CHAPTER – 5

E-CHANNELS AND REGULATORY FRAMEWORK

This chapter has been divided into two parts. First part deals with the analysis of e-channels. Customers’ responses have been analyzed in order to know the customers’ perception about different e-channels. Issues of complaints have also been viewed. Second part deals with the regulatory framework for e-banking in India. The rules and regulations for e-banking given by RBI have been discussed.

5.1 E-Channels

Banking is done through different e-channels viz. ATM, net banking, mobile banking and phone banking. An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller. Using an ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and check their account balances. Mobile banking can be defined as conducting banking and stock market services, administering accounts and accessing customized information through handheld electronic communication devices like mobile or cellular phones. It is also referred to as Wireless banking, SMS banking or m-banking. The mobile technology enables the customers to pay the bill, to check account balance and cheque status, account statement enquiries, cheque book requests, to get minimum balance alerts, to request for recent transaction history and interest rates/exchange rates, and to get new product announcements on their mobile itself. Phone banking is a service provided by a financial institution which allows its customers to perform transactions over the telephone. Most telephone banking institutions use an automated phone answering system with phone keypad response or voice recognition capability. To guarantee security, the customer must first authenticate through a numeric or verbal password or through security questions asked by a live representative. With the obvious exception of cash withdrawals and deposits, it offers virtually all the features of an automated teller machine account balance information and list of latest transactions, electronic bill payments, funds transfers between a customer’s accounts, etc. Internet banking
enables a customer to perform banking transactions through the bank’s website. This is also called virtual banking, net banking, or anywhere banking. It is like bringing the bank to one’s computer at the place and time of one’s choice. This can be very useful, especially for banking outside bank hours through internet access. The number of customers who chose online banking as their preferred method of dealing with their finances is growing rapidly. Online banking usually offers features like electronic bill payment. There are growing numbers of banks that operate exclusively online due to cost advantage compared to traditional banks.

This section deals with the analysis of the customers’ responses about the usage, popularity, suitability and use of different e-channels. Also, this section reveals that the most important among all e-channels as per the customers is ATM.

5.1.1 Usage of E-Channels

E-channels which facilitate e-banking include ATM, net banking, mobile banking and phone banking. Survey has been made regarding the usage of these e-channels through a questionnaire. Customers were asked which e-channel they used the most among all. Some customers chose only ATM and some chose net banking. But there were multiple responses too. Customers used multiple channels for their banking. The usage of different e-channels can be seen through the following figures:

<table>
<thead>
<tr>
<th>E-Channel</th>
<th>Frequency</th>
<th>% (Of 500)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>443</td>
<td>88.6</td>
</tr>
<tr>
<td>Net Banking</td>
<td>307</td>
<td>61.4</td>
</tr>
<tr>
<td>Mobile Banking</td>
<td>92</td>
<td>18.4</td>
</tr>
<tr>
<td>Phone Banking</td>
<td>199</td>
<td>39.8</td>
</tr>
</tbody>
</table>

The above table shows that eighty eight percent of the customers use ATM for their banking transactions and sixty one percent use net banking. It can be concluded from the above depiction that ATM is most commonly used e-channel and second comes net banking. Phone banking and mobile banking are less in use as compared to the other two channels. Also, among the mobile and phone banking, phone banking is much in use.
5.1.2 Suitability of E-Channels

The customers were questioned as to which e-channel they found most suitable for their banking transactions. There were multiple responses in this regard. Some customers found a single channel suitable but some customers find more than one channel suitable depending upon the transaction. The responses regarding the suitability of e-channels are depicted in the below table 5.2. It can be seen from the table – 5.2 that ATM is the most suitable for banking transactions among all the e-channels. Ninety one percent of the customers find ATM most suitable for their transactions. Fifty eight percent of the customers find net banking suitable. Mobile banking’s suitability is very less considerable whereas phone banking also suits to twenty one percent of the customers.

<table>
<thead>
<tr>
<th>E-Channel</th>
<th>Frequency</th>
<th>% (Of 500)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>457</td>
<td>91.4</td>
</tr>
<tr>
<td>Net Banking</td>
<td>291</td>
<td>58.2</td>
</tr>
<tr>
<td>Mobile Banking</td>
<td>35</td>
<td>7.0</td>
</tr>
<tr>
<td>Phone Banking</td>
<td>107</td>
<td>21.4</td>
</tr>
</tbody>
</table>

These responses include multiple responses too. One customer can find two channels suitable for his/her transactions. The analysis of usage and suitability of e-channels reveals that customers find ATM the most suitable and most usable channel among all e-channels. Net banking is also considerably used and suitable for their banking transactions. Comparably phone banking and mobile banking are not so suitable to customers.

5.1.3 Frequency of using e-channels

All banking transactions are not to be transacted daily. There is a time frame involved in banking transactions. Though there is no hard and fast rule for the transactions but there can be some frequency of using e-channels. The parameters used for knowing the frequency of the usage of e-channels broadly include daily, weekly, fortnightly,
monthly and once in a two months. Following presentation shows the frequency of usage of e-channels by the customers for their banking transactions.

Chart – 5.1 Frequency of e-channel usage

The above pie presentation shows that maximum usage of e-channels is done daily and weekly. Most of the customers use e-channels for their banking transactions daily or weekly. Other parameters of frequency of usage are not of much consideration.

5.1.4 Visiting bank branches besides using e-channels

Besides using e-channels for banking transactions, customers also visit bank branches for some of the operations. The customers were asked to respond 'yes' or 'no' for whether they visited bank branches besides using e-channels. The responses are depicted through the below chart-5.2. This chart shows that out of 500, 397 customers responded yes to the question. This implies that seventy nine percent of the customers do visit bank branches besides using e-channels for their banking transactions. This shows that besides the benefits and popularity of e-channels, customers still prefer going to bank branches for some of their banking transactions.
The customers who visit bank branches for their banking transactions besides using e-channels mentioned some of their purposes of visiting bank branches.

- Issuance of demand drafts
- Investment Planning
- Cash transactions
- Opening of new accounts
- Issue of fresh currency
- Complaints
- Cheque deposit

5.1.5 Complaints regarding e-channels

Besides the benefits of e-channels and their increasing popularity, there are lots of issues that create complaints regarding e-channels. Customers do complain about the e-channels to different authorities. As can be seen from table-5.3 out of the total 500 customers, 297 customers responded yes to the issue of making complaints about e-channels to different authorities. Sixteen customers did not respond to the question of making complaints.
Table – 5.3: Complaints about E-Channels

<table>
<thead>
<tr>
<th>Response</th>
<th>Frequency</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>297</td>
<td>59.4</td>
</tr>
<tr>
<td>No</td>
<td>187</td>
<td>37.4</td>
</tr>
<tr>
<td>No Response</td>
<td>16</td>
<td>3.2</td>
</tr>
<tr>
<td>Total</td>
<td>500</td>
<td>100</td>
</tr>
</tbody>
</table>

Different channels are involved in complaint handling process. These are junior staff members of the bank, branch managers, regional heads, customer care cell of the bank itself and banking ombudsman. Customers can complain about e-channels to any of these channels. Most customers complain to the branch personnel only, it may be branch head or the junior staff members.

Table – 5.4: Complaint Channels of E-Channels

<table>
<thead>
<tr>
<th>Complaint Channel</th>
<th>Frequency</th>
<th>% (App.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junior Staff</td>
<td>98</td>
<td>33.0</td>
</tr>
<tr>
<td>Branch Manager</td>
<td>101</td>
<td>34.0</td>
</tr>
<tr>
<td>Regional Head</td>
<td>91</td>
<td>30.6</td>
</tr>
<tr>
<td>Customer Care Cell</td>
<td>7</td>
<td>2.4</td>
</tr>
<tr>
<td>Banking Ombudsman</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Total</td>
<td>297</td>
<td>100</td>
</tr>
</tbody>
</table>

Different customers gave different issues of the complaints they made regarding e-channels. Some of the complaints frequently made are listed below:

- ATM not working
- ATM PIN not been accepted by the terminal
- Mobile banking not working
- Phone banking not responding
- Net banking site down
- Delay in processing of some transaction
- Account debited twice against one transaction through ATM / Net
These are some of the issues of complaints regarding e-channels. Besides there benefits, e-channels do suffer from some limitations which give rise to these issues. To solve these issues regulatory bodies are being set up by the government.

5.2 Regulatory framework for E-Banking

This part deals with the regulatory framework for e-banking in India. The amendments made by IT Act 2000 in other acts have been adhered to.

5.2.1 Some Issues of E-Banking

The banking sector is one of the leading users of information technology worldwide. The introduction of information technology has transformed banking almost beyond belief in the last decade and a half. Most of all, customers have benefited, as have the banks themselves. There have been very significant gains in the efficiency of banks leading to greater potential for higher profitability and consequent benefit to the economy as a whole. The changes staring in the face of bankers relate to the fundamental way of banking - which is undergoing a rapid transformation in the world of today. It is widely recognized that the core banking functions alone do not add to the bottom line of banks - value added services are slowly but steadily emerging as a substantial opportunity for banks to exploit. Prime factors necessitating these changes relate to the forces of competition, productivity and efficiency of operations, reduced operating margins and the need for better asset - liability management. With hair-thin profit margins being the order of the day, the solution to this would lie in increasing volumes so as to result in better operating results for banks. This is best achieved by exploiting the benefits of technology which facilitates handling of increased volumes at higher levels of efficiency. It is in this context that there is an imperative need for not mere technology upgradation but also integration of technology with the general way of functioning of banks.

Reserve Bank of India had set up a ‘Working Group on Internet Banking’ to examine different aspects of E-Banking. The Group had focused on three major areas of e-banking, i.e., (i) technology and security issues, (ii) legal issues and (iii) regulatory and supervisory issues. The recommendations of the Group have been implemented in
a phased manner. Accordingly, the following guidelines were issued by RBI for implementation by banks.

I. Technology and Security Standards

Security and technology are the major issues which are required to be addressed. There is a considerable threat of unauthorized access/loss or damage of data by hackers; loss of damage of data by virus; and unauthorized access within the network.

a. Banks should designate a network and database administrator with clearly defined roles.

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.

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.

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 inspect all packets of information, and past and present transactions are compared. These generally include a real time security alert.

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.

f. PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. However, as it is not yet commonly available, banks should use the 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.

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.

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.

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’).

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.
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.

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.

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.

II. Legal Issues

Legal issues arise due to the geographical scope of the banking services. Working Group of RBI has raised some legal issues relating to e-banking and further RBI has provided guidelines which the banks have to meet.

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. This has to be done in order to comply with the KYC norms.

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.

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.

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.

e. 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.

III. Regulatory and Supervisory Issues:

As recommended by the Group, the existing regulatory framework over banks will be extended to e-banking also. In this regard, RBI has issued following guidelines:

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.

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.

c. The RBI as supervisor will cover the entire risks associated with electronic banking as a part of its regular inspections of banks.

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.
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.

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.

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.

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.

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.

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.
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.

5.2.2 Laws for E-Banking

There is a general misunderstanding that the entire Indian cyber law is encapsulated in the Information Technology Act, 2000. It needs to be digested that cyber law in India consists of a group of laws, each of which operates independently and also interplays with one another.

a) Indian Contract Act, 1872 and E-Banking

Every e-commerce transaction is in essence a contract. The law of contracts has been stated in the Indian Contract Act, 1872. However, sections 12 and 13 of the IT Act, 2000 have significant implications on e-contract formation and hence the necessity of a harmonious analysis of the two laws. The law of jurisdiction of courts in civil disputes is stated in the Code of Civil Procedure, 1908. Section 13 of the IT Act, 2000 has the effect of silently amending the civil law of jurisdiction insofar as civil disputes arising in the cyber world by dispatch and receipt of electronic records are concerned. Since every e-commerce transaction is a contract, it is imperative to understand the relevant aspects of the Indian Contract Act, 1872 and relate them to the IT Act, 2000. When and where an e-contract is formed, are two important questions which create a contractual relationship of rights and obligations between the parties, determine territorial jurisdiction of courts in the event of a dispute, and may also be important for deciding which legal system’s law would govern the transaction. E-Contract formation is significant in the context of the growing cross-border e-commerce. The legal validity shrink-wrap and click-wrap contract is also a significant issue. Unfortunately, in India, not much attention is being paid to draft e-contracts.
appropriate to the transaction. There is general tendency to copy others’ contracts which mostly proves to be a liability rather than a cure, in the event of a dispute. By drafting e-contracts properly, several frequent problems can be avoided. Since e-commerce transactions travel across borders with luxurious ease, there is a risk of being sued in foreign lands. In certain parts of the world such as U.S., the level of damages awarded by courts could be mind-boggling for e-businesses and e-services based in India. These and several other aspects ought to be considered while drafting e-contracts.

b) Bankers’ Books Evidence Act, 1891 and E-Banking

Several amendments have been made to the Bankers’ Books Evidence Act, 1891 by the IT Act, 2000. The definition of “bankers’ books” has been amended by IT Act, 2000 so as to include within its ambit “print-outs of data stored in a floppy, disc, tape or any other form of electronic magnetic data storage device”. The act has given certain conditions in the printout. A printout of entry shall be accompanied by a certificate that the printouts have been issued by the principal accountant or branch manager; a certificate by computer system in-charge that the safeguards have been adopted by the system to ensure the unauthorized change of the data and the accuracy of the system; and a further certificate that the information provided is to the best of the knowledge and belief of the person-in-charge of computer systems.

c) Criminal Procedure Code 1973 and E-Banking

The IT Act, 2000 defines and punishes only a few cyber crimes. Online fraud, for example, is no offence under the IT Act, 2000 nevertheless it may amount to cheating punishable under section 420 of the Indian Penal Code 1860. Although the powers of entry, search and arrest have been granted to the specified police and other officers under the IT Act, 2000, the entire procedure of criminal investigation and trial is stated in the Criminal Procedure Code 1973. The IT Act, 2000 is silent on whether the cyber crimes defined and punishable therein are bailable or non-bailable, for which one has to again travel through Criminal Procedure Code.

d) RBI Act, 1934 and E-Banking

The amendment made by IT Act, 2000 to RBI Act, 1934 has granted power for the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions refer to in clause (c) of section 45-I,
including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers.

The nature of e-banking is such that it promotes global communication in complete disregard to distances and geography. To rob a bank through internet, the robber does not have to physically go at the place of robbery to complete his task. For investigating any e-crime, evidence of the identity of cyber criminal and the weapon of offence is not available in most cases and without such evidence, the satisfaction of proof beyond reasonable doubt required in criminal cases is next to impossible. As a result, most cyber crimes go unpunished. Cross-border cyber crimes are only adding to the problems of collecting evidence and conducting investigation. Legal, judicial and sometimes political barriers have to be crossed for investigations across borders, which cause delay and are fatal to the prosecution of the accused. All the problems of evidence are due to the nature of electronic evidence, computers and the Internet, and hence are a challenge to technology and not to the Indian Evidence Act, 1872. It is the technology that needs to catch up with cyber crime, not the law.

5.3 Summary

This chapter studies the different channels of e-banking. The responses of the customers’ have been analyzed to know their perceptions about e-channels. Among all the e-channels, customers find ATM the most suitable channel for their transactions. Besides using e-channels for the banking transactions, customers still visit bank branches for some of their needs. Complaints regarding e-channels have also been viewed. Further, the regulatory framework for e-banking has been examined. Certain amendments made by IT Act, 2000 in other acts have been adhered to.