) Act, 1949. Different types of activities which a bank may undertake and other prudential requirements are provided under this Act. Acceptance of deposit from public by a non-bank attracts regulatory provisions under Reserve Bank of India Act 1934. Under the Foreign Exchange Management Act 1999, no Indian resident can lend, open a foreign currency account or borrow from a non-resident, including non-resident banks, except under certain circumstances provided in law. Besides these, banking activity is also influenced by various enactments governing trade and commerce, such as, Indian Contract Act, 1872, the Negotiable Instruments Act, 1881, Indian Evidence Act, 1872, etc. Internet banking is an extension of the traditional banking, which uses Internet both as a medium for receiving instructions from the customers and also delivering banking services.

Hence, conceptually, various provisions of law, which are applicable to traditional banking activities, are also applicable to Internet banking. However, use of electronic medium in general and Internet in particular in banking transactions, has put to question the legality of certain types of transactions in the context of existing statute. The validity of an electronic message / document, authentication, validity of contract entered into
electronically, non-repudiation etc. are important legal questions having a bearing on electronic commerce and Internet banking. It has also raised the issue of ability of banks to comply with legal requirements / practices like secrecy of customers account, privacy, consumer protection etc. given the vulnerability of data / information passing through Internet. There is also the question of adequacy of law to deal with situations which are technology driven like denial of service / data corruption because of technological failure, infrastructure failure, hacking, etc. Cross border transactions carried through Internet pose the issue of jurisdiction and conflict of laws of different nations.

This dichotomy between integration of trade and finance over the globe through ecommerce and divergence of national laws is perceived as a major obstacle for ecommerce/i-banking and has set in motion the process of harmonization and standardization of laws relating to money, banking and financial services. A major initiative in this direction is the United Nations Commission on International Trade Law (UNICITRAL)’s Model law, which was adopted by the General Assembly of United Nations and has been recommended to the member nations for consideration while revising / adopting their laws of electronic trade.

Government of India has enacted The Information Technology Act, 2000, in order to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as ‘electronic commerce’...The Act, which has also drawn upon the Model Law, came into force with effect from October 17, 2000. The Act has also amended certain provisions of
the Indian Penal Code, the Indian Evidence Act, 1872, The Bankers Book of Evidence Act, 1891 and Reserve Bank of India Act 1934 in order to facilitate ecommerce in India.

However, this Act will not apply to:

1. A negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
2. A power-of-attorney as defined in section 1A of the Power-of-Attorney Act, 1882;
3. A trust as defined in section 3 of the Indian Trusts Act, 1882;
4. A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925;
5. Any contract for the sale or conveyance of immovable property or any interest in such property;
6. Any such class of documents or transactions as may be notified by the Central Government in the official Gazette.

In the course of providing Internet banking services the banks in India are facing new challenges relating to online opening of accounts, authentication, secrecy of customers accounts, non-repudiation, liability standards and consumer protection, etc., each of which has been examined in the context of existing legal framework.

**Online opening of account:** The banks providing Internet banking service, at present are only willing to accept the request for opening of accounts. The accounts are opened only after proper physical introduction and verification. This is primarily for the purpose of proper identification of the customer and also to avoid benami accounts as also money laundering activities that might be undertaken by the customer. Supervisors
world over, expect the Internet banks also to follow the practice of ‘know your customers’.

As per Section 131 of the Negotiable Instruments Act, 1881 (the Act) a banker who has in good faith and without negligence received payment for a customer of a cheque crossed generally or specially to himself shall not, in case the title to the cheque proves defective, incur any liability to the true owner of the cheque by reason only of having received such payment.

The banker’s action in good faith and without negligence have been discussed in various case laws and one of the relevant passages from the judgment of Justice Chagla in the case of Bapulal Premchand Vs Nath Bank Ltd. (AIR 1946 Bom.482) is as follows:

“Primarily, inquiry as to negligence must be directed in order to find out whether there is negligence in collecting the cheque and not in opening the account, but if there is any antecedent or present circumstance which aroused the suspicion of the banker then it would be his duty before he collects the cheque to make the necessary enquiry and undoubtedly one of the antecedent circumstances would be the opening of the account. In certain cases failure to make enquiries as to the integrity of the proposed customer would constitute negligence”.

Further the Supreme Court of India in Indian Overseas Bank Ltd. Vs. Industrial Chain Concern [JT1989(4)SC 334] has stated that as a general rule, before accepting a customer, the bank must take reasonable care to satisfy himself that the person in question is in good reputation and if he fails to do so, he will run the risk of forfeiting the protection given by Section 131 of Negotiable Instruments Act, 1881 but reasonable care depends upon the facts and circumstances of the case. Similarly, the Delhi High Court
was also of the view that the modern banking practice requires that a constituent should either be known to the bank or should be properly introduced. The underlying object of the bank insisting on producing reliable references is only to find out if possible whether the new constituent is a genuine party or an imposter or a fraudulent rogue [Union of India Vs National Overseas Grindlays Bank Ltd. (1978) 48 Com.Cases 277 (Del)].

Thus, the introduction of a new customer by a third party reference is a well-recognized practice followed by the banks before opening new accounts in order to prove the reasonable care and absence of any negligence in permitting the new customer to open the account. Further, in order to establish the reasonable care the banks have to make enquiries about the integrity/reputation of the prospective customer. It is not a mere enquiry about the identity of the person. The Group, therefore, endorses the practice presently followed by the banks in seeking proper introduction before allowing the operations of the customers’ accounts. In the context of Internet banking and after the coming into force of the Information Technology Act, 2000, it may be possible for the banks to rely on the electronic signatures of the introducer. But this may have to await till the certification machinery as specified in the Information Technology Act, 2000 comes into operation.

Authentication

One of the major challenges faced by banks involved in Internet banking is the issue relating to authentication and the concerns arising in solving problems unique to electronic authentication such as issues of data integrity, non-repudiation, evidentiary standards, privacy, confidentiality issues and the consumer protection. The present legal
regime does not set out the parameters as to the extent to which a person can be bound in respect of an electronic instruction purported to have been issued by him. Generally, authentication is achieved by what is known as security procedure. Methods and devices like the personal identification numbers (PIN), code numbers, telephone-PIN numbers, relationship numbers, passwords, account numbers and encryption are evolved to establish authenticity of an instruction.

From a legal perspective, the security procedure requires to be recognized by law as a substitute for signature. Different countries have addressed these issues through specific laws dealing with digital signatures. In India, the Information Technology Act, 2000 (the "Act") in Section 3 (2) provides that any subscriber may authenticate an electronic record by affixing his digital signature. However the Act only recognizes one particular technology as a means of authenticating the electronic records (viz, the asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record). This might lead to the doubt of whether the law would recognize the existing methods used by the banks as a valid method of authenticating the transactions. The approach in the other countries has been to keep the legislation technology neutral. The Group is of the view that the law should be technology neutral so that it can keep pace with the technological developments without requiring frequent amendments to the law as there exists a lot of uncertainty about future technological and market developments in Internet banking. This however would not simply that the security risks associated with Internet banking should go unregulated.
Hence, Section 3(2) of the Information Technology Act 2000 may need to be amended to provide that the authentication of an electronic record may be effected either by the use of the asymmetric crypto system and hash function, or a system as may be mutually determined by the parties or by such other system as may be prescribed or approved by the Central Government. If the agreed procedure is followed by the parties concerned it should be deemed as being an authenticate transaction. A clarification to this effect by way of an amendment of the aforesaid Act will facilitate the Internet banking transactions.

Further, the banks may be allowed to apply for a license to issue digital signature certificate under Section 21 of the Information Technology Act, 2000 and become a certifying authority for facilitating Internet banking. The certifying authority acts like a trusted notary for authenticating the person, transaction and information transmitted electronically. Using a digital certificate from trusted certificate authority like a bank shall provide a level of comfort to the parties of an Internet banking transaction. Hence, it is recommended by the Committee that the Reserve Bank of India may recommend to the Central Government to notify the business of the certifying authority under Clause (o) of Section 6(1) of the Banking Regulation Act, 1949, to permit the banks to act as such trusted third parties in e-commerce transactions.

**Mode of Payment under the Income Tax Act, 1961:** Section 40A(3) of the Income tax Act, 1961, dealing with deductible expenses, provides that in cases where the amount exceeds Rs. 20,000/-, the benefit of the said section will be available only if the payment is made by a crossed cheque or a crossed bank draft. One of the services provided by the
banks offering Internet banking service is the online transfer of funds between accounts where cheques are not used, in which the above benefit will not be available to the customers.

The primary intention behind the enactment of Section 40 A of the Income tax Act, 1961 is to check tax evasion by requiring payment to designated accounts. In the case of a funds transfer, the transfer of funds takes place only between identified accounts, which serves the same purpose as a crossed cheque or a crossed bank draft. Hence, the Committee recommends that Section 40A of the Income Tax Act, 1961, may be amended to recognise even electronic funds transfer.

Secrecy of Customer's Account

The existing regime imposes a legal obligation on the bankers to maintain secrecy and confidentiality about the customer’s account. The law at present requires the banker to take scrupulous care not to disclose the state of his customer's account except on reasonable and proper occasions. While availing the Internet banking services the customers are allotted proper User ID passwords and/or personal identification numbers and/or the other agreed authentication procedure to access the Internet banking service and only users with such access methodology and in accordance with the agreed procedure are authorized to access the Internet banking services. In other words a third party would not be able to withdraw money from an account or access the account of the customer unless the customer had divulged his/her password in the first place.

However, if the password or the identification number is misplaced or lost or gets into the hands of the wrong person and such person procures details about the customers
account then the banker may be faced with legal proceedings on the grounds of violation of the obligation to maintain secrecy of the customer's accounts. This concern of the bankers is very high especially in the case of joint accounts where both the parties share one personal identification numbers or relationship numbers and operate the account jointly.

Further, by the very nature of Internet the account of a customer availing Internet banking services would be exposed to the risk of being accessed by hackers and inadvertent finders. The Internet banking services at present are being provided by most of the banks by systems which are only accessible through "secure zones" or SSL (Secure Sockets Layer) to secure and authenticate the user through a secure browser. Most of the banks have adopted 128 Bit strong encryption which is widely accepted worldwide as a standard for securing financial transaction. To reduce the risk of the customers’ account information being accessed by third parties, it is very important that the banks continue to be obliged to protect the customer account.

However, it is equally important to note that the banks may still be exposed to the risk of liability to customers and hence they should adopt all reasonable safety controls and detection measures like establishment of firewalls, net security devices, etc. Further, banks should put in place adequate risk control measures in order to minimize possible risk arising out of breach of secrecy due to loss/ misplacement/ theft of customers’ ID/PIN, etc.
Revocation and Amendment of Instructions

The general revocation and amendment instructions to the banks are intended to correct errors, including the sending of an instruction more than once. Occasionally, a revocation or amendment may be intended to stop a fraud. Under the existing law, banks are responsible for making and stopping payment in good faith and without negligence. In an Internet banking scenario there is very limited or no stop-payment privileges since it becomes impossible for the banks to stop payment in spite of receipt of a stop payment instruction as the transactions are completed instantaneously and are incapable of being reversed. Hence the banks offering Internet banking services may clearly notify the customers the time frame and the circumstances in which any stop payment instructions could be accepted.

Rights and Liabilities of the Parties

Typically, the banker-customer relationship is embodied in a contract entered into by them. The banks providing the Internet banking services currently enter into agreements with their customers stipulating their respective rights and responsibilities including the disclosure requirements in the case of Internet banking transactions, contractually. A Standard format/minimum consent requirement to be adopted by the banks offering Internet banking facility, could be designed by the Indian Banks’ Association capturing, inter alia, access requirements, duties and responsibilities of the banks as well as customers and any limitations on the liabilities of the banks in case of negligence and non-adherence to the terms of agreement by customers.
Internet Banking and Money Laundering

One of the major concerns associated with Internet Banking has been that the Internet banking transactions may become untraceable and are incredibly mobile and may easily be anonymous and may not leave a traditional audit trail by allowing instantaneous transfer of funds. It is pertinent to note that money-laundering transactions are cash transactions leaving no paper trail. Such an apprehension will be more in the case of use of electronic money or e-cash.

In the case of Internet Banking the transactions are initiated and concluded between designated accounts. Further Section 11 of the proposed Prevention of Money Laundering Bill, 1999 imposes an obligation on every Banking Company, Financial Institution and intermediary to maintain a record of all the transactions or series of transactions taking place within a month, the nature and value of which may be prescribed by the Central Government. These records are to be maintained for a period of five years from the date of cessation of the transaction between the client and the banking company or the financial institution or the intermediary. This would apply to banks offering physical or Internet banking services. This will adequately guard against any misuse of the Internet banking services for the purpose of money laundering. Further the requirement of the banking companies to preserve specified ledgers, registers and other records for a period of 5 to 8 years, as per the Banking Companies (Period of Preservation of Records) Rules, 1985 promulgated by the Central Government also adequately takes care of this concern.
Maintenance of Records

Section 4 of the Bankers’ Books Evidence Act, 1891, provides that a certified copy of any entry in a banker’s book shall in all legal proceedings be received as a prima facie evidence of the existence of such an entry. The Banking Companies (Period of Preservation of Records) Rules, 1985 promulgated by the Central Government requires banking companies to maintain ledgers, records, books and other documents for a period of 5 to 8 years. A fear has been expressed as to whether the above details of the transactions if maintained in an electronic form will also serve the above purpose. The Group is of the considered opinion that that this has been adequately taken care of by Section 7 and Third Schedule of the Information Technology Act, 2000.

Inter-Bank Electronic Funds Transfer

The Electronic Funds Transfer via the Internet, in its present form is provided only between accounts with the same bank. The transaction is effected by the originator who gives the electronic payment order to one branch of a bank offering the Internet banking facility ("the Sending Branch"). The electronic instruction is processed by the backend software of the branch to confirm the account number and the person’s identification and instruction is issued by the Sending Branch to the branch having the account of the beneficiary ("Beneficiary Branch") to credit the account of the beneficiary. The Sending Branch debits the account of the originator at its end. At present there is no clearing mechanism in place for settlement of inter-bank electronic funds transfer. The entire gamut of electronic funds transfer and the legal issues and risks involved in the same are currently being examined by a committee set up by the Reserve Bank of India. The 4th Schedule to the Information Technology Act, 2000 has amended the Reserve
Bank of India Act. 1934 empowering the Reserve Bank of India to regulate electronic funds transfer between banks and banks and other financial institutions.

**Miscellaneous**

During the course of deliberations, the Group discussed certain issues where the legal position is not clear but have a bearing on Internet banking. Certain issues have also not been addressed by the Information Technology Act, 2000. Such issues are briefly discussed below. The Consumer Protection Act 1986 defines the rights of consumers in India and is applicable to banking services as well. The issues of privacy, secrecy of consumers’ accounts and the rights and liabilities of customers and banks, etc. in the context of Internet banking have been discussed in earlier paragraphs. In cases where bilateral agreements defining customers rights and liabilities are adverse to consumers than what are enjoyed by them in the traditional banking scenario, it is debatable whether such agreements are legally tenable.

For example, whether a bank can claim immunity if money is transferred unauthorized by a hacker from a customers account, on the pretext that it had taken all reasonable and agreed network security measures. In a traditional banking scenario, a bank has normally no protection against payment of a forged cheque. If the same logic is extended, the bank providing I-banking may not absolve itself from liability to the customers on account of unauthorized transfer through hacking. Similar position may obtain in case of denial of service. Even though, The Information Technology Act, 2000 has provided for penalty for denial of access to a computer system (Section-43) and hacking (Section – 66), the liability of banks in such situations is not clear. The Group
was of the view that the banks providing Internet banking may assess the risk and insure themselves against such risks.

Bankers’ secrecy obligation mostly followed from different case laws. In UK, the Data Protection Act 1984 specifically prohibits personal data from being disclosed for purposes other than for which the data is held. This prohibits use of customer data relating to their spending habits, preferences etc., for any commercial purpose. The Office of the Controller of Currency have also issued directions to US banks enforcing customers’ privacy. The Information Technology Act, 2000, in Section 72 has provided for penalty for breach of privacy and confidentiality. Further, Section 79 of the Act has also provided for exclusion of liability of a network service provider for data travelling through their network subject to certain conditions. Thus, the liability of banks for breach of privacy when data is travelling through network is not clear. This aspect needs detailed legal examination. The issue of ownership of transactional data stored in banks’ computer systems also needs further examination.

The applicability of various existing laws and banking practices to e-banking is not tested and is still in the process of evolving, both in India and abroad. With rapid changes in technology and innovation in the field of e-banking, there is a need for constant review of different laws relating to banking and commerce. The Group, therefore, recommends that the Reserve Bank of India may constitute a multi disciplinary high level standing committee to review the legal and technological requirements of e-banking on continual basis and recommend appropriate measures as and when necessary.
4.2 E-BANKING IN INDIA – GUIDELINES

Reserve Bank of India had set up a ‘Working Group on Internet Banking’ to examine different aspects of Internet Banking (I-banking). The Group had focused on three major areas of I-banking, i.e, (i) technology and security issues, (ii) legal issues and (iii) regulatory and supervisory issues. A copy of the group’s report is enclosed. RBI has accepted the recommendations of the Group to be implemented in a phased manner. Accordingly, the following guidelines are issued for implementation by banks. Banks are also advised that they may be guided by the original report, for a detailed guidance on different issues.

4.2.1 TECHNOLOGY AND SECURITY STANDARDS

a.) Banks should designate a network and database administrator with clearly defined roles as indicated in the Group’s report.

(Para 6.2.4)

b.) Banks should have a security policy duly approved by the Board of Directors. There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems. Further, Information Systems Auditor will audit the information systems.

(Para 6.3.10, 6.4.1)

c.) Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies.

(Para 6.4.2)
d.) At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank’s system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, a stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real time security alert.

(Para 6.4.3)

e.) All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server.

(Para 6.4.4)

f.) PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services.

**Following alternative system during the transition, until the PKI is put in place:**

1. Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the banks themselves using a Certificate Server.

2. The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like passwords in transit within the enterprise itself.

(Para 6.4.5)
g.) It is also recommended that all unnecessary services on the application server such as FTP (File Transfer Protocol), telnet should be disabled. The application server should be isolated from the e-mail server.

(Para 6.4.6)

h.) All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be reported and follow up action taken should be kept in mind while framing future policy. Banks should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate their security personnel and also the end-users on a continuous basis.

(Para 6.4.7, 6.4.11, 6.4.12)

i.) The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include:

1. Attempting to guess passwords using password-cracking tools.
2. Search for back door traps in the programs.
3. Attempt to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.
4. Check if commonly known holes in the software, especially the browser and the e-mail software exist.
5. The penetration testing may also be carried out by engaging outside experts (often called ‘Ethical Hackers’).

(Para 6.4.8)
j.) Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats.

(Para 6.4.9)

k.) Banks should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank’s security policy. Business continuity should be ensured by setting up disaster recovery sites. These facilities should also be tested periodically.

(Para 6.4.10)

l.) All applications of banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form.

(Para 6.4.13)

m.) Security infrastructure should be properly tested before using the systems and applications for normal operations. Banks should upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control.

(Para 6.4.15)

4.2.2 LEGAL ISSUES

a.) 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)

b.) 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)

c.) 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)

d.) 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)
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)

4.2.3 REGULATORY AND SUPERVISORY ISSUES

As recommended by the Group, the existing regulatory framework over banks will be extended to Internet banking also. In this regard, it is advised that:

1.) Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer Internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer Internet banking services to Indian residents.

2.) The products should be restricted to account holders only and should not be offered in other jurisdictions.

3.) The services should only include local currency products.

4.) The ‘in-out’ scenario where customers in cross border jurisdictions are offered banking services by Indian banks (or branches of foreign banks in India) and the ‘out-in’ scenario where Indian residents are offered banking services by banks operating in cross-
border jurisdictions are generally not permitted and this approach will apply to Internet banking also. The existing exceptions for limited purposes under FEMA i.e. where resident Indians have been permitted to continue to maintain their accounts with overseas banks etc., will, however, be permitted.

5.) Overseas branches of Indian banks will be permitted to offer Internet banking services to their overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor.

*Given the regulatory approach as above, banks are advised to follow the following instructions:*

a.) All banks, who propose to offer transactional services on the Internet should obtain prior approval from RBI. Bank’s application for such permission should indicate its business plan, analysis of cost and benefit, operational arrangements like technology adopted, business partners, third party service providers and systems and control procedures the bank proposes to adopt for managing risks. The bank should also submit a security policy covering recommendations made in this circular and a certificate from an independent auditor that the minimum requirements prescribed have been met. After the initial approval the banks will be obliged to inform RBI any material changes in the services / products offered by them.

(Para 8.4.1, 8.4.2)

b.) Banks will report to RBI every breach or failure of security systems and procedure and the latter, at its discretion, may decide to commission special audit / inspection of such banks.

(Para 8.4.3)
c.) The guidelines issued by RBI on ‘Risks and Controls in Computers and Telecommunications’ vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4th February 1998 will equally apply to Internet banking. The RBI as supervisor will cover the entire risks associated with electronic banking as a part of its regular inspections of banks.

(Para 8.4.4, 8.4.5)

d.) Banks should develop outsourcing guidelines to manage risks arising out of third party service providers, such as, disruption in service, defective services and personnel of service providers gaining intimate knowledge of banks’ systems and misutilizing the same, etc., effectively.

(Para 8.4.7)

e.) With the increasing popularity of e-commerce, it has become necessary to set up ‘Inter-bank Payment Gateways’ for settlement of such transactions. The protocol for transactions between the customer, the bank and the portal and the framework for setting up of payment gateways as recommended by the Group should be adopted.

(Para 8.4.7, 8.4.9.1 – 8.4.9.5)

f.) Only institutions who are members of the cheque clearing system in the country will be permitted to participate in Inter-bank payment gateways for Internet payment. Each gateway must nominate a bank as the clearing bank to settle all transactions. Payments effected using credit cards, payments arising out of cross border e-commerce transactions and all intra-bank payments (i.e., transactions involving only one bank) should be excluded for settlement through an inter-bank payment gateway.

(Para 8.4.7)
g.) Inter-bank payment gateways must have capabilities for both net and gross settlement. All settlement should be intra-day and as far as possible, in real time.

(Para 8.4.7)

h.) Connectivity between the gateway and the computer system of the member bank should be achieved using a leased line network (not through Internet) with appropriate data encryption standard. All transactions must be authenticated. Once, the regulatory framework is in place, the transactions should be digitally certified by any licensed certifying agency. SSL / 128 bit encryption must be used as minimum level of security. Reserve Bank may get the security of the entire infrastructure both at the payment gateway’s end and the participating institutions’ end certified prior to making the facility available for customers use.

(Para 8.4.7)

i.) Bilateral contracts between the payee and payee’s bank, the participating banks and service provider and the banks themselves will form the legal basis for such transactions. The rights and obligations of each party must be clearly defined and should be valid in a court of law.

(Para 8.4.7)

j.) Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template. The banks should also provide their latest published financial results over the net.

(Para 8.4.8)
k.) Hyperlinks from banks’ websites, often raise the issue of reputational risk. Such links should not mislead the customers into believing that banks sponsor any particular product or any business unrelated to banking. Hyperlinks from a banks’ websites should be confined to only those portals with which they have a payment arrangement or sites of their subsidiaries or principals. Hyperlinks to banks’ websites from other portals are normally meant for passing on information relating to purchases made by banks’ customers in the portal. Banks must follow the minimum recommended security precautions while dealing with request received from other websites, relating to customers’ purchases.

(Para 8.4.9)

2. The Reserve Bank of India have decided that the Group’s recommendations as detailed in circulars should be adopted by all banks offering Internet banking services, with immediate effect. Even though the recommendations have been made in the context of Internet banking, these are applicable, in general, to all forms of electronic banking and banks offering any form of electronic banking should adopt the same to the extent relevant.

4.3  **E- BANKING IN INDIA – REVISED GUIDELINES**

As per the earlier circular DBOD No.Comp.BC.130/07.03.23/2000-01 dated June 14, 2001 banks were advised to seek prior approval of Reserve Bank of India before offering transactional services on the Internet. However vide circulation dated 20/7/05 banks were advised that while the offering of Internet Banking services continue to be governed by the provisions of the earlier circular, no prior approval of the Reserve Bank of India need to be required for offering Internet Banking services.
4.3.1 Current Legal Framework for Branchless Banking

“Banking” in India is defined as “the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawal by cheque, draft, order or otherwise.” Until 2006, banking activities could be conducted only by licensed banks and could not be outsourced.  

Pursuant to the BC Circular issued by RBI in January 2006, banks were permitted to use BCs for a variety of services: (i) identification of borrowers, (ii) collection and preliminary processing of loan applications including verification of primary information/data, (iii) creating awareness about savings and other products and education and advice about managing money and debt counseling, (iv) processing and submission of applications to banks, (v) post-sanction monitoring, (vi) disbursal of small-value credit, (vii) recovery of principal and collection of interest, (viii) collection of small-value deposits, (ix) sale of micro-insurance and other third-party products, and (ix) receipt and delivery of small value remittances and other payment instruments. Pursuant to the BC Circular, banks are liable to their customers for their BCs’ “acts of omission and commission.”

---

1 Bank Regulation Act (1949), § 5(b).
2 Ibid., §§ 5(b), 22. The law makes clear that a manufacturing or trading business that accepts deposits from the public to finance its business is not deemed to be engaged in banking.
3 RBI, Circular DBOD.No.BL.BC.58/22.01.001/2005-2006, “Financial Inclusion by Extension of Banking Services—Use of Business Facilitators and Correspondents” (hereinafter BC Circular), 25 January 2006. Business facilitators can provide only nonfinancial services and are therefore not a focus of this paper.
4 These first five listed services may also be performed by "business facilitators," which may be NGOs, post offices, IT-enabled rural outlets of corporate entities, cooperatives, insurance agents and others. RBI approval is not required for the use of business facilitators.
5 BC Circular, § 5.2(b).
While the BC Circular was an important step in facilitating bank-based branchless banking models, it also placed restrictions on the model, including (i) limiting the institutions eligible to operate as BCs to nonprofit institutions, post offices, and cooperatives and (ii) prohibiting banks from charging customers for services rendered by BCs, thereby preventing cost recovery and limiting available funds for fees to BCs.

These restrictions stymied initial product offerings and uptake, leading RBI to form a working group to assess the BC regulatory landscape and recommend suitable changes. The working group’s August 2009 report recommended that (i) a broader range of entities be allowed to serve as BCs; (ii) banks engage BCs to offer a fuller range of banking services, beyond merely opening and administering no-frills accounts; (iii) banks be permitted to charge fees to customers for using BCs; and (iv) banks provide more incentives for BCs (including better compensation, temporary overdraft facilities without charging interest, and funds for initial set-up expenses).

On 30 November 2009, largely based on the recommendations in the report of the working group, RBI issued significant revisions to the 2006 Circular. First, the revisions permit banks to charge customers “reasonable fees” for using BCs under Board-approved policies, a change that improves the business case for banks and should enable better compensation for BCs, particularly as they expand the range of services offered.

---

6 The Khan Report proposed a wider range of institutions to be permitted to act as BCs, including for-profit institutions. The list included NBFCs and “government/corporate supported IT enabled outlets which already conduct cash transactions on behalf of the corporate entities.” The BC Circular initially permitted nondepository NBFCs to be BCs; two months after the issuance of the BC Circular, RBI issued a new circular providing that only NBFCs formed as a Section 25 nonprofit company could operate as BCs.

7 BCs were also prohibited from charging customers any fee directly.

8 The BC Circular also required that all transactions be reflected on the books of the bank by the next working day. Banks have been relatively successful leveraging technology to address this requirement. ICICI, for example, launched FINO, which provides an application to easily transfer transaction data to the bank with the help of smart cards and point-of-sale terminals.

Second, the revisions expand the scope of permissible BCs to include individual “kirana” medical, and fair price shop owners; individual Public Call Office (PCO) operators; individuals who are petrol pump owners; agents of small savings/insurance schemes; retired teachers; and functionaries of well-run SHGs linked to banks. NBFCs were notably absent from the new list of permissible BCs, despite being recommended for inclusion by the working group. Many believe that MFI NBFCs would be well poised to reach underserved customers on behalf of banks, given their extensive existing physical infrastructure and customer relationships.

However, RBI appears to be concerned about commercial entities making a profit based on charges imposed on the poor, and consequently opted against NBFCs as BCs. Third, the revisions make allowances for reaching the highly underserved northeastern regions, including exemption processes for permissible BC entities and from certain accounting standards. Also, earlier in April 2009, RBI had increased the maximum distance permitted between the place of business of a BC and the bank branch, from 15 kms to 30 kms, further facilitating the expansion of BCs.

Regarding outsourcing generally, in November 2006, RBI issued outsourcing guidelines (“Outsourcing Guidelines”) for banks that prohibit the banks from outsourcing

---

10 Kirana shops are small, owner-staffed shops used by the majority of Indians (particularly rural) for basic groceries and fast moving consumer goods.

11 RBI, DBOD.No.BL.BC. 63 /22.01.009/2009-10, 30 November 2009.

their core management functions, including internal audit and decision-making functions (such as loan approval and determining compliance with know your customer (KYC) norms for opening deposit accounts). The Outsourcing Guidelines articulate “necessary safeguards” for addressing the risks inherent in outsourcing financial services, with the objective being that “the regulated entity should ensure that outsourcing arrangements neither diminish its ability to fulfill its obligations to customers and RBI nor impede effective supervision by RBI.” The guidelines specifically provide that outsourcing should not affect the rights of a customer against the bank and that the bank remains responsible for the actions of its agents. In addition, bank contracts with agents are required by the guidelines to provide RBI with the right (i) to inspect the agent and (ii) to review agents’ information and records that are relevant to the outsourced activities.

4.3.2 AML/CFT

AML/CFT issues are regulated under the Prevention of Money Laundering Act 2002. The law applies to banks and financial institutions. For banks, RBI has issued KYC guidelines and AML standards. The guidelines advise banks to categorize customers into low, medium, and high risk and to adjust identification requirements according to such risk category.

---


14 Ibid., Annex, §1.5.

15 Ibid., Annex, §§ 4.1, 4.3, 5.5.1.

16 Only the AML/CFT requirements applicable to banks are discussed because currently there are no NBFCs taking deposits, and NBFCs (other than those formed as Section 25 nonprofit companies) are not permitted to act as BCs for banks.
According to the guidelines, low-value accounts with low turnover were low risk. Notwithstanding this, banks reported that the KYC procedures remained a challenge for many low-income clients. In response, RBI issued a circular substantially relaxing the identification and proof of residence requirements for small-value accounts with a maximum account balance of Rs. 50,000 (approximately US$1,100) and maximum money deposit into the account per year of Rs. 100,000 (approximately US$2,200). For such accounts, identity and address can be proven through,

(i) introduction by another account holder who (a) went through full KYC procedures and opened an account at least six months prior and (b) can certify the applicant’s address and provide a photograph of the applicant, (or)

(ii) production of any other evidence as to the identity and address of the customer to the satisfaction of the bank.

Under this KYC regime it is unlikely that customer identification and address verification constitute a problem for small-value transactions. In October 2006, the RBI Governor announced that bank KYC procedures would be further simplified in the interest of financial inclusion.

---

17 For purposes of KYC requirements, the term “customer” includes any person with a bank account or Other relationship with the bank, any beneficial owner of an account, and any person connected with a financial transaction that can pose a significant reputational or other risk to the bank (the guidelines give as an example a wire transfer). RBI, Circular DBOD.No.AML.BC.58/4.01.001/2004-05, “Know Your Customer (KYC) Guidelines—Anti Money Laundering Standards,” 29 November 2004.
According to this announcement, for opening small accounts with outstanding balances up to Rs. 50,000 and total annual transactions up to Rs. 200,000 banks would need only a photograph of the account holder and self-certification of the account holder’s address. Unfortunately, changes have since been stalled, and it is not clear when or even if such proposed changes will be made.

However, the RBI's 2009 “Policy Guidelines for Issuance and Operation of Prepaid Payment Instruments in India”\textsuperscript{20} provide further relaxed standards for certain prepaid payment instruments. Specifically, (i) semi-closed instruments (as defined in the Guidelines and discussed in Section 3.3 below) of Rs. 1,000 or less may be issued against any identity document (provided that an issuer must insure that a customer holds only one such active instrument at any time), (ii) any prepaid instrument of Rs. 5,000 or less may be issued against any officially valid document defined as such under the Prevention of Money Laundering Act, (iii) semi-closed instruments used only for payment of utility bills or essential services up to Rs. 10,000 can be issued without any KYC by the issuer (provided that the institutions receiving payments maintain the full identity of their customers), and (iv) semi-closed instruments of up to Rs. 5,000 may be issued to companies which then may issue the instruments to their employees or other beneficiaries, provided that such companies maintain full details of their employees or other beneficiaries. Aside from these specified exceptions, the guidelines provide that all prepaid instrument issuers comply with existing AML/CFT rules.

In addition, issuers must maintain a log of all transactions undertaken using prepaid instruments, which should be available for review by RBI. RBI also allows for nonface-to-face customer identification, but only if there are specific and adequate procedures to mitigate the higher risk involved.\textsuperscript{21} The guidelines’ recommendations—certification of all documents presented and requiring the first payment to be effected through the customer’s account with another bank—are likely to create high barriers for remote account opening.

Except as noted below, for international transfers of funds, banks are required to include accurate and meaningful originator information (name, address, and account number). The information must be preserved for at least 10 years. For domestic transfers, the same applies except that there is a threshold of Rs. 50,000 (approximately US$1,100) below which only suspicious transactions require identification.\textsuperscript{22} This is an important consideration for business models built around domestic person-to-person transfers via mobile or any other electronic device.

In a promising development, the Government of India launched in 2009 a new initiative to provide all Indians with a unique identification (UID) number. The initiative, headed by Nandan Nilekani, an Indian Minister of State and one of the founders of the technology firm Infosys, is still in its initial stages and is seeking broader support throughout the government. It is expected that UIDs will voluntarily offer residents of

\textsuperscript{21} RBI, Circular UBD.BPD(PCB)MC.No.9/13.01.00/2005-06, Master Circular “Maintenance of Deposit Accounts,” 11 August 2005, Annex A to Annexure III.

India a unique identifying number that can be verified electronically via a biometrically read fingerprint. This effort could have positive implications for branchless banking efforts by removing identification risks associated with remote account opening and transactions—though there will undoubtedly be challenges posed by the expense involved in developing biometric reading infrastructure.

4.3.3 Regulation of E-Money and Other Similar Stored-Value Instruments

Until 2009, only banks and financial institutions were permitted to issue e-money and collect funds for payment to third parties.23 In April 2009, RBI issued its Prepayment Instrument Guidelines pursuant to the 2007 Payment and Settlement Systems Act. The Guidelines identify three categories of prepaid instruments, which term includes smart cards, magnetic stripe cards, Internet wallets, and mobile accounts and wallets, paper vouchers. The three categories are: (i) “closed” system payment instruments, which may be used only for the purchase of goods and services from the issuer itself and therefore, as explicitly stated, are not classified as payment systems;24

23 In 2004, RBI issued a circular announcing that only banks were permitted to issue smart cards, debit cards, stored-value cards, and value-added cards. RBI, Circular DBODNo.FSC.BC.106/24.01.019/2003-04, “Issue of Smart / Debit Cards,” 30 June 2004. Two years later, responding to the “internet based electronic purse schemes” that were cropping up, RBI announced that such schemes were “in the nature of acceptance of deposits” and therefore companies engaged in such activities were in violation of the RBI Act governing registration of deposit-taking NBFCs. RBI, Circular DBODNo.BP.BC22/08.12.01/2006-2007, “Providing Clearing and Settlement Services for internet-based electronic purse schemes,” 14 July 2006. RBI explicitly advised banks not to associate themselves with such schemes. One month later, RBI issued guidelines for cards issued by banks, including prepaid/stored-value cards RBI, Circular DBOD.FSD.BC.9/24.01.001/2006-07, Master Circular “Para-banking,” 1 July 2006, 9, Annexure 1 (also included in the more recently issued RBI, Circular DBOD.FSD.BC.18/24.01.001/2007-08, Master Circular “Para-banking” 2 July 2007,9, Annex 1).

24 Under the PSS Act, a payment system (defined as a system that enables payments to be effected between a payer and beneficiary and involves clearly, payment and/or settlement services but excluding a stock exchange) must be authorized by RBI. The Act specifically provides that such authorization is not required for payment agents, any company accepting payments from its holding company, any subsidiary thereof or any subsidiary of the receiving company, or any other company specifically exempted by RBI.
(ii) “semi-closed” payment instruments, which may be used at a group of clearly identified merchant locations and/or establishments that have contracted to accept such instruments, but which may not be used for cash withdrawal or redemption; and (iii) “open” system payment instruments, which may be used at any point-of-sale (POS) enabled merchant and for cash withdrawal at automatic teller machines (ATMs). Only banks may issue all three types of instruments (and only those banks which have been permitted by RBI to provide mobile banking transactions may launch mobile accounts and wallets). NBFCs and “other persons” may issue only semi-closed or closed instruments. There are a variety of rules regarding the issuance of these instruments, including minimum capital requirements, special AML/CFT policies, maximum value (Rs. 50,000), minimum validity period (six months), and guidelines for how they can be issued and reloaded. There are also limits on how the collected funds can be used. For example, nonbanks must keep the funds collected in a non interest-bearing escrow account with a scheduled commercial bank, and can collect interest on only a portion of these amounts, and only if other conditions are met.\(^\text{25}\) This practice ensures that banks largely continue to control and benefit from the float, and encourages nonbanks to focus only on fee-based (rather than float-based) business models.

\(^\text{25}\) While nonbanks cannot earn interest on collected funds deposited into an escrow account, nonbanks are permitted to move a “core portion” of the funds into a separate interest-earning account subject to certain additional considerations, such as continued operation for at least one year and linkage of the separate account to the escrow account to satisfy any shortfalls. The “core portion” is determined with reference to the lowest daily outstanding balance of an escrow account over a year, and it is intended to be sure that a nonbank collects interest only on stable funds not subject to the characteristic high turnover of a payments transaction account. See Prepaid Instrument Guidelines, Section 7.
In August 2009, RBI amended the guidelines to permit “Other Persons” to issue mobile phone-based semi-closed prepaid instruments, although such instruments are restricted to a maximum of Rs. 5,000 (approximately US $110) value, cannot be purchased or recharged with mobile phone airtime, and can be used only for the purchase of goods and services (i.e., no person-to-person transfers).\(^{26}\) RBI has since suggested that these revisions were intended in part to provide MNOs a way to offer customers a “mobile wallet” through banks, thus ensuring that the float would remain with banks, a clear objective of RBI.

4.3.4 Payment Systems

Until late 2007, India did not have a payment systems law. The 2007 Payment and Settlement Systems (PSS) Act, which came into force 12 August 2008, provides for the regulation and supervision of payment systems in India and establishes RBI as the authority for payment systems. Under the Act, a payment system (defined as a system that enables payments to be effected between a payer and beneficiary and involves clearly, payment and/or settlement services but excluding a stock exchange) must be authorized by RBI. Such authorization is not required, however, for payment agents, any company accepting payments from its holding company, any subsidiary thereof or any subsidiary of the receiving company, or any other company specifically exempted by RBI.

The RBI may prescribe and adopt regulations on the format of payment instructions, the standards for payment systems, the conditions for system participants participating in fund transfers, and procedures for the appointment and operation of a Board for Regulation and Supervision of Payment and Settlement Systems (BPSS) within RBI to exercise its powers and discharge its duties under the Act.

Today, only banks and the India Post may provide domestic money transfer services.27 (Although, as noted below, banks may offer mobile services as a channel for existing customers.) International money transfers into India are addressed by RBI’s Money Transfer Service Scheme,28 which permits the following institutions to receive international remittances: authorized dealers (primarily banks authorized to deal in foreign exchange under the Foreign Exchange Management Act [FEMA] 1999), RBI Licensed fully fledged money changers, NBFCs, and IATA-approved travel agents with a minimum net worth of Rs. 250,000 (approximately US$ 5,500). Prepaid instruments may be used for cross-border transactions only if the issuer is authorized under FEMA and is a participant in a payment system.29 In October 2008, RBI issued the Operative Guidelines for Mobile Banking Transactions in India pursuant to the PSS Act in acknowledgment of the growing opportunity to use mobile phones as an alternative channel for banking services.30

---

27 Indian Post Office Act (1898), Chapter IX, authorizes post offices to engage in money transfer services through money orders.
29 The Prepaid Instrument Guidelines, Art. 6.2.
30 RBI, Circular DPSS.CO.No.619/02.23.02/ 2008-09, 8 October 2008 (hereinafter Mobile Banking Guidelines).
In summary, these guidelines provided that,\(^{31}\)

(a) Only banks licensed and supervised in India \textit{and} with a physical presence in India can offer mobile banking to customers (i.e., MNOs and nonbanks cannot offer mobile banking services)

(b) Mobile banking services are limited to existing customers of banks.

(c) Cross-border and foreign currency remittances are not allowed.

(d) Services must be interoperable across MNOs within six months of offering.

(e) Daily transactions are limited to a value of Rs. 5,000 (approximately US$110) for transfers and Rs. 10,000 (approximately US$220) for purchases involving goods and services.

(f) Banks offering mobile banking services must obtain a one-time prior approval of RBI.

These guidelines also required a two-factor authentication (including mPIN) and suggested end-to-end encryption. In late December 2009, these guidelines were updated to increase the transaction limit to Rs. 50,000 on all forms of transactions and remove encryption requirements for transactions below Rs.1,000.\(^{32}\)

\(^{31}\) http://www.cgap.org/gm/document-1.9.42398/\nUpdated_Notes_On_Regulating_Branchless_Banking_India.pdf

4.4 RIGHT TO INFORMATION ACT, 2005

The Right to Information Act which replaces the Freedom of Information Act, 2002 received the assent of the President and has come into force from 12th October 2005. All public sector banks and other institutions, constituted by an Act of Parliament or owned and controlled by the Government are public authorities within the meaning of the above Act and are required to comply with the provisions of the Act. All the public authorities are required to take certain steps within 120 days from the date of commencement of the Act. One such requirement is that the public authority has to publish following particulars about its organization:

i. The particulars of its organization, functions and duties

ii. The powers and duties of its officers and employees

iii. The procedure followed in the decision making process, including channels of supervision and accountability

iv. The norms set by it for the discharge of its functions

v. The rules, regulations, instructions, manuals and records, held by it or under its control or used by its employees for discharging its functions.

vi. A statement of the categories of documents that are held by it or under its control
vii. The particulars of any arrangement that exists for consultation with, or representation by the members of the public in relation to the formulation of its policy or implementation thereof

viii. A statement of the boards, councils, committees and other bodies consisting of two or more persons constituted as its part or for the purpose of its advise, and as to whether meetings of those boards, councils, committees and other bodies are open to the public, or the minutes of such meetings are accessible for public

ix. A directory of its officers and employees

x. The monthly remuneration received by each of its officers and employees, including the system of compensation as provided in its regulations

xi. The budget allocated to each of its agency, indicating the particulars of all plans, proposed expenditures and reports on disbursements made

xii. The manner of execution of subsidy programmes, including the amounts allocated and the details of beneficiaries of such programmes

xiii. Particulars of recipients of concessions, permits or authorizations granted by it
xiv. Details in respect of the information, available to or held by it, reduced in an electronic form

xv. The particulars of facilities available to citizens for obtaining information, including the working hours of a library or reading room, if maintained for public use

xvi. The names, designations and other particulars of the Public Information Officers

xvii. Such other information as may be prescribed; and thereafter update these publications every year

xviii. Publish all relevant facts while formulating important policies or announcing the decisions which affect public

xix. Provide reasons for its administrative or quasi judicial decisions to affected persons. The Act also requires every public authority to designate Central Public Information Officers in all administrative units or offices under it as may be necessary to provide information to persons requesting for information under this Act. Section 22 of the Act provides that the provisions of the Act shall have effect notwithstanding anything inconsistent therewith contained in the Official Secrets Act 1923 and any other law for he time being in force. The effect of this provision is that the law overrides all provisions contained in the Banking Laws, which cast obligation on banks to maintain secrecy about the affairs of customers.
2. **Certain aspects of the right to information need to be noted as under,**

a) All Public Sector Banks constituted by an Act of Parliament or owned and controlled by the Government are Public Authorities within the meaning of section 2(h) of the Right to Information Act, 2005.

b) As Public Authorities, the public sector banks are required to publish information as specified in section 4 of the Act and also designate Public Information Officers under section 5 of the Act.

c) The right to information is provided to all citizens and a company or any other incorporated entity, which is not a citizen, cannot call for any information under the Act.

d) In terms of sub section 2 of section 6 an applicant making request for information is not required to give any reason for requesting the information or any other personal details except those that may be necessary for contacting him.

e) In terms of section 7(1) of the Act, any request for information is to be disposed of within 30 days of receipt of request.

f) If request for information is rejected, the concerned Public Information Officer has to record reasons for rejection, state the period within which an appeal against such rejection may be preferred and particulars of the appellate authority, in the order of rejection.
3. In regard to the exemptions provided for in section 8 of the Act, the position is as under, Clause (d) of sub-section 1 of section 8 provides for exemption from disclosure of information including commercial confidence trade secrets or intellectual property, the disclosure of which would harm the competitive position of a third party unless the competent authority is satisfied that larger public interest warrants the disclosure of such information. The expression "third party" is defined by section 2 (n) as a person other than a citizen making a request for information and includes a public authority. Since the definition of third party includes a public authority, the exemption referred to in section 8(1)(d) is available to the banks if the disclosure of information is likely to harm the competitive position of the bank itself.

4. Exemption under section 8(1)(e) - Information available in fiduciary capacity,
In cases where a bank is acting in capacity as a trustee, any information conveyed to the bank as a trustee can be treated as confidential and exempted from disclosure.

5. Section 8 (1)(j) - Personal Information, As stated above, clause (j) of sub-section (1) of Section 8 of the Right to Information Act exempts disclosure of personal information which has no relation to any public activity or interest or which would cause unwarranted invasion of the privacy of the individual. As stated above, all information relating to affairs of the customers, including persons who have furnished information for the purpose of obtaining a loan from the bank can be treated as personal information. Further all information relating to employees such as employees who have taken VRS, terminal benefits paid to such employees etc. can be treated as personal information. Also a person may ask for information of name and address of persons who
have taken car loans exceeding a particular amount or having a deposit above a specified amount, such information being personal can be declined.

6. Sub section (9) of section 7 - The form of information Sub section 9 of section 7 provides that information shall ordinarily be provided in the form in which it is sought unless it would disproportionately divert the resources of the public authority or would be detrimental to the safety or preservation of the record in question.

7. In terms of subsection (3) of section 7 it is permissible for the public authority to demand further fees being the cost of providing the information. Hence, in cases where detailed information is called for month wise or vehicle wise or any other basis that involves collection of voluminous information and high cost, such costs can be computed and conveyed to the concerned applicant as further fee to be deposited for furnishing the information.

8. Maintenance of Records, All the public sector banks are advised to maintain records for 20 years as envisaged under the Right to Information act. Such requirement would be effective from the date the Right to Information Act has come into force. Such requirement will be applicable to all existing records not yet destroyed as also to the records created after the commencement of the Right to Information Act i.e. 15th June 2005.