IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 1, January 2015.
www.ijiset.com
ISSN 2348 – 7968

Threat Perception of the customer and the role of RBI in Online Banking

Mr. Susil Kumar Sarangi
Assistant Professor in Department Of MBA, Kalam Institute of Technology
GovindaVihar, Berhampur-10

Abstract

There has been an inexorable growth in online banking around the world, with penetration rates reaching over 80% of adults in some countries using online banking regularly. India is at an earlier stage of development in mobile banking, but given the ubiquity of mobile phones, and the fact that most banks will have a full suite of mobile banking services within the next few years. Rapid growth here is also inevitable. Banks in developed countries have largely been successful at moving transactions away from branches to other channels. The dynamics are slightly different in developing countries where in some cases more branches are needed, but the longer term trend will be the same. With fewer customers visiting branches, banks have to come up with better ways of marketing through digital channels. Digital marketing is more of a challenge for established banks operating in a more regulated environment. With the advent of e-banking, India is facing unprecedented competition from the World at large. If technology is not updated in financial sector, international trade would be a distant dream. The deregulation of the banking industry coupled with the emergence of new technologies has enabled new competitors to enter the financial services market quickly and efficiently. The need of the hour is to meet the global challenge of providing different services to customers and also keeping vigil eye, to curtail the risk arising due to e-banking.

Key Words: Digital Marketing, Mobile banking, Regulated Environment. Risk arising due to e-banking.

INTRODUCTION

Internet banking is an electronic payment system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution, such as a retail bank, virtual bank, credit union or building society. Online banking is also referred as, Online banking,e-banking, virtual banking and by other terms. Services of Internet-banking includes

1. Information System

2. Electronic Information Transfer System

3. Fully Electronic Transactional System

E-banking services can be availed for payment of bill, fund transfer, credit card, railway and air ticket booking, investment, recharging phones and mobiles and shopping. Generally banks do not charge customers for providing certain services.

ISSN 2348 – 7968

OBJECTIVES OF THE STUDY:

- To study the Internet utilities and its effectiveness to the Banking organization in general.
- To study the customer perception and attitude towards Internet safety.
- To study the role RBI in the changing scenario of internet Banking.
- To study the quantitative as well as qualitative security in internet Banking.

IMPORTANCE OF THE STUDY:

Theoretical and practical study cannot be separated in any course of action. One can have a complete knowledge in any course when he/she is acquired with both theory and practice. The main objective of the study is to observe the actual practice that are prevalent in the organization evaluate how far these practice confirm to the accepted and established scientific standard and norms. This study will highlight the importance of security practices in the pace of organizational effectiveness.

METHODOLOGY:

Research methodology in research has thus stay as an integral part of research. Today it is accepted that identification as well as solution of all research activity lies in intensive and proper use of research methods. Research methodology includes data sources, sample size and methods of data presentation.

SOURCES OF DATA:

Data are collected from both primary as well as secondary sources. Primary data will be collected from the customers of the bank through a structured questionnaire. Data regarding organization history, history of internet Banking activities are collected from secondary sources like Annual reports, Journals, Periodicals published by the organization and websites.

SAMPLE

Sufficient care has been taken to select the sample of respondents. For this purposes random sampling has been used to select the respondents. There are 50 respondents interviewed to fulfill the objectives of the study.

DATA PRESENTATION:

Data presented through tables and different chart. The score obtained from Questionnaires is summed up by percentile technique analysis is carried out. On the basis of information gathered from the secondary documents the Questionnaire is developed.

INTERNET-BANKING

Internet Banking is a product of e-commerce in the field of banking and financial services. In what can be described as B2C domain for banking industry, Internet Banking offers different online services like balance enquiry, requests for cheque books, recording stop-payment instructions, balance transfer instructions, account opening and other forms of traditional banking services. Mostly, these are traditional services offered through Internet as a new delivery channel. Banks are also offering payment services on behalf of their customers who shop in different e-shops, e-malls etc. Further, different banks have different levels of such services offered, starting from level-1 where only information is disseminated through Internet to level-3

ISSN 2348 – 7968

where online transactions are put through. Considering the volume of business e-commerce, particularly in B2B domain, has been generating, it is natural that banking would position itself in an intermediary role in settling the transactions and offering other trade related services. This is true both in respect of B2C and B2B domains.

In B2B scenario, a new form of e-commerce market place is emerging where various players in the production and distribution chain are positioning themselves and are achieving a kind of integration in business information flow and processing (STP or near STP) leading to efficiencies in the entire supply chain and across industries. Banks are positioning themselves in such a market in order to be a part of the financial settlements arising out of transactions of this market and providing wholesale financial services. This needs integration of business information flow not only across the players in the supply chain, but with the banks as well. Such institutions have the advantage of long standing relationships, goodwill and brand, which are important sources of assurance in a virtual market. Banks are in fact, converting this goodwill into a business component in e-commerce scenario in providing settlement and other financial services. Some banks have also moved to providing digital certificates for transactions through e-markets.

Banks' strategies in B2B market are responses to different business models emerging in e-commerce. A recent study by Arthur Andersen shows that banks and financial service institutions generally adopt one of three business models to respond to e-business challenges.

1.They treat it as an extension of existing business without any significant changes other than procedural and what technology demands.

2. Takes the same approach as the first but introduces structural changes to the underlying business.

3. Banks launch e-business platform as a different business from the existing core business and as a different brand of product.

There is no definite answer as to which approach is appropriate. Perhaps it depends on the type of market the bank is operating, its existing competencies and the legal and regulatory environment. It is, however, sure that e-banking is evolving beyond the traditional limits of banking and many new products / services are likely to emerge as e-commerce matures.

UTILITIES OF INTERNET BANKING

Electronic Payments: The initiatives taken by RBI in the mid-eighties and early-nineties focused on technology-based solutions for the improvement of the payment and settlement system infrastructure, coupled with the introduction of new payment products by taking advantage of the technological advancements in banks. The continued increase in the volume of cheques added pressure on the existing set-up, thus necessitating a cost-effective alternative system.

ECS Suite of products: ECS is an electronic mode of funds transfer from one bank account to another. It can be used by institutions for making payments such as distribution of dividend

ISSN 2348 – 7968

interest, salary, and pension, among others. It can also be used to pay bills and other charges such as telephone, electricity, water or for making equated monthly installments payments on loans as well as SIP investments. ECS can be used for both credit and debit purposes.

ECS (RECS) (Debit and Credit): To take care of pan-state / group of states payments from a location within the state itself and leveraging on CBS available in the banks, RECS was launched during the year 2009. Presently RECS is available in 12 RBI centres (Ahmadabad, Bangalore, Bhubaneswar, Chandigarh, Chennai, Guwahati, Hyderabad, Jaipur, Kolkata, Nagpur, New Delhi and Thiruvananthapuram.

National Electronic Clearing Service (NECS) Credit: To further leverage on technological development in the banking and leveraging on CBS in banks, RBI launched NECS in October 2008. The scheme is operated from National Clearing Cell (NCC), Mumbai. NECS (Credit) facilitates multiple credits to beneficiary accounts with destination branches across the country against a single debit of the account of the sponsor bank. This arrangement obviates multiple setups across country for facilitating ECS payments and saves a lot of resources for all the stakeholders. As of now, 76,310 bank branches spread across country are covered under the scheme and the same are growing every month.

Real Time Gross Settlement(RTGS)is the continuous (real-time) settlement of funds transfers individually on an order by order basis (without netting)Here the words 'Real Time' refers to the process of instructions that are executed at the time they are received, rather than at some later time. On the other hand "Gross Settlement" means the settlement of funds transfer instructions occurs individually (on an instruction by instruction basis). The settlement of funds actually takes place in the books of RBI and thus the payments are considered as final and irrevocable.

National Electronic Funds Transfer (NEFT) System: This retail electronic funds transfer system introduced in the late 1990s enabled an account holder of a bank to electronically transfer funds to another bank account holder with any other participating bank. EFT was available across 15 major centers in the country has been replaced by state of art, feature rich and more efficient system. NEFT launched in November 2005, is a more secure system introduced by Reserve Bank of India for facilitating one-to-one funds transfer requirements of individuals / corporate. NEFT is now the main electronic system for retail electronic payments operating in a near-real-time mode. Under NEFT, individuals, firms and corporate can electronically transfer funds from any branch to any individual, firm or corporate having an account with any other bank branch in the country. NEFT system provides for batch settlements at hourly intervals, thus enabling near real-time transfer of funds. Certain other unique features viz. accepting cash for originating transactions, initiating transfer requests without any minimum or maximum amount limitations, facilitating one-way transfers to Nepal, receiving confirmation of the date / time of credit to the account of the beneficiaries, etc., are available in the system.

Collaterised Borrowing and Lending Obligation (CBLO): CBLO is another money market instrument operated by the Clearing Corporation of India Ltd. (CCIL), for the benefit of the entities that have either no access to the interbank call money market or have restricted access in terms of ceiling on call borrowing and lending transactions.

ISSN 2348 – 7968

POS (points of Sales) terminals: this facility is used for enabling online payments for goods and services. There are around 10 lakh POS (points of Sales) terminals in the country, which enable customers to make payments for purchases of goods and services by means of credit/debit cards. The online payment are enabled through own payment gateways or third party service providers called intermediaries. In payment transactions involving intermediaries, these intermediaries act as the initial recipient of payments and distribute the payment to merchants. In this regard safeguard the interests of customers and to ensure that the payments made by them using Electronic/Online Payment modes are duly accounted for by intermediaries receiving such payments, directions were issued in November 2009. Directions require that the funds received from customers for such transactions need to be maintained in an internal account of a bank and the intermediary should not have access to the same.

Immediate Payment Service (IMPS): It is a payment service introduced by National Payments Corporation of India (NPCI). The service, launched as an instant mobile remittance solution in November, 2010 has today evolved as a multi-channel, multi-dimensional remittance platform. The IMPS platform today is capable of processing P2P (Person to Person), P2A (Person to Account) and P2M (Person to Merchant) remittance and transactions can be initiated from Mobile, Internet as well as ATM channel. In addition to banking customers, non-banking customers can also avail the IMPS facility through PPIs issued by non-bank issuer authorized by Reserve Bank of India. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones. IMPS facilitate customers to use mobile instruments as a channel for accessing their bank accounts and put high interbank fund transfers in a secured manner with immediate confirmation features. This facility is provided by NPCI through its existing NFS switch.

As can be seen from Table 2.1, it is observed that the use of debit cards is growing increasing over the period of last 3 years both in terms of number of transactions and value also. In the year 2012-13, number of transactions through credit cards and debit cards were 396.6 million and 469.1 million respectively.

ISSN 2348 – 7968

Table 2.1: Payment System - Annual Turnover

Item	Volume (million)			Value (₹ billion)		
	2010-11	2011-12	2012-13	2010-11	2011-12	2012-13
1	2	3	4	5	6	7
Systemically Important Payment Systems (SIPS) through RTGS	**49.3**	**55.0**	**68.5**	**484872.3**	**539307.5**	**676841.0**
Total Financial Markets Clearing (1+2+3)	**1.7**	**1.9**	**2.26**	**383901.3**	**406071.2**	**501598.5**
1. CBLO	0.15	0.14	0.16	122597.4	111554.3	120480.4
2. Government Securities Clearing	0.36	0.44	0.70	69702.4	72520.8	119948.0
3. Forex Clearing.	1.20	1.30	1.40	191601.5	221996.1	261170.1
Others (4+5+6)	**1387.4**	**1341.9**	**1313.7**	**101341.3**	**99012.1**	**100181.8**
4. CTS	160.4	180.0	275.1	14391.2	15103.7	21779.5
5. MICR Clearing	994.6	934.9	823.3	68621.0	65093.2	57504.0
6. Non-MICR Clearing	232.3	227.0	215.3	18329.1	18815.1	20898.3
Total Retail Electronic Clearing (7+8+9)	**406.3**	**512.3**	**692.8**	**11944.9**	**20574.9**	**31876.8**
7. ECS DR	156.7	164.7	176.5	736.5	833.6	1083.1
8. ECS CR	117.3	121.5	122.2	1816.9	1837.8	1771.3
9. EFT/NEFT	132.3	226.1	394.1	9391.5	17903.5	29022.4
Total Cards (10+11)	**502.2**	**647.5**	**865.7**	**1142.1**	**1500.4**	**1972.9**
10.Credit Cards	265.1	320.0	396.6	755.2	966.1	1229.5
11.Debit Cards	237.1	327.5	469.1	386.9	534.3	743.4
Total Others (4 to 11)	**2295.9**	**2501.7**	**2872.2**	**114428.2**	**121087.4**	**134031.4**
Grand Total (1 to 11)	**2346.9**	**2558.6**	**2942.9**	**983201.8**	**1066466.1**	**1312470.9**

(Source: RBI Annual Report 2012-2013)

Share of electronic based payment transactions has been increasing both in volume and values terms. Whereas share of Paper based payments transactions are gradually decreasing both in terms of volume and value of transactions.

An overview on volume of transactions and their values in various payments system during the years is illustrated as shown below:

RTGS transactions have shown growth of 11.2 percent in transaction value for the period 2011-2012 as compared with the period 2010-2011. Further the transaction value has increased by 25.5 percent for the period 2012-13 as compared with the previous period 2011-2012. From both the charts, it may be concluded that share of RTGS transactions (in value terms) have increased from 51 percent in 2011-12 to 52 percent in 2012-13. Share of paper based payment system has declined significantly.

Table 2.2: PKI Vs Non-PKI Payment System - Annual Turnover

Sr. No.	Item	2012-13 Volume (million)	2012-13 Value (Rs. Billion)
	PKI enabled Payment Systems		
1	SIPS through RTGS	68.5	6,76,841.0
2	CBLO	0.2	1,20,480.4
3	Government Securities Clearing	0.7	1,19,948.0
4	FOREX	1.4	2,61,170.1
5	CTS	275.1	21,779.5
6	NEFT	394.1	29,022.4
	Sub Total (1+2+3+4+5+6)	740.0	12,29,241.4

ISSN 2348 – 7968

	Non-PKI		
7	MICR clearing	823.3	57,504.0
8	Non-MICR clearing	215.3	20,898.3
9	ECS DR	176.5	1,083.1
10	ECS CR	122.2	1,771.3
11	Credit Cards	396.6	1,229.5
12	Debit Cards	469.1	743.4
	Sub Total (7+8+9+10+11+12)	2,203.0	83,229.6
	Grand Total	2,943.0	13,12,471.0

(Source : RBI Annual Report 2012-2013)

INTERNET USERS RESPONSE

To gauge the real time response from the customers, the researcher made a survey of 60 online banking users to find out their perception regarding threats in their mind. The respondents are customers of Union Bank of India. The attempt is made by summarizing the results of response.

Internet Users Response:

Internet Users Response	Number of respondents				
Statements	Almost True	Mostly True	Sometimes True	Rarely True	Nat at all time
1. Internet Banking in my Bank is excellent	25	15	06	02	02
2. Disputes are settled amicably by coordination, mutual interest and understanding.	18	17	11	03	01
3. Employees are well trained to develop excellent customer service.	20	17	12	01	00
4. Mutual understanding between Internet users view and employees view.	15	13	09	08	05

ISSN 2348 – 7968

5. Employees work is a team to fulfill organisation's objectives	22	19	07	01	01
6. Working condition of the Internet Banking is good for Safety and Security	21	13	10	04	02
7. The security measures provided by the Govt .to protect internet Banking users interest is excellent	19	16	09	05	01

Statement 1- Around 67% of the respondents felt that the services of internet banking are excellent.

Statement 2- Around 58% of the respondents felt that the disputes whatever is arising during the transaction are amicably settled by coordination, mutual interest and understanding.

Statement 3- 62% of the respondents felt the employees are well trained to develop excellent customer service.

Statement 4- Mutual understanding between Internet users view and employees view is ensured felt only 47% of the respondents. This shows majority of the issue resolutions are not based on mutual understanding.

Statement 5- Teamwork of Employees is to fulfill organisation's objectives is consented by 52% of the respondents.

Statement 6- The working place which is very important for safety and security of the customer is ensured properly by 57% of the respondents.

Statement 7-The security measures provided by the Govt .to protects internet Banking users' interest is excellent is felt by 58% of the respondents.

ISSN 2348 – 7968

ISSUES ON INTERNET BANKING

Some of the issues as comes out in the primary survey are discussed in this passage. It is to be noted from the study that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

THREATS IN INTERNET BANKING:

Some of the common threats seen in the internet banking are listed below.

Eavesdropping: When an attacker is eavesdropping on the 'clear text' communications, it is referred to as to 'listen in' or interpret (read), sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, the data can be read by others as it traverses the network.

Data Modification: After an attacker has read payment data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if the customers do not require confidentiality for all communications, the customers do not want any of the messages to be modified in transit. For example, if the customers are exchanging purchase requisitions, they do not want the items, amounts, or billing information to be modified.

Identity Spoofing (IP Address Spoofing): Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete customer’s data. The attacker can also conduct other types of attacks, as described in the following sections.

Password-Based Attacks: A common denominator of most operating system and network security plans is password-based access control. This means customers’ access rights to a computer and network resources are determined by who he/she is, that is, his/her user name and his/her password. Older applications do not always protect identity information as it is passed

ISSN 2348 – 7968

through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time. After gaining access to the payment network with a valid account, an attacker can do any of the following:

1. Obtain lists of valid user and computer names and network information.
2. Modify server and network configurations, including access controls and routing tables.
3. Modify, reroute, or delete customers' data.

Denial-of-Service Attack: Unlike a password-based attack, the denial-of-service attack prevents normal use of the computer or network by valid users. After gaining access to payment network, the attacker can do any of the following:

1. Randomize the attention of internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
2. Send invalid data to applications or network services, which causes abnormal termination or behaviour of the applications or services.
3. Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
4. Block traffic, which results in a loss of access to network resources by authorized users.

Man-in-the-Middle Attack: As the name indicates, a man-in-the-middle attack occurs when someone between the customer and the person with whom the customer is communicating is actively monitoring, capturing, and controlling the communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-the-middle attacks are like someone assuming identity in order to read customer's message. The person on the other end might believe it is payer (Sending Customer) because the attacker might be actively replying as he/she likes to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

Compromised-Key Attack: A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

ISSN 2348 – 7968

Sniffer Attack: A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key. Using a sniffer, an attacker can do any of the following:

1. Analyze network and gain information to eventually cause the network to crash or to become corrupted.
2. Read the communications.

Application-Layer Attack: An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of the application, system, or network, and can do any of the following:

1. Read, add, delete, or modify the data or operating system.
2. Introduce a virus program that uses computers and software applications to copy viruses throughout the network.
3. Introduce a sniffer program to analyze the network and gain information that can eventually be used to crash or to corrupt the systems and network.
4. Abnormally terminate data applications or operating systems.
5. Disable other security controls to enable future attacks.

PRINCIPLES OF INFORMATION SECURITY:

The core principles of Information Security are:

Confidentiality: Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Confidentiality is necessary for maintaining the privacy of the people whose personal information is held in the system.

Integrity: In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID (Atomicity, Consistency, Isolation, Durability) model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to

ISSN 2348 – 7968

access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Authenticity: In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as 'digital signatures', which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

Non-repudiation: In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

LEGAL PROVISIONS ON E-BANKING IN INDIA

India is a signatory of WTO. The basic principles of WTO are Liberalization, Globalization and Privatization. Therefore, trade and commerce in India has been liberalized. Incidentally, the financial sector has also undergone major changes. With the advent of e-banking, India is facing unprecedented competition from the World at large. If technology is not updated in financial sector, international trade would be a distant dream. The deregulation of the banking industry coupled with the emergence of new technologies has enabled new competitors to enter the financial services market quickly and efficiently. Various provisions of law, which are applicable to traditional banking activity, are also applicable to internet banking.

RBI REGULATION: OBLIGATION OF BANKS AND THE ONLINE BANKING

There are certain obligations which the banker is supposed tofulfill. They are

1. Banks have to maintain secrecy of customers account. This obligation dates back to 1924 where in a casepopularly known as *Tournier*in which it was heldthat banker should not disclose customers financialposition and the nature and the details of his account toanybody, since it may affect his reputation, creditworthiness and business. Now with the advent of newtechnology, this obligation has become a difficult task forthere are hackers who can operate others account. Banks come to knowonly when the customer informs them of some irregularityin their transaction. Hence, to meet out this obligation,banks have to update their technology to the requirement.

2. Banks are also under obligation (public duty), toproduce documents to the court whenever called for. InformationTechnology Act, 2000 was drafted to facilitate users ofelectronic communication similar to other paper based ororal testimony means. Records can be kept in electronicform. Electronic form means information generated, sent,received or stored in media, magnetic, optical, computermemory, micro film, etc. Now in the eyes of law writtenrecords means electronic records which can be producedbefore the court like it was produced previously. But banks have to reproduce the documents and store themproperly. If the software is attacked

ISSN 2348 – 7968

with virus it washes ofall the documents. Hence, banks have to carefully handlethe electronic documents or else they will be accountable tothe law.

3. Obligation to verity forgery of signatures. Banks haveto verify the signature of the customer before paying theircheques. This obligation is on the paying banker. The lawis very strict; and in case of forgery the banker is liable.These signatures are in electronicform attached to electronic record. The obligation of thebanker to verify the signature is continuing here for digitalsignature. Hence, the banker should adopt technologywhich can identify the sender by recognizing messageoriginator, authentication and non reputable that affixes acoded message to the document. It is used to sign therecord. Banker has to maintain records of the digitalsignature and also educate the customer in this regard.

4. The other obligation on the banker is to provide properservice to the customer. Otherwise the bank isanswerable. Not providing proper service attractsConsumer Law which amounts to deficiency in providingservice. It has been held in *Vimal Chandra Grover v. Bankof India*, that banking is a business transaction of a bank and customers of a bank are consumers within the meaningof Section 2(1) (d) (ii) of the Act. This obligation extendsto electronic banking also.RBI circular to control risk due to internet bankingThe Reserve Bank of India has issued New Circular to InternetBanking. The Reserve Bank of India as a supervisor will coverthe entire risks associated with electronic banking as a part ofits regular duty. It is the statutory duty on every bank that theyshould develop a clear Customer Acceptance Policy layingdown explicit criteria for acceptance of customers. TheCustomer Acceptance Policy must ensure that explicitguidelines are in place on the following aspects of customerrelationship in the bank.

5. No account should be opened in anonymous orfictitious/benami name. Banks should not allow theopening of or keep any anonymous account or accounts infictitious name or account on behalf of other persons whoseidentity has not been disclosed or cannot be verified. Parameters of risk perception are clearly defined in termsof the nature of business activity, location of customer andhis clients, mode of payments, volume of turnover, socialand financial status etc., to enable categorization ofcustomers into low, medium and high risk Customersrequiring very high level of monitoring, may, if considerednecessary, be categorized even higher.

Banks should pay special attention to any moneylaundering threats that may arise from new or developingtechnologies including internet banking that might favor anonymity, and take measures, if needed, to prevent theiruse in money laundering schemes. Banks are required to ensurefull compliance with all KYC/AML/CFT guidelines issuedfrom time to time, in respect of add-on/ supplementarycardholders also. Further, marketing of credit cards isgenerally done through the services of agents. Banksshould ensure that appropriate KYC procedures are dulyapplied before issuing the cards to the customers. It is alsodesirable that agents are also subjected to KYC measures.

Wire transfer is an instantaneous and most preferred routefor transfer of funds across the Globe. Hence, there is aneed for preventing terrorists and other criminals fromhaving unfettered access to wire transfers for moving theirfunds and further for detecting their misuse. Theinformation can be used by Financial Intelligence Unit -India (FIU-IND) for analyzing suspicious or unusualactivity and disseminating it. The originator informationcan also be put to use by the beneficiary bank to facilitateto identify suspicious transactions for filing SuspiciousTransaction

ISSN 2348 – 7968

Reports (STRs) to Financial Intelligence Unit-India (FIU-IND) Banks should put in place a system ofperiodical review of risk categorization of accounts and theneed for applying enhanced due diligence measures. Suchreview of risk categorization of customers should becarried out at a periodicity of not less than once in sixmonths.

The originator informationcan also be put to use by the beneficiary bank to facilitate

1. .Attract new customers.
2. Provide services offered by competitors.
3. Reduce customer attrition.

A multi-layered security architecture comprising firewalls,filtering routers, encryption and digital certification ensuresthat customers account information is protected fromunauthorized access. Apart from this, the Reserve bank of India has issued circular for the convenience of working withelectronic banking as there is a steep rise in the risk involveddue to internet banking. The need of the hour is to meet theglobal challenge of providing different services to customersand also keeping vigil eye, to curtail the risk arising due to e-banking.

SUGGESTIONS:

In the light of above discussion over the matter, theresearcher warrants to make certain suggestions to convert the hugelyun-tapped the internet users to make them online banking users.

1. Banks are under obligation to maintain secrecy of customers account. The new RBI new circular has givenguidelines to minimize risk of hacking. However, it is the dutyon the banker to adopt technology to discharge his duty in amore effective manner. Reserve Bank of India should alsoensure that the banks are using new technology. The RBIshould appoint technicians and ask them to report the sameunder security policy.

2. The auditor appointed to inform as the misappropriationof funds even at the minutest level. Electronic banking hasenhanced the risk of misappropriation of funds by the bankersas it goes undetected.

3. The Automatic Teller Machine is widely used today. It isobserved that these machines fail frequently and causesinconvenience to the customer. RBI in its next circular has tomention the number of times banks are not penalized for suchfailures. After a particular limit the banks should pay penaltywhich alerts them to keep check on the working of themachine.

4. Speedier and cheaper justice is the hallmark of theConsumer Protection Act. And as discussed above the Act isapplication to banking service also. The scope of the Actshould be extended specifically to electronic banking also incases of frequent failure of ATM machines, non compliance ofsecurity which results in hacking, and exuberant charges leviedby bank for fund transfer, etc. Though this are covered underRBI circular, they should be brought within the purview of thelegislation, which will be convenient to customers, Under Section 35 of RBI Act.

References:

ISSN 2348 – 7968

1. “India - internet market and forecasts,” BuddeComm, July 2010, p.3; “India - broadband market, internet serviceand forecasts,” BuddeComm, July 2011, p.2;

2. “The Indian telecom services performance indicators - July – September2011,” TRAI, 9 January 2012, p.5; “India goes digital - a bird’s eye view of the Indian digital consumer industry,”

3. Delivery to be the prominent payment mode for domestic e-com,”

4.VCCircle website, www.vccircle.com/500/news/cashon-delivery-to-be-the-prominent-payment-mode-for-domestic-e-com, accessed 21 February 2012. “Report on Internetin India.

5. RBI Annual Report 2012-2013

6.Caruana, Jaime (2012), ‘Shareholder Value and Stability in Banking; is there a Conflict?’

7. Danielsson, Jon, ‘Blame the Model’, Journal of Financial Stability 4 (2008)

8. Derman, Emanuel (2011), ‘Models Behaving Badly’, Free Press

9. Diebold, Francis X, Doherty, Neil A, Herring, Richard J (2010), ‘The Known, the Unknown and the Unknowable in Financial Risk Management’, Princeton University Press

10. Dowd, Kevin and Hutchinson, Martin, ‘Alchemists of Loss’’, Times Group Books

11. Group of Thirty, ‘Toward Effective Governance of Financial Institution’

12. Haldane, Andrew G (2012), ‘Tails of the Unexpected’

13. Institute of International Finance (2009), ‘Risk Models and Statistical Measures of Risk’

14. Ecommerce@its.best.uk1999