2013

Manisha Chaturvedi

[AN EXPLANATORY NOTES ON INTERNET BANKIN AND VARIOUS CREDIT CARDS]

In internet banking system the bank has a centralized database that is web-enabled. All the services that the bank has permitted on the internet are displayed in menu. Any service can be selected and further interaction is dictated by the nature of service. The term online became popular in the late '80s and referred to the use of a terminal, keyboard and TV (or monitor) to access the banking system using a phone line.

INTRODUCTION TO INTERNET BANKING

Internet banking (or E-banking) means any user with a personal computer and a browser can get connected to his banks website to perform any of the virtual banking functions. In internet banking system the bank has a centralized database that is web-enabled. All the services that the bank has permitted on the internet are displayed in menu. Any service can be selected and further interaction is dictated by the nature of service. The traditional branch model of bank is now giving place to an alternative delivery channels with ATM network. Once the branch offices of bank are interconnected through terrestrial or satellite links, there would be no physical identity for any branch. It would a borderless entity permitting anytime, anywhere and anyhow banking.

The network which connects the various locations and gives connectivity to the central office within the organization is called intranet. These networks are limited to organizations for which they are set up. SWIFT is a live example of intranet application. The precursor for the modern home online banking services were the distance banking services over electronic media from the early 1980s. The term online became popular in the late '80s and referred to the use of a terminal, keyboard and TV (or monitor) to access the banking system using a phone line. 'Home banking' can also refer to the use of a numeric keypad to send tones down a phone line with instructions to the bank. Online services started in New York in 1981 when four of the city's major banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) offered home banking services using the videotex system. Because of the commercial failure of videotex these banking services never became popular except in France where the use of videotex (Minitel) was subsidised by the telecom provider and the UK, where the Prestel system was used.

The UK's first home online banking services known as Homelink was set up by Bank of Scotland for customers of the Nottingham Building Society (NBS) in 1983. The system used was based on the UK's Prestel view link system and used a computer, such as the BBC Micro, or keyboard (Tandata Td1400) connected to the telephone system and television set. The system allowed on-line viewing of statements, bank transfers and bill payments. In order to make bank transfers and bill payments, a written instruction giving details of the intended recipient had to be sent to the NBS who set the details up on the Homelink system. Typical recipients were gas, electricity and telephone companies and accounts with other banks. Details of payments to be made were input into the NBS system by the account holder via

Prestel. A cheque was then sent by NBS to the payee and an advice giving details of the payment was sent to the account holder. BACS was later used to transfer the payment directly.

Stanford Federal Credit Union was the first financial institution to offer online internet banking services to all of its members in October 1994. Today, many banks are internet only banks. Unlike their predecessors, these internet only banks do not maintain brick and mortar bank branches. Instead, they typically differentiate themselves by offering better interest rates and more extensive online banking features.

INTERNET BANKING IN INDIA

The Reserve Bank of India constituted a working group on Internet Banking. The group divided the **internet banking products in India into 3 types based on the levels of access granted.** They are[1]:

i) Information Only System: General purpose information like interest rates, branch location, bank products and their features, loan and deposit calculations are provided in the banks website. There exist facilities for downloading various types of application forms. The communication is normally done through e-mail. There is no interaction between the customer and bank's application system. No identification of the customer is done. In this system, there is no possibility of any unauthorized person getting into production systems of the bank through internet.

ii) Electronic Information Transfer System: The system provides customer-specific information in the form of account balances, transaction details, and statement of accounts. The information is still largely of the 'read only' format. Identification and authentication of the customer is through password. The information is fetched from the bank's application system either in batch mode or off-line. The application systems cannot directly access through the internet.

iii) Fully Electronic Transactional System: This system allows bi-directional capabilities. Transactions can be submitted by the customer for online update. This system requires high degree of security and control. In this environment, web server and application systems are linked over secure infrastructure. It comprises technology covering

[1] RBI-website

computerization, networking and security, inter-bank payment gateway and legal infrastructure.

ADVANTAGE OF INTERNET BANKING

As per **the Internet and Mobile Association of India's report on online banking 2006**:

"There are many advantages of online banking. It is convenient, it isn't bound by operational timings, there are no geographical barriers and the services can be offered at a miniscule cost."

Through Internet banking, you can check your transactions at any time of the day, and as many times as you want to. Where in a traditional method, you get quarterly statements from the bank. If the fund transfer has to be made outstation, where the bank does not have a branch, the bank would demand outstation charges. Whereas with the help of online banking, it will be absolutely free. **Automated Teller Machine (ATM),** another advantage of internet banking is designed to perform the most important function of bank. It is **operated by plastic card with its special features**. The plastic card is **replacing cheque, personal attendance of the customer, banking hours restrictions and paper based verification**. There are debit cards. ATMs **used as spring board for Electronic Fund Transfer**. ATM itself can provide information about customers account and also receive instructions from customers - ATM cardholders. An ATM is an Electronic Fund Transfer terminal **capable of handling cash deposits, transfer between accounts, balance enquiries, cash withdrawals and pay bills. It may be on-line or 0ff-line. The on-line ATN enables the customer to avail banking facilities from anywhere**. **In off-line the facilities are confined to that particular ATM assigned.** Any customer possessing ATM card issued by the Shared Payment Network System can go to any ATM linked to Shared Payment Networks and perform his transactions.

INTERNET BANKING GUIDELINES IN INDIA BY RBI

RBI as issued its guidelines on Internet banking[2] that it is all set for a big growth in India. With increasing emphasis upon e-governance and **e-commerce,** Internet banking in

[2] Posted on January 4, 2013 by PTLB

India would be used more frequently. However, along with the benefits of use of Internet banking, the cyber crimes and financial fraud risks are also increasing.

Cyber security of banks in India is still not given a priority. Banks are not interested in ensuring cyber security of electronic transactions. Even the recommendations of Reserve Bank of India (RBI) to ensure cyber security, appointment of chief information officers (CIOs), establishing a steering committee at board level, etc have remained unfulfilled. Even RBI has warned banks for inadequate cyber security.

As per the **notification number DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01 of RBI,** issued on 14th June 2001, RBI has issued the following guidelines to be implemented by banks in India regarding Internet banking :

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[3].

(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[4].

(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[5].

(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

[3] (Para 6.2.4)
[4] (Para 6.3.10, 6.4.1)

[5] (Para 6.4.2)

information, and past and present transactions are compared. These generally include a real time security alert[6].

(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[7].

(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:

(i) 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.

(ii) 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[8].

(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[9].

(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[10].

---

[6] (Para 6.4.3)

[7] (Para 6.4.4)
[8](Para 6.4.5)

[9] (Para 6.4.6)
[10] (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:

(i) Attempting to guess passwords using password-cracking tools.

(ii) Search for back door traps in the programs.

(iii) Attempt to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.

(iv) Check if commonly known holes in the software, especially the browser and the e-mail software exist.

(v) The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers')[11].

(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[12].

(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[13].

(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[14].

(m) Security infrastructure should be properly tested before using the systems and applications for normal operations. Banks should upgrade the systems by installing patches

[11] (Para 6.4.8)
[12] (Para 6.4.9)

[13] (Para 6.4.10)
[14] (Para 6.4.13)

released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control[15].

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[16].

(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[17].

(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[18].

(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[19].

---

[15] (Para 6.4.15)
[16] (Para 7.2.1)

[17] (Para 7.3.1)

[18] (Para 7.5.1-7.5.4)
[19] (Para 7.6.1)

(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[20].

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:

(a) 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.

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

(c) The services should only include local currency products.

(d) 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.

---

[20] (Para 7.11.1)

(e) 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[21].

(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[22].

(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[23].

(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[24].

---

[21] (Para 8.4.1, 8.4.2)

[22] (Para 8.4.3)
[23] (Para 8.4.4, 8.4.5)
[24] (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[25].

(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[26].

(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[27].

(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[28].

(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[29].

---

[25] (Para 8.4.7, 8.4.9.1 – 8.4.9.5)
[26] (Para 8.4.7)

[27] (Para 8.4.7)
[28] (Para 8.4.7)
[29] (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[30].

(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[31].

The Reserve Bank of India has decided that the Group's recommendations as detailed in this circular 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.

All banks offering Internet banking are advised to make a review of their systems in the light of this circular and report to Reserve Bank the types of services offered, extent of their compliance with the recommendations, deviations and their proposal indicating a time frame for compliance. The first such report must reach them within one month from the date of this circular. Banks not offering any kind of I-banking may submit a 'nil' report.

Banks who are already offering any kind of transactional service are advised to report, in addition to those mentioned in paragraph above, their business models with projections of cost / benefits etc. and seek their post-facto approval.

CRIME AND FRAUDS VIS-A-VIS INTERNET BANKING

Hacking would involve someone gaining unauthorized access, to a communication between the banker and customer that may contain commercial terms, secrets or credit

[30] (Para 8.4.8)
[31] (Para 8.4.9)

details, for the purpose of either intentionally changing the contents of the communication to prejudice the interests of the parties to the communication, or using the information for some other illegal use[32]. The essence of hacking is to cause a breach in the established network security protocols and measures. An act of hacking is intensely a technological issue, and may be perpetrated with many different intentions including that of causing harm, embarrassment, disrepute and even fraud or forgery. Hence **all hacking will not constitute forgery.**

Even in case **hacking results in forgery Section 66 of the Information Technology Act, 2000** specifically provides as under:

> (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.
>
> (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto 2 lakh rupees, or with both.

This section clearly specifies that a hacker will be penalised for his actions.

Secondly, Section 79 of the Information Technology Act, 2000 excludes the liability of a network service provider to any third party if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence, or contravention.

Given that the law has deemed it fit to specifically affix responsibility for hacking, on the hackers and not on any other party other than the hackers, the bankers should not be at any cost made party for hacking or for something that did not occur with its knowledge or instruction and where it had taken all reasonable and due care within its control.

Hence it may not be unreasonable for bankers to either limit their liability or specify and require via its bilateral agreements with the customers that losses on account of hacking are not its responsibilities.

---

[32] Annexure-1 to Report on Internet Banking (Part 2 of 2) by working group-on 22 June, 2001

Further, a bank does have protection against payment of a forged cheque albeit under certain circumstances. This problem is specifically dealt with in **the Negotiable Instruments Act 1881 ("the Act"). Section 85 and 128 read with Section 10 of the said Act[33] gives statutory protection to a paying banker in regard to loss by interloper fraud subject to the conditions that the payment must have been made in good faith and in due course.** It has also been viewed that when an improper payment is made by the fact of the banker having been misled by contributory negligence or other fault on the part of the drawer, without which the forgery won't have taken place, then **the bank can set up such negligence as a defence and secure the protection under Section 85 of the said Act.** However, in order to do so, the bank must not be negligent. Thus, even with respect to the forged cheques, for occurrences beyond the control of the banker, a banker is exempted from any liability.

Under **the Information Technology Act, 2000, Section 42 clearly imposes the obligation on the subscriber to ensure that the private key is not compromised and the liability of the certifying authority for any compromise of the private key has been specifically excluded unless the subscriber informs the certifying authority of the same.**

In the light all the above submissions and given the fact that **law relating to the liability of banks on account of unauthorized transfer through hacking is still unsettled** and evolving it would not be proper for the Working Group to conclude in its Report that the bank providing internet banking may not absolve itself from liability to the customers on account of unauthorized transfer through hacking especially in the light of the fact that this Report can be used, quoted and relied by any Person in any court of law as a persuasive authority.

Thirdly, to revert to the Report of RBI, in the same paragraph 7.1 1.1, a similar conclusion has been reached with respect to denial of services. Denial of service can be either due to the circumstances beyond the control of the bank or due to non-compliance to the eligibility norms.

Very clearly, the bankers would be formulating transparent and pre-notified eligibility norms for availing of services by any person from it. Non-fulfilment of such eligibility norms would lead to denial of service by the bankers. Without probing into the actual eligibility norms, the intent of the same must be appreciated. These eligibility norms complement and

[33] the Negotiable Instruments Act 1881

supplement the know-your- customer philosophy and aids prevention as also combating money laundering, frauds, etc.

Reference drawn to the provisions of **Section 43 of the Information Technology Act,** is incorrect as the said provision states:

"if any person without the permission of the owner (the banker) or any other person who is in charge of a computer ... denies or causes denial of access to any person authorised to access any computer, computer system or computer network by any means, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."

Clearly the section appreciates that the denial has not been caused by the owner, and in fact caused by a third party, and aims at ensuring compensation being payable by such third party to the party affected.

Upon raising queries with the relevant persons when the draft Information Technology Act was made available for comments, it was clarified that in case of damages beyond Rs 1 crores, the remedy for the person affected lies in the civil courts. Clearly at no point in time, can the banker be made liable for denial of service due to circumstances beyond its control.

Security Precautions

Customers should never share personal information like PIN numbers, passwords etc with anyone, including employees of the bank. It is important that documents that contain confidential information are safeguarded. PIN or password mailers should not be stored, the PIN and/or passwords should be changed immediately and memorised before destroying the mailers.

Customers are advised not to provide sensitive account-related information over unsecured e-mails or over the phone. Take simple precautions like changing the ATM PIN and online login and transaction passwords on a regular basis. Also ensure that the logged in session is properly signed out.

NEW RBI GUIDELINES ON E-BANKING SECURITY

Apart from the card related security measures covered in the previous article, the RBI circular also touches on some of the aspects of RTGS, NEFT and IMPS. The recommendations are[34]:

1. Customer induced options may be provided for fixing a cap on the value and mode of transactions/beneficiaries. Additional authorization may be insisted when the customer wants to exceed the cap.

2. Limiting the number of beneficiaries to be added per day to be considered.

3. System alert to be introduced for 4.Number of transactions per day/per beneficiary may be monitored for suspicious transactions beneficiary addition.

5. Introduction of additional factor of authentication (preferably dynamic) for unusual transactions to be authenticated on special request.

6. Banks may consider implementation of digital signature for large value payments for all customers, to start with the RTGS transaction.

7. IP address capture for transaction may be considered.

8. "Adaptive Authentication" (means of providing authentication for end users without them having to know it is as work) may be considered for fraud detection.

These suggestions are also on the lines suggested by the **Damodaran Committee on Customer service. Though the circular uses the word "may" while referring to these suggestions, it mentions at the end that all these suggestions are "Expected" to be put in place by banks.**

[34] Post written by Vijayashankar Na at March 1, 2013

CREDIT CARDS/DEBIT CARDS:

The Credit Card holder is empowered to spend wherever and whenever he wants with his Credit Card within the limits fixed by his bank. Credit Card is a post paid card. Debit Card, on the other hand, is a prepaid card with some stored value. Every time a person uses this card, the Internet Banking house gets money transferred to its account from the bank of the buyer. The buyers account is debited with the exact amount of purchases. An individual has to open an account with the issuing bank which gives debit card with a Personal Identification Number (PIN). When he makes a purchase, he enters his PIN on shops PIN pad. When the card is slurped through the electronic terminal, it dials the acquiring bank system - either Master Card or VISA that validates the PIN and finds out from the issuing bank whether to accept or decline the transactions. The customer can never overspend because the system rejects any transaction which exceeds the balance in his account. The bank never faces a default because the amount spent is debited immediately from the customers account.

Smart cards:

Banks are adding chips to their current magnetic stripe cards to enhance security and offer new service, called Smart Cards. Smart Cards allow thousands of times of information storable on magnetic stripe cards. In addition, these cards are highly secure, more reliable and perform multiple functions. They hold a large amount of personal information, from medical and health history to personal banking and personal preferences. **One can avail following services through e-banking:**

Online Bill Payment:

You can facilitate payment of electricity and telephone bills, mobile phone, credit card and insurance premium bills as each bank has tie-ups with various utility companies, service providers and insurance companies, across the country. To pay your bills, all you need to do is complete a simple one-time registration for each biller. You can also set up standing instructions online to pay your recurring bills, automatically. Generally, the bank does not charge customers for online bill payment.

Fund Transfer:

You can transfer any amount from one account to another of the same or any another bank. Customers can send money anywhere in India. Once you login to your account, you need to mention the payees's account number, his bank and the branch. The transfer will take place in a day or so, whereas in a traditional method, it takes about three working days. ICICI Bank says that online bill payment service and fund transfer facility have been their most popular online services.

Credit Card Customers:

With Internet banking, customers can not only pay their credit card bills online but also get a loan on their cards. If one lose your credit card, one can report lost card online.

Railway Pass:

This is something that would interest all the aam janta. **Indian Railways has tied up with ICICI bank and you can now make your railway pass for local trains online.** The pass will be delivered to you at your doorstep. But the facility is limited to Mumbai, Thane, Nasik, Surat and Pune.

Investing through Internet Banking:

One can now open an FD online through funds transfer. Now investors with interlinked de-mat account and bank account can **easily trade in the stock market and the amount will be automatically debited from their respective bank accounts and the shares will be credited in their de-mat account.** Moreover, some banks even give you the facility to purchase mutual funds directly from the online banking system. Nowadays, most leading banks offer both online banking and de-mat account. However, if you have your de-mat account with independent share brokers, then you need to sign a special form which will link your two accounts.

Recharging prepaid phone:

Now just top-up your prepaid mobile cards by logging in to Internet banking. By just selecting your operator's name, entering your mobile number and the amount for recharge, your pone is again back in action within few minutes.

Shopping :

With a range of all kind of products, you can shop online and the payment is also made conveniently through your account. You can also buy railway and air tickets through internet banking.

How do credit cards work?

The Reserve Bank of India is doing its best to encourage alternative methods of payments which will bring security and efficiency to the payments system and make the whole process easier for banks. The Indian banking sector has been growing successfully, innovating and trying to adopt and implement electronic payments to enhance the banking system. Though the Indian payment systems have always been dominated by paper-based transactions, e-payments are not far behind. Ever since the introduction of e-payments in India, the banking sector has witnessed growth like never before. According to a survey by Celent, the ratio of e-payments to paper based transactions has considerably increased between 2004 and 2008. This has happened as a result of advances in technology and increasing consumer awareness of the ease and efficiency of internet and mobile transactions.

In the case of India, the RBI has played a pivotal role in facilitating e-payments by making it compulsory for banks to route high value transactions through Real Time Gross Settlement (RTGS) and also by introducing NEFT (National Electronic Funds Transfer) and NECS (National Electronic Clearing Services) which has encouraged individuals and businesses to switch to electronic methods of payment. With the changing times and technology so have changed the methods of payments in India. E-payments in India have been growing at a fast rate of 60% over the last 3 years.

In India ‘plastics’ have been fast over-taking ‘papers’. With 130 million cards in circulation currently, both credit and debit, and an increasing consumer base with disposable income, India is clearly one of the fastest growing countries for payment cards in the Asis-Pacific region. Behaviourial patterns of Indian customers are also likely to be influenced by their internet accessibility and usage, which currently is about 32 million PC users, 68% of whom have access to the net. However these statistical indications are far from the reality where customers still prefer to pay “in line” rather than online, with 63% payments still being made in cash. E-payments have to be continuously promoted showing consumers the various routes through which they can make these payments like ATM’s, the internet, mobile phones and drop boxes.

The Indian payments systems have however undergone a change with respect to methods of payments, there now being card-based payments, Electronic Funds Transfers, Electronic Clearing Services and ways to pay via the mobile and internet. In India payments can be divided in two ways- firstly, large-scale payments and small-scale payments and secondly, paper-based and electronic. Most large-scale payments concern corporate or government payments and are settled by the RBI. Small-scale payments are mainly retail payments concerning individuals which are generally paper-based transactions. Most large-value payments are handled electronically. However, even the retail payments are showing a tendency of shifting to the e-payment mode, mainly because of consumer awareness and regulations by the RBI.

HOW FAR HAS INDIA MOVED TO AN E-PAYMENT SYSTEM?

India Data Talk[35]: Electronic payment systems have become increasingly popular in India. In fiscal year 2012, electronic payments grew 26.8% to 1.21 billion transactions from 0.96 billion transactions in fiscal year 2011, while the amount of cheque clearance slid from 1.39 billion units to 1.34 billion units over the same period. In terms of total transaction value, 98% of all electronic payments consist of large value payments through real time gross settlement (RTGS) systems, and the remaining 2% comes from retail electronic payments, including credit cards, debit cards, electronic clearing services (ECS) credit and debit payments, and electronic funds transfers (EFTs). The picture was just the opposite in terms of total transaction volume – only 4.5% of transactions came from payments through RTGS systems, while retail electronic payment transactions acc! ounted for the other 95.5%.

The growth in electronic payments was largely evident in the growth of large value transactions through the RTGS system. Introduced in March 2001, the RTGS system was primarily meant for large value transactions to settle customer remittance and inter-bank transactions of values over INR 2 lakh (INR 0.2 million). Within five years, the volume of transactions on the RTGS system had increased almost tenfold, from 5.85 million units in fiscal year 2008 to 55.05 million units in fiscal year 2012.

[35] Posted by **India CEIC Database Team**, as on August 27, 2012

CONCLUSION:

In conclusion, as has been rightly noted by the Working Group that "the applicability of various existing laws and banking practices to e-banking is not tested and is still 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 establishment of the multidisciplinary high level standing committee to review the legal and technological requirements of e-banking on a continual basis and recommendations of appropriate measures as and when necessary would really be a panacea for legal clarifications as and when they arise.

The key in such future and further deliberations would be to encourage banks towards innovation and where necessary or required evolve new practices and customs to complement the banking laws in force from time to time.