"E-BANKING PRACTICES IN SELECTED PUBLIC AND PRIVATE SECTOR BANKS"

M. SREE SAKTHI VELAN,
MBA, M.Com, M.Phil., (Phd),
FACULTY IN MANAGEMENT STUDIES, K.S.R. COLLEGE OF ENGINEERING, TIRUCHENGODE.

DR. V. BALACHANDRAN,
MCS, MBA, M.Com, M.Phil., Phd,
PROFESSOR IN CORPORATE SECRETARYSHIP, ALAGAPPA UNIVERSITY, KARAIKUDI

E-BANKING:

Internet banking involves consumers using the Internet to access their bank account and to undertake banking transactions. At the basic level, Internet banking can mean the setting up of a Web page by a bank to give information about its product and services.

At an advance level, it involves provision of facilities such as accessing accounts, funds transfer, and buying financial products or services online. This is called ``transactional" online banking.

There are two ways to offer e-banking:

i.) an existing bank with physical offices can establish a web site and offer Internet banking in addition to its traditional delivery channels.

ii.) a bank may be established as a "branch less, Internet only, or virtual bank" without any physical branch.

SERVICES OFFERED THROUGH E-BANKING:

In general, Internet banking products are offered,

* *A **basic tier** internet banking products includes,*
Customer account inquiry
Funds transfer and
Electronic bill payment.

* *A **premium tier** includes,*
1) Brokerage.
2) Cash management.
3) Credit applications.
4) Credit and debit cards.
5) Customer correspondence.
6) Demat holdings.
7) Financial advice
8) Foreign exchange trading.
9) Insurance.
10) Online trading.
11) Opening accounts
12) Requests and intimations.
13) Tax services.
14) E-shopping.
15) Standing instructions.
16) Investments.
17) Asset management services etc.

E-BANKING Vs. TRADITIONAL BANKING:

S. NO.	E-BANKING	TRADITIONAL BANKING
1.	It enables the customers to perform the basic banking transactions by sitting at their homes or at offices through a desktop or laptop round the clock globally through electronic media.	The customer has to visit the branch of the bank in person to perform the basic banking operations. **viz.,** account enquiry, funds transfer, cash withdrawing etc.,
2.	Customers can make use of these services with no restricted banking hours, no queues, no tellers and no waiting.	Restricted banking hours and procedures.
3.	The customers can access the banks' website for viewing their account details and perform the transactions as per their requirements.	Restricted banking hours and procedures.
4.	It is also called as, "Any time, Any where banking."	Restricted banking hours and procedures.

FUNDAMENTALS:

Internet banking (or E-banking) means any user with a personal computer and a browser can get connected to his bank -s 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. 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:

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

EXAMPLES:

Automated Teller Machine (ATM):

ATM 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.

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 customer’s account.

Smart Card:

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. Currently around 78 per cent of the bank's customer base is registered for Internet banking."

To get started, all you need is a computer with a modem or other dial-up device, a checking account with a bank that offers online service and the patience to complete about a one-page application--which can usually be done online.

ADVANTAGES OF E-BANKING:

(i) Round the clock banking :

E-banking facilitates performing basic banking transactions by customers round the clock globally. In fact there is no restricted office hours for E-banking.

(ii) Convenient Banking:

Customers can perform basic banking transactions by simply sitting at their office or at home through PC or LAPTOP. No personal visit to the branch is required for routine basic transactions.

(iii) Low Cost Banking:

The operational costs have come down due to technology adoption. The cost of transactions through internet banking is much less than any other traditional mode. There is also much saving on the cost of infrastructure as the banks can have access to a greater number of potential customers without the commitment costs of physically opening branches. Moreover, requirements of staff at the banks get reduced to a greater extent.

(iv) Profitable Banking:

The increased speed of response to customer requirements, can enhance customer satisfaction and consequently can lead to higher profits as a result of handling more number of customer accounts.

(v) Quality Banking:

Internet banking allows the possibility of improved quality and an enlarged range of services being made available to customers.

(vi) Speed Banking:

The increased speed of response to customer requirements will lead to greater customer satisfaction and handling a large number of transactions at a lesser time. Thus, it increases the customers' convenience to a greater extent and facilitates better customer retention.

(vii) Service Banking:

Banks can also offer many cash management products. Instant credit, one day credit, immediate payment of utility bills, instant transfer of funds etc., is possible under E-banking.

CONSTRAINTS IN E-BANKING :

Although there are obvious benefits in Internet Banking , there are some hurdles in the smooth implementation of Internet-banking.

(i) Start-up cost :

The initial start-up cost for venturing into e-banking is on the higher side and it includes the following:

Connection cost to the Internet or any other mode of electronic communication

Cost of sophisticated hardware, software and other related components like

Modem, Router, Bridges, network management system

Cost of maintenance of all equipment, web sites, skill level of employees

Cost of setting up organizational activities

(ii) Training and Maintenance:

The introduction of Internet banking involves 24 hours support environment, quality service to end users and other partners which would necessitate a well qualified and robust group of skilled people to meet external and internal commitments. Hence the bank has to spend a lot on training.

(iii) Lack of skilled personnel:

It is a well known fact that there is an acute scarcity of web developers, content providers and knowledgeable professionals to route banking transactions through internet.

(iv) Security:

A security threat is defined as a circumstance decision or event with potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of services, fraud, waste and abuse.

There are chances that the documents such as cheque, passbook etc., can be modified without leaving any visible trace. Distortions of information are also possible. Providing appropriate security may require a major initial investments in the form of application encryption require a major investments in the form of application encryption techniques, implementation of firewalls etc.,

(v) Legal Issues:

Legal framework for recognizing the validity of banking transactions conducted through the ' NET' is still being put in place. Though initial legal framework has been devised for E-banking activities, it is uncertain as to what possible legal issues may pop up in future as banking on Internet progresses.

(vi) Restricted clientele and technical problems:

The user of E-Banking needs a computer and time to log on to the site, which means that the target clientele is restricted to those who have a home PC or can access the 'Net' through the office or cyber cafe. Moreover technical constraints due to telephone connectivity, modem connections etc., may cause constraints.

SECURITY MEASURES TOWARDS E-BANKING:

Most of the problems mentioned above are in the nature of teething problems and hence they can be eliminated over a period of time.

However, for venturing into E-Banking, the following major controls must be ensured:

 # Authenticity controls:

To verify identity to individuals like password, PIN etc.,

 # Accuracy control:

To ensure the correctness of the data, flowing across the network.

 # Completeness control:

To make sure that no data is missing

 # Redundancy controls:

To see that data is traveled and processed only once and there is no repetitive sending of data.

 # Privacy controls:

To protect the data from inadvertent or unauthorized access

 # Audit Trail Controls:

To ensure keeping chronological role of events that are occurred in the system.

 # Existence controls:

To make sure that on going availability of all the system resources with the same throughout

 # Efficient:

To ensure that the system uses minimum resources, to achieve the desired goal.

 # Fire wall controls:

To prevent unauthorized users accessing the private network, which are connected to Internet.

 # Encryption controls:

To enable only those who possess secret key to decrypt the cyber text.

SOME RECENT ISSUES ABOUT E-BANKING:

"Consumer Confidence In Online Banking Declines"

Consumers are increasingly worried about the safety and security of Internet banking. The attitude shift is occurring even as more people move to online banking.

According to a new consumer survey from Informa Research Services, consumer attitudes toward Internet-based banking transactions have changed for the worse. Confidence, which had been on the rise from 2000 to 2003, moved sharply lower in the latest survey.

"Where there was consistent growth from 2000 to 2001 (+7%) and 2001 to 2003 (+14%) in the number of consumers who completely or strongly agreed with the statement, 'Internet based transactions handled by financial institutions are safe and secure,' there was a significant decrease (-11%) from 2003 to 2005," says Paul Lubin of Informa.

The findings are in line with the results of a survey conducted earlier in the year by the Conference Board and TNS NFO, which found almost 60% of US households were "extremely concerned" about banking online.

But online banking continues to grow more common. "The amount of consumers who reported having used the Internet for a financial transaction in the past six months rose 15% from 2003 to 2005 despite the decline in perceived Internet banking security," says Mr. Lubin. "As consumers become more adept with Internet based financial transactions, they are also becoming more concerned about the safety and security of Internet banking."

Fortunately, there are steps banks can take to remedy the situation. The Ponemon Institute polled consumers to find out what would make them feel more secure about banking online. Limiting third-party sharing of information was at the top of the list.

(source: emarketer, orginally published at: http://www.emarketer.com/Article.aspx?1003527)

"Internet Banking Security: Separating Fact From Fiction:"

Businesses across the country must keep things in perspective and shouldn't lose faith in Internet banking just because there have recently been a series of highly publicized data breaches. These incidents, while regrettable, have absolutely nothing to do with online banking, which is a very safe and secure channel for both consumer and commercial banking transactions.

Indeed, the latest and most comprehensive research, conducted by phone among 4,000 consumers by Javelin Strategy & Research, shows that identity theft is more prevalent off-line with paper than online and that Internet-related fraud problems are less severe and generally less costly than paper-related fraud. Also, Internet-related fraud isn't as widespread as many people believe.

The most frequently reported source of information used to commit fraud was a lost or stolen wallet or checkbook; computer crimes accounted for just 11.6% of all known-cause identity fraud in 2004 -- and half these digitally driven crimes stemmed from spyware, software the computer user unknowingly installed to make ads pop up when the consumer is online.

Among cases where the perpetrator's identity is known, half of all identity fraud is committed by a friend, family

member, relative, neighbor or in-home employee -- someone known by the victim.

The majority of actual identity fraud crimes in the U.S. are self-detected. This reinforces the benefits of activity monitoring through electronic review of transactions, statements and credit reports that allow consumers to check their account activities quickly and efficiently -- without waiting for a paper bill or statement. Victims of identity theft who detected the crime by monitoring accounts online experienced financial losses that were less than one-eighth of those who detected the crime via paper statements. Still, online fraud remains a risk. So what can your business do?

For starters, you can assess your financial institutions. In most cases, the financial sector has been out front in implementing more rigorous security measures -- not only because it's entrusted with sensitive account information, but also because this sector is highly regulated. Yet there is still quite a difference in the way security measures are implemented across the financial industry; for example, not all firms require their corporate customers to use two-factor authentication for any monetary transactions.

Consider the following factors when evaluating your bank's commitment to safeguarding your accounts and information:

State-of-the-art technology. Data centers should be protected with state-of-the-art technology that includes extensive firewalls and Secure Sockets Layer encryption for data communications between customers and the bank.

Round-the-clock monitoring. Check that all transactions are monitored around the clock to flag unauthorized modification, destruction or disclosure (whether accidental or intentional) as well as to ensure the authenticity, integrity, availability and confidentiality of that information.

Secured data centers. Data centers should be unmarked, in locations dispersed throughout the country and protected by extensive physical security controls, including cameras, guards, man traps, biometric identification and locked storage.

Privacy protection. Ensure that confidential information is restricted to only those who are authorized to have access, that all sensitive data on employees' computers is automatically encrypted and that unauthorized log-in attempts are blocked. Beyond these basic security measures, you should also look for ways to gain added control over your business transactions and accounts. Consider some of these extra controls:

Administrative controls. Tools that allow you to authorize which of your employees can access which accounts, data and services online.

Fraud prevention. There are a host of fraud-prevention tools such as basic positive pay and positive pay with payee validation, stop-payment services and automated clearinghouse (ACH) fraud filter. All these services are readily available round-the-clock online and will allow you to quickly flag suspect transactions. Coupled with e-mail alerts that notify you directly when suspect transactions are waiting your review, these go a long way toward preventing fraud.

Electronic payments. If you have a high volume of check payments, consider moving to electronic payments to give you automated control points, whether via ACH, wires or check conversion. And online reporting helps you keep a constant watch over all transactions.

Our customers place a great deal of trust in financial services sector to safeguard their accounts and financial information. It's up to the entire industry to honor that trust by continually investing in the highest standards of security and safety.

(source: computer world, originally published at: http://www.computerworld.com/securitytopics/security/story/0,10801,103035,00.html)

"Banks and regulators link arms to fight online fraud"

While online identity theft has been big news worldwide in the past year, Hong Kong seems to be weathering the scourge effectively.

Despite the large amount of business that runs through Hong Kong's Internet networks, banks, working closely with the Hong Kong Monetary Authority, seem able to keep the local fraud rate low.

The Hong Kong Monetary Authority's online banking analyst Li Shu-pui says that transparency between banks and regulators is the key.

``We are 100 percent supporting transparency, because it's a very good way to educate the public about online security," Li said. ``We're probably the most transparent Internet regulators in the world," he said. Li added that the authority dispatched 50-60 press releases last year alerting the public to trends in online security threats. Rather than adopt a legislative approach, the authority believes that keeping a clear line of communication between the regulator and the banks was the safest and most efficient way to go.

``We have told the banks to monitor any unusual activities," said Li. ``If they notice unusual activity, they have to notify customers."

Since 2003, when ``phishers" began sending out millions of fake e-mails to unwitting customers and lured them into revealing online data, the Hong Kong Monetary Authority has demanded that all the city's big banks begin introducing ``two-factor authentication," a system of encryption and two-step security procedures that safeguard customers from online piracy.

It seems to be working. The Hong Kong Police Force's Technology Crime Division keeps a record of online and computer security crimes. The numbers are admirably low. Only 19 people suffered online theft in 2004, according to the division's data. There were only 11 reported cases of illegal access attempts via telecommunications equipment last year, down dramatically from 275 in 2000.

``Our aim is to do firefighting, to handle incidents. The most important [thing we do] is [teach] how to prevent incidents from happening," said Li. He cited online security interactive games available on the Web, pamphlets, on-the-spot checks of banks and their online facilities and the flurry of press releases the government body distributes to banks and customers. There is also an E-Banking Working Group, set up by the Banking Association at the end of 2002, with members from the police, seven major local and international banks and the monetary authority.

Most banks are reluctant, however, to discuss specifics. Caoimhe Buckley, corporate affairs spokeswoman for Standard Chartered Bank, said that it was unlikely that anyone at her bank would want to disclose any information about online security.

``It's not a subject [to which] we want to give too much voice," she said. ``The more we tell, the more vulnerable we become, and we don't want to leave a negative sentiment ... nor do we want to appear too confident. We're not going to disclose any of our security measures."

At the Bank of China, a spokesman said no one was available for comment.

``As a bank in Hong Kong we are required to report every type of security breach to the monetary authority," said Peter Brooks, online banking manager for HSBC.

The bank started deploying its two-factor authentication system in May - a small random number generating device, which online customers will have to use to access Internet banking, in addition to their passwords.

``We do report [infringements], the transparency is between us and the regulators," he said.

Brooks said HSBC has been taking steps in educating its customers, though information distribution on the Internet could be burdensome. ``Having been involved in this for a long time, the amount of information we give to customers can be quite overwhelming, so we need to find that balance," he said. ``The way we are trying to communicate with customers is by saying these are the [issues] you need to pay attention to."

With reports that Russia-based hackers have moved to a new technology called ``malicious software," or ``malware," which tracks keystrokes whenever banking customers visit online banks,

Brooks says the best offense is a good defense and advises that users keep an updated computer with plenty of anti-virus software on it and run legitimate software.

CONCLUSION:

E Banking is becoming immensely popular globally, and India is no exception to it. The declining Internet rates, falling PC prices, broad bandwidth access through cable and digital subscriber lines, accessing the NET through cable TV etc., would definitely encourage the boom in E Banking in India.

With the globalization of business and services, our country cannot lag behind in niche areas of Electronic Banking. In the new global era of multi currency, multi-legal and multi regulatory systems, with the freedom of E-Commerce, banks have to operate like multinational corporations to grow and survive by adopting E banking.