Legal Regulations on Internet Banking

Dr. V.K. Unni
Professor
IIM Calcutta
E-mail: unniv@iimcal.ac.in

Internet Banking

- Internet banking means a system that enables bank customers to access accounts and general information on bank products and services through a personal computer or similar systems.
- Across the globe two broad business models of Internet banking have emerged.
- First, Internet banking within existing banks, as an extra channel for their traditional services provided by traditional branches, for e.g. SBI may offer its customers the facility of Internet Banking
- Second is standalone entities, which are Internet-only banks, owned by new players entering the banking industry, in India as of now such systems are not there

Internet Banking

Presently almost all banks use their Internet presence to provide the following types of Internet banking services:

1. **Informational**--this is the most fundamental level of Internet banking and here the bank uses the Internet as a delivery tool to provide general information for promoting their various investment plans
   - Here the risk is relatively low, as informational systems typically have no connection between the server and the bank's internal network.
2. **Communicative**—Here there will be contacts between the bank's system and the customer.
   - At the basic level the customer may wish to apply to open an account or request products and services

Internet Banking

- At an intermediary level, the bank allows clients to view their transaction history, order new cheques, view mini statement or print out balance statements.

3. **Transactional**—This is the most sophisticated level of Internet banking and here the customer can access his account in order to carry out several transactions such as fund transfers and bill payments.

- Thus it becomes clear that only in the cases of communicative and transactional service, there is a connection between the server and the bank or outsourcer's internal network.
- Thus only in these two services the level of risk reaches its peak and thus sufficient care should be taken by all the concerned parties.

Internet Banking

- In 2001 RBI has appointed a “Working Group on Internet Banking” which focused on three major areas of I-banking, i.e., (i) technology and security issues, (ii) legal issues and (iii) regulatory and supervisory issues.

Technology and Security Standards:

- Banks should designate a network and database administrator with clearly defined roles
- Banks should have a security policy duly approved by the Board of Directors.

Internet Banking

- 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
- 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.

Internet Banking

- 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.
- For sensitive systems, a stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared
- 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 an alternative system called SSL until the PKI is put in place
- SSL (Secured Socket Layer), ensures server authentication

Internet Banking

- 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
- The information security officer and the information system auditor should undertake periodic hacking tests of the system, which should include: Attempting to guess passwords using password-cracking tools

Internet Banking

- 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
- 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

Internet Banking

Legal Issues:

- 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
- The security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature.
- In India, the IT Act, 2000 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

Internet Banking

- The risk of banks failing to maintain secrecy and confidentiality of customers` account is high in the case of net banking
- Banks should, therefore, institute adequate risk control measures to manage such risks.
- 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

Internet Banking

- 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
- 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

Internet Banking

Regulatory and Supervisory Issues:

- The banks operating in physical world are regulated and supervised by the RBI on regular basis.
- This regulation and supervision is required to be extended to Internet banking as well.
- 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.

Internet Banking

- The net banking products should be restricted to account holders only and should not be offered in other jurisdictions.
- The services should only include local currency products.
- 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 home supervisor.
- All banks, who propose to offer transactional services on the Internet, should obtain prior approval from RBI.
- Banks will have to 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.

Internet Banking

- 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
- Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template.

Internet Banking

- 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
- The RBI has directed that all banks offering Internet banking services, with immediate effect, should adopt the Group's recommendations.

Internet Banking

Phishing

- Phishing uses e-mail messages that purport to come from legitimate businesses that one might have dealings with -- banks such as Citibank; insurance agencies
- The messages may look quite authentic, featuring corporate logos and formats similar to the ones used for legitimate messages.
- Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes.

Internet Banking

- Since these e-mails look so official, many unsuspecting recipients may respond to them, resulting in financial losses, identity theft and other fraudulent activity against them

Spoofing

- Spoofing refers to intentionally deceiving an Internet user into believing the website or e-mail he/she is viewing is authentic as to its apparent origin, when in reality it was developed and/or communicated by another entity.
- Websites can also be spoofed to make the site appear to come from a trusted source, when it was actually generated by another disguised host.

Internet Banking

- A spoof website is one that mimics another website to lure a customer into disclosing confidential information
- To make spoof sites seem legitimate, spoof web sites use the names, logos, graphics and even code of the real bank's site.

Phone Phishing

- Not all phishing attacks use a fake website, even a phone can be used for this
- In an incident in 2006 messages that claimed to be from a bank told users to dial a phone number regarding a problem with their bank account.
- Once the phone number (owned by the phisher, and provided by a Voice over IP provider) was dialed, prompts told users to enter their account numbers and PIN

Credit Cards

- Credit cards are more than simple payment devices - they provide direct access to a line of credit.
- While the credit is important in its own right, it has larger implications as well.
- The financial institutions that sign up either cardholders or merchants are functioning as financial intermediaries, and by providing that intermediating function, minimize the risk to the transacting parties.
- The intermediaries charge for these services through a discount rate charged to merchants and through interest charges and service fees charged to cardholders.

Credit Cards

- Because the credit card system is a closed system, in which no one can participate as a cardholder, merchant, card issuer or financial intermediary without agreeing to be bound by the system rules, the fact that a merchant accepts credit cards provides consumers with a guarantee of recourse in the event of a dispute in the underlying transaction.
- Similarly, the card issuer screens cardholder's creditworthiness for merchants.
- The four parties involved in a typical credit card transaction are: (1) the person using the credit card, known as the cardholder; (2) the merchant who uses credit cards as a way to allow customers to pay for goods and services; (3) those banks that issue cards to cardholders, known as issuer banks; and (4) those banks that deal with the merchant (known as merchant banks) in establishing credit accounts for the merchant

Secure Electronic Transactions ("SET")

- Standardization is an essential element of any widely distributed system for electronic commerce, and the development of technical standards for interoperability between vendors of electronic payment services has been no exception.
- Leading players such as Visa and MasterCard have attempted to seize the initiative in innovative electronic payment systems by controlling the development of technical standards.
- This, in turn, would guarantee a continued role for their proprietary payment services in the electronic commerce markets of the future.
- The vast financial resources that they can command have been poured into the development and marketing of the Secure Electronic Transactions ("SET") standard, which, if widely adopted, would permit the use of advanced encryption technology in credit card transactions and would help preserve the dominance of credit cards among electronic payment services.

Secure Electronic Transactions ("SET")

- The promise of asymmetric cryptography, in the form of digital signatures, to resolve some of the new security issues raised by conducting business over open, public computer networks was widely recognized in the technology community a decade ago.
- Without standards to facilitate the adoption of cryptography, however, there was no way for application developers to realize its promise.
- Visa and MasterCard initially began work on separate standards for the use of public key cryptography in connection with electronic funds transfers, but in 1996 decided to join forces in developing a single standard for secure electronic transactions, or SET.

Secure Electronic Transactions ("SET")

- In 1997, SET was widely expected to make the Internet safe for electronic commerce by resolving some of the uncertainty that prospective transactors felt about the security of Internet transmissions.
- SET would require each cardholder, financial intermediary and merchant to use a digital signature certificate in Internet transactions.
- Consumers would send their signed orders to Internet merchants together with encrypted credit card information that would be passed on, unread, to the financial intermediary. The intermediary would process the credit card authorization and notify the merchant, who would then complete the transaction with the consumer

Secure Electronic Transactions ("SET")

- The SET system ran into problems almost from the outset, and by early 1999 was no longer in the forefront of discussions about Internet commerce security.
- While SET may be a very sophisticated system for improving the security of electronic funds transfers over open networks such as the Internet, it is also a complex and cumbersome one.
- The operation of SET procedures seemed likely to be too demanding of existing computers and networks
- Notwithstanding the outpouring of support for SET, by now it is established that SET had failed to garner any significant share of the U.S. market and achieved only a few isolated implementations outside the U.S

Secure Electronic Transactions ("SET")

- Secure Sockets Layer ("SSL"), The Secure Sockets Layer ("SSL") standard, developed by the Netscape as a simple, stop-gap solution pending the development of more sophisticated standards such as SET, has achieved widespread acceptance as the standard for communicating credit card information over the Internet.
- It represents an unusual situation where technology has enhanced the position of other payment systems in Internet commerce.
- SSL lacks the elegance and coherence of SET, but it has come to dominate the market for retail electronic commerce by meeting the minimum requirements of the relevant stakeholders.

Secure Electronic Transactions ("SET")

- The SSL standard does not use digital signatures to bind human identities to online communications.
- Instead, it relies on the use of a digital certificate to identify a computer, the e-commerce server.
- The consumer's browser validates the server's certificate, and then uses the public key in the certificate to share a symmetric key with the server.
- For the remainder of the session, the shared symmetric key is used to encrypt communications between the browser and the server, preventing credit card or other sensitive information from being sent over the Internet.

SSL

- The SSL standard has proven highly successful because it does not place excessive demands on the average consumer's home PC and has removed what was one of the most pressing concerns associated with Internet commerce: the public nature of its communications infrastructure.
- The SSL standard does not address the security of credit card information once it is on the merchant's e-commerce server, nor does it provide any information about which human being entered the credit card information transmitted to the vendor.
- Purchasers have been happy with the level of protection provided by SSL because the normal consumer-friendly credit card system rules apply.

PSS ACT 2007

Payment and Settlement Systems Act, 2007 (PSS Act, 2007)

- The PSS Act, 2007 provides for the regulation and supervision of payment systems in India and designates the RBI as the authority for that purpose and all related matters
- The Act provides the legal basis for "netting" and "settlement finality".
- This has great significance, because in India, other than the Real Time Gross Settlement (RTGS) system all other payment systems function on a net settlement basis.

PSS ACT 2007

- Under the PSS Act, 2007, RBI passed the Payment and Settlement Systems Regulations, 2008.
- It covers matters like

1. form of application for authorization for commencing/ carrying on a payment system
2. grant of authorization, payment instructions and determination of standards of payment systems, furnishing of returns/documents/other etc

PSS ACT 2007

- PSS Act 2007 defines terms like payment obligation, payment instruction, payment system etc
- "Payment obligation" is defined as what is owed by one participant in a payment system to another such participant which results from clearing or settlement or payment instructions relating to funds, securities or foreign exchange or derivatives or other transactions
- Payment Instruction" is defined as any instrument, including electronic means, to effect a payment by a person to a participant in a payment system or from one participant in such a system to another participant in that system

PSS ACT 2007

- "Settlement" means the settlement of payment instructions received and these include settlement of securities, foreign exchange or derivatives or other transactions
- RBI has issued various directives under PSS Act 2007 one recent such directive (2009) deals with the additional authentication/validation based on information not visible on the cards for all cards not present transactions
- It also mandates a system of "Online Alerts" to the cardholder for all 'card not present' transactions of the value above a particular amount

Thank You

Dr. V.K. Unni
Professor
IIM Calcutta
E-mail: unniv@iimcal.ac.in