Changing Dimension of E-Banking Froude: Indian Perspective

***Dr. Rekha**

Introduction

Technological development has transformed the manual transactions of banking into electronic form of banking transaction. The reforms in banking sector were introduced in earlier 1990s. Till 1980 banks were offering their customers to do banking transactions through only one channel that is by visiting the bank and after the reforms now the banks are offering to their customers multiple channels for doing the banking transactions and that to faster than the manual banking process. Technology development has brought the vast change in the banking sector. E- Banking offers banking services through electronic media. Private sector banks at initial stage were not fully computerized whereas new private sector banks and foreign banks were fully computerized from their establishment itself. Reforms in the banking sector have brought with it many new challenges. Private Sector banks e. g ICICI bank, HDFC etc were the first to offer internet banking services in India, after that the foreign banks and public sector banks have started providing e-banking services to their customers. Public sector banks has widened their network and have reached to every corner of the country this was possible only due to e-banking service system implement by Banks with the technology development. ICICI bank initial provide limited services like having access to bank account etc and later on slowly and gradually it started providing various other electronic banking services to its customers. After ICIC bank other banks such as Citibank, Induced, HDFC bank and various other private, public and foreign sector banks started providing electronic banking services to their customers. State Bank of India was first to start amongst public sector banks electronic banking services. The drawback of technology development in banking sector is if the security standards are not maintained by banks than the whole bank is on a click to the hacker which ultimately increases the chances of risk involved of commission of e-banking frauds. Electronic banking means bank's services are delivered to customer at their work place or home or where ever they are with the help of electronic technology. Internet has made it possible to provide banking services at the door step of the customer. The public sector banks have implemented the e-banking system little later. Private sector banks have covered their 70% of the business through e-banking system. The first steep of banks towards e-banking was by issuing the plastic cards then came up the telebanking and there after the full fledge online banking services are offered by majority of the banks. The technology advancement has brought the drastic change in the banking sector. The e-

banking system has made the fraudsters or hackers to have full information and data by the click of button and having access to banks network in the absents of good security standards which is of great risk of having increase in number of financial losses and frauds. Fraudsters have got an easy way to commit the crime in banking sector through an instrument called as computer. Electronic banking has tried to achieve the objective of the world trade organization by liberalization. And through e-banking trading has also become faster and easier which has led to globalization of the India market. It is because of E-banking there is a great development in the sector of e-commerce. With the development and revolution in banking sector and establishment of e- banking system many challenges and issues are faced. Information Technology has changed the manual banking sector into electronic banking sector. The e-banking has reduced the laborious paper works and which in turn has reduced the time for transacting banking transaction. There are various channels through which e-banking transactions can be done. Automatic Teller Machine, Debit Cards, Credit Cards, Internet banking and Mobile banking are the few channels for e- banking. E-banking means and includes internet banking, telephone banking, mobile banking etc. Through online banking customers can manage their banking transactions with the help of various kinds of browsers. Reserve Bank of India has played a vital role in implementing the electronic banking system. RBI had formed various committees in order to work in the area of implementing electronic banking system.

Benefits to the Banks:

Banks have reached customers from remote places which have helped them in increase of their business and because of e-banking, banks are able to sale and advertise their various other products relating insurance, loan, investment and etc to the customers. More and more people have started using e-banking services as there are lots of advantages. More than half of the population is today using e-banking services. Banks are successfully doing their business due to providing e-banking facilities to their customers that covers more than 70% of their business. Benefits to the merchants and traders: E-banking provides the credit card services to customer. Credit card holders can do shopping without having cash immediately in hand, they can buy first with help of credit card and later on can make the payment of the same, and hence indirectly this has increased the business to the traders and merchants. It is due to e-banking services traders and merchants have entered the global market and are able to do business in the global market smoothly.

Benefits to the Government and Nation:

The objective of liberalization and globalization in the trade is achieved because of ebanking services to some extent. E-banking will help in over all development of the nation smoothly. E-banking will also help in increasing the investments in India by the people from outside India as the e-banking system facilitates the easy transfer of funds and also in exchange of foreign currency. Inspite of having so many advantages and benefits to customers, banks, merchants, traders, government and nation there is no much development because with these benefits there are lot of challenges and issues faced in e-banking system so the people all over have not stared using the e-banking services fully and on the contrary they are scared and reluctant to use the e-banking services in order to the

banking transactions and they still follow the manual way of transacting banking transactions, they feel that there is security threat, there are legal, operational and other issues. So the development has not taken place yet in the developing countries like India. E-banking means doing banking transactions through various electronic media. Then came up the system of mobile banking where through mobile customers can check their balance and also do the banking transactions over mobile. The mobile banking services were available not only for the customers holding bank account but also for the customers who are holding credit cards. Now- a- days with advanced technology in banking sector, most of the banks have stared providing electronic banking services, as the technology helps the banks to have easily accessible to huge number of customers and at a low cost. Moreover through electronic banking the banking transactions can be done much faster than the olden method of doing banking transactions.

Internet banking:

Through internet banking banks are providing the opportunity to their customers to do the banking transactions over the internet. Customers need to have the internet connection in order to use this facility provided by their banks. Through internet banking customers can have access to their accounts from any where even by sitting at home. Also through internet banking customers can do other banking transaction. Banks provides to their customer's user ID and password in order to operate their account via internet.

Information:

The banks provide information regarding various services and products offered by them on their website. It is possible that the servers or banks website may be vulnerable to make any changes in the information provided. Hence some control is required to keep a watch on unauthorized changes to data on the banks web site

Communication:

This is one of the types of internet banking that allows the communication between the customer and banks system. It may be related to account inquiry, for loan application or may be for static file updates. There are high chances of data leakage, data alteration or else unauthorized access to account information and hence there is a need to have control in order to prevent such kinds of things to happen because if it is not controlled it will result into huge financial losses to the customers.

Transaction:

Under this type of internet banking customers are allowed to execute their banking transactions as per their requirement. This type of internet banking is more risky as compared to the other two that is information and communication. This type of internet banking needs to have the highest control and watch, so that the internet banking frauds can be prevented. Customers banking transactions are transfer of funds, accessing the account, paying the bills online, shopping online via online purchase and so on. This type of internet banking requires the highest security system.

Legal issues:

There is constant violation of laws, rules and regulations which is not completely controlled by the system and because of that number of electronic banking frauds are on rise each day. Banks are facing customer's legal actions against them for the losses caused to them by the fraudsters. As a result banks have to suffer many a times and pay high compensations to the victims because the true fraudsters are not found as there are loopholes in laws and also the police personnel handling such cases for investigation are not trained well. Many a times there is jurisdiction problems also. India is currently facing legal issues arising from e-banking services provided to the customers by banks, as there are no much legislative provisions in Indian laws for the crimes committed by criminals in the e-banking area. In counties like USA there are enough laws that are specifically related to e-banking system and e–banking related crimes. Existing laws are with ambiguity as there is no certainty as to which legislations will be applicable to the e-banking transactions which are taking place across the border. The legislation relating to jurisdiction of laws is in question in such a case. There is a possibility that the laws in India and across the border relating to e-banking might differ and may be contradictory to each other in such case it becomes difficult to decide which legislations applies.

Operational risk:

Operation risk, are the risks which are faced in the day to day banking transactions. One of it is error risk there are changes to making error while feeding the data in computer for doing the banking transaction and which is very common another is computer frauds, using computer for banking transactions have increased the number of new opportunities to fraudsters for committing frauds.

Automatic Teller Machine (ATM):

Automatic teller Machine is also called as Automatic Banking Machine. Banking transactions can be done from anywhere that is why it is also called as anywhere banking system. Customers can get their bank account details even at the remote places. ATM is a computerized instrument used for telecommunication and provides the various facilities to the customers of banks such as having cash withdrawal facility anytime from anywhere, where there are ATM centers, having access to the accounts, obtaining the balance details, getting the mini bank statement and many more other facilities are provided.

Debit card:

Debit card is used by the bank customers to do payments for the shopping from the person who has made necessary arrangement with the card issuing bank. Most of the card issuers are affiliated to the two most common issuers they are VISA and Master card.

Credit cards

Banks have stared credit card system commonly known as plastic money. Banks are offering credit cards mainly to the customers who are having certain amount of income or have current or savings account with the bank and they are issuing the credit cards to customers free of charge.

Mobile banking:

Mobile banking is a service provided by banks to their customers wherein customers can do the banking transaction through mobile phone via mobile service provider. Through mobile banking customers can only have the information and cannot do the cash transactions. Mobile banking is one step ahead of internet banking. Banks with the help of mobile service providers offers the banking services to their customers.

Tele Banking:

Tele banking is one of the new electronic banking channels. Customers can do lot of transactions through tele banking by just sitting at home or anywhere. Customers can have their bank account information, can transfer funds and also can pay bills through tele banking system.

Telephone:

Customers have started to have communication with the banks over telephone for the various services provided by banks through telephone say for example balance inquiry, transaction status, issue of bank statement and so on. The telephone number of bank is toll free.

E-banking frauds committed by insiders.

E-banking frauds committed through use of wire: Now a day's huge amount of money can be transferred easily by the electronic media and once the transfer is made it is not easy to reverse the entry easily and sometimes even not possible to reverse the entry or transfer made. There is risk that the insiders or bank employees may not know or might not be having proper knowledge and experience of handling the e-banking system concerned with transfer of funds then the employee may make mistake which would lead to huge losses to the customers. Identity Theft: The few employees in banks are dishonest and tend to disclose the personal information's of the customers to a stranger who is actually called as fraudster. This information received by the fraudster is used by him to committee the fraud. This personal information's received by the fraudster about any customer is used by him to get the debit cards and credit cards by using that customers name and other detail information received by him through the bank employee. Frauds committed by outsiders:

Credit Card Frauds:

Credit cards are made of three plastic sheets and are commonly called as plastic money. The middle sheet of the credit card is called as core stock. The details of the cardholder are embossed over the credit card. Credit card frauds take place by various ways such as duplicate credit cards are made, original credit cards are either manipulated or altered, original credit cards are received by the fraudsters on making fraudulent applications in the name and address of the persons and are used by the fraudsters to committee the fraudulent acts. With the technological development and increasing in use of e-banking and mobile banking system the fraud cases committed with the help of credit cards are causing huge financial losses to the victims and this kind of fraud is increasing tremendously.

Skimming of cards details:

The seller copies the buyer's credit card numbers which is later misused. A fraudster uses the machine to copy the magnetic stripe from the card and a hidden camera is placed to capture the number embossed on the face of the card. This kind of machines and hidden cameras are also installed at public Automatic Teller Machine boots sometimes by the fraudsters. A fraudulent card stripe reader would take away the details of the magnetic stripe and the hidden camera will try to capture the user's Personal Identification Number. The fraudulent machine will then be removed and the detail information captured will be used to create or make duplicate cards which can then be misused to withdraw cash from ATM from the victim's bank account.

Phishing:

Forged emails are sent impersonating an online bank, such email takes the user to forged website, which is designed in such manner that it looks as if the user has logged to the original website. This forged website asks the user to give his personal details. This details taken through the forged website is then used to committee other frauds causing financial losses to the victims. Many types of Trojan horse programmes are also used to snoop on internet users when they are online, to capture confidential data which is then send to outside sites. And again such data, information is used to committee the e-banking frauds. Hacker asks the personal details as if for verification through fake emails which are made in such way that it looks like as if the email is the original message. In this way data is received and the same is misused to cause huge financial losses.

Spoofing:

The duplicate website is created by sing the same name, logo and so on which look as if it is the original website and it asks the user to enter the login address and password. The movement the user enters the same the information goes to the hacker and is used to commit the offence or the financial frauds. Phone Phishing: To file a complaint of the customers for the problems relating to their bank accounts hacker asks the customers to give their identification details and password through in voice. After receiving the details it is use to cause huge financial losses to the customers. Viruses: Viruses are used in the data theft. Viruses are inserted into the computer system and data is stolen from the user's computer which is used to commit the frauds. The security issues can be resolved by using data encryption, use of cryptography, firewall, hardware and software controls, data capture and output controls, network security. RBI had established a working group on internet banking to find out the different aspects of internet banking. Reserve Bank of India had accepted the suggestions given by the group to be implemented. As per the guidelines given by RBI it is responsibility of the banks to settle the compensation claims for damages suffered by their customers who are the victims of e-banking frauds as RBI interprets that banking company was negligent in providing safe and secured e-banking services to their customers.

The group emphasized on three main areas they are as follows:

(i) Security issues
(ii) Legal issues S Legal Issues Security Issues Supervisory Issues
(iii) Supervisory issues.

TYPES OF E- BANKING FRAUDS

1. E-mail Spoofing and Phishing:

In the e-mail spoofing one person sends the e-mail to another person in such a manner that it looks as if the e-mail is send by someone else. Spoofing is basically used to get the password detail of the system or computer. It has become most popular so it is very difficult now-a-days to distinguish the two as to whether the e-mail is come from the same person as mentioned as the sender or from any other person. Hackers use this method of sending the e-mail in which initially the original sender's address appears and the later part is altered so the sender's address looks similar to the original sender. In the way web page spoofing is done by the hackers. Hackers create a website similar to the original bank website and the used are misguided as the start part of the web page address would be similar to the original one and the later part is altered and which is fake. Normally people just write few words in search engine and as they see similar website from rage of sites they directly click on that website without verifying the whole url address, this is because the hackers are the successors and they succeed in committing the fraud easily.

Phishing - scams that ask for your account information to steal valuable information like card number, user ID and passwords as it is a form of Internet is "Phishing" that is it is one of the kind of electronic banking frauds through internet. A fake web site as it is like a legitimate web site of the organization such as a bank is created. Email or messages on mobile to the recipient, including the security access code to access the fake web site and then the customers enter their personal details as requested. This page looks if it is genuine but information entered by users inadvertently is send to the fraudster who has the access to the user's personal details.

Identity Theft: Crimes relating to identity theft are on the rise in India. The theft of identity can take place in various forms; your entire identity can be used for fraudulent use of credit cards, debit cards, to get a loan, to open accounts, and to do any other illegal activities. Be suspicious if someone asks for your personal information's. Fraudsters use convincing stories and explain you the reasons in such a way that you tend to give them your personal details. About 57% of the respondents have stated that they have suffered the identity theft. Identity theft means getting another's identity details by way of fraud or cheating. The major chances of identity theft are through the service providers as they have all the details of the person. The identity of another is used by the fraudster to assure the third person that he is so and so person and under the impression that fraudster is so and so person the third party may do the needful as instructed by the fraudster in the name of the another person. In such a case of identity theft the fraudster may misuse the password, digital signature and other things of the victim to commit the e-banking fraud. Here to help protect your financial identity are few simple strategies: Make sure that the letter box placed outside the door is locked so that it is protected from tampering. In case if one will be away from home for a long period of time, one must make arrangements such as ask friends to receive their letters that are coming or mail to be held at their local post office for collection. Tearing or shredding of important documents containing personal as well as financial details such as account statements, bills and receipts etc before throwing

them away is a safe manner of disposal and by doing so it helps in protecting the identity of the person. Regularly keep a check that all expected bills and statements have been received or not. If not found means thief i.e. fraudster has removed it from your mailbox. The same should be immediately followed and necessary steps are to be taken for stopping any further commission of frauds.

Viruses and Trojans:

Viruses and Trojans are the programs which are harmful and are silently uploaded on your computers without your knowledge. Many a times you tend to click on pop up advertisements and they start getting downloaded along with it the virus programs are also downloaded and which will help the fraudsters get all your secret information's and confidential personal details. This program is uploaded to steal your data or cause damage to your information; they may also flood you with variety of advertisements. Viruses once entered into computer it could be harmful as your data can be stolen easily by the fraudsters. Trojans looks like as if original and genuine applications and then they embed in computers to keep a watch on your activities and start gathering the information. Having latest anti viruses' software installed in computers can help in reducing the chances of viruses getting downloaded on you computers or else using firewall.

Spreading Virus or Worms:

Virus attacks are most popular kind of activity relating to causing harm to computer. It is very easy to transfer virus from one device to another. If the person uses the pen drive containing virus on another person laptop or computer without having antivirus installed in the computer or laptop, it will result into that the virus will automatically get spread into computer or laptop in which pen drive is used. Virus is capable of sending your data stored in computer to the third person and also later on deleting the same from your computer. The data received by third person may be misused for committing the offence of e-banking fraud. Therefore it is stated that spreading of virus in one's computer is also called as one of the criminal offence committed and is punishable as cognizable, bailable and compoundable with the permission of court in which the matter is pending.

Trojan Horse: Trojan horse has come from the Greek fable. A giant wooden horse to the Trojans as a peace offering was presented by the Greeks. Trojan horse is one of the useful computer programs where on the hand it is such a program which causes damage to the computer. The initial stage of attack on computer to cause damage is Trojans. Trojans stay hidden when then the downloading and installation of dangerous threat called as boot is being done. Viruses and worms spread by themselves where as Trojan horses are unable of getting spread by themselves. An email message is send as if like in the form of joke through malicious website in order to insert the Trojan horse in the one's computer. A link may be given as if for example stating an offers and discounts advising to click on the link which will automatically install the Trojan horse in computer with the help of internet explorer. Once the Trojan horse gets installed in the computer it starts lurking and carries out its activities without being visible. Activities such as automatically downloading spyware at the same time the victim is doing his other activities on computer. Therefore Trojan horse is not the direct attacker but indirect and silent attacker. It is invisibly doing activities which cause damage to

computer simultaneously when the user is doing his other activities on computer. Same like virus it can send the data stored in computer to third party, third party can have unauthorized access to victim's computer through Trojan horse. And the same data is misused by fraudster to commit the offence of ebanking fraud or other such connected offences.

Spyware and Adware: When you click on the advertisements that pop on the screen of the computer they open in a different browser window. And the free applications, services or programs start getting downloaded from internet and along with this spyware or adware also gets downloaded. Spyware and Adware software program once enters the computer starts collecting your user details and keeps a watch on your internet activities. And these data collected can be misused by the fraudsters for the fraudulent purposes. Therefore it is advisable never to click on the pop up adds or free application download or free programs. Install the latest security software in your computers in order to detect and remove spyware. Spyware is a computer program which covertly monitors one's activities on his computer. Spyware can gather victim's personal information like password, user id, and banks account number or banks other details and so on. Few of the Spyware specifically are for monitoring internet behavior of the victim such kind of spyware can track places visited by victim on the website, emails written, send and received by victim as well as the various conversations on websites. Spyware is also downloaded on installed maliciously by clicking the fake links by the victim, it is same as how Trojan horse is downloaded and installed in computer. One of the ways by pop up advertises also spyware gets downloaded on computer and gets installed. So if the fraudster wants to monitor the net banking activities of the victim he can do so easily with the help of spyware program. Therefore with the help of spyware fraudsters get all the net banking details and other information of the victim which can used by fraudster to commit the crime of e-banking fraud. Card Skimming: Card skimming means to copy and capture magnetic stripe of the card and PIN data on debit and credit card illegally. Skimming of card is done mostly at any bank Automatic Teller Machine center or through machine called EFTPOS. Fraudsters make use to this captured card and PIN details to make a fake or duplicate credit or debit card. Such fake card is then used by the fraudsters to fraudulently withdraw cash and do other transactions.

Automatic Teller Machine (ATM) Skimming:

On original existing Automatic Teller Machine fraudster may attach false PIN pad or a card skimming device called camouflaged on card reader entry with a camera concealed into it so that the PIN entry will be recorded and captured into it. This captured PIN details can be used by fraudsters to make a fake card and misuse use it for fraudulent withdrawals from account and do other transactions. Therefore it is suggested that before inserting your card into ATM machine to check and conform that ATM machine is not having any skimming device attached to it.

EFTPOS Skimming:

This is a kind of machine which is capable of copying and capturing card and PIN details. The fraudsters make use of this machine to get your details when you give your card out of your sight to process the transaction. Phishing over phone and messages on mobile: Phishing attacks were initially

done through emails. Nowadays phishing attacks are done over phones also by playing a trick on the people, giving a call and representing people that they are genuine and trusted entity and inducing the people to voluntarily reveal all their personal or bank account details. Most of the times fraudsters ask for your internet banking sing in details or your mobile security code like password. The fake messages on mobile are also sent by the fraudsters for example stating that you have won a lottery and we require your details so send the amount, people by reading such messages tend to give their details and which is misused by the fraudsters. It is suggested that never to reveal your personal, bank account or security code details to any over phone. If you have a doubt regarding genuineness of the caller, take their name and phone number to call them back later on cross check the number with the organization's number in phone directory.

Hacking:

The fraudsters hack the websites to steal the data and personal details which are then misused by them to commit the frauds. Hacking means having unauthorized access of another's data, personal information stored in computer or computer system or computer programs or networks. A hacker was originally or initially called as a gifted programmer but later on slowly and steadily he has acquired the negative tag. According to the Information technology Act hacking means to do the below mentioned acts with the intention or knowledge to cause damage or loss to another person:

(i) The act of deleting, modifying or destroying the data which is stored.

(ii) Having access to another's computer without authority.

(iii) Cause Injury by affecting or causing damage to computer.

Having access to another network or internet activities without the users knowledge. One of the examples of hacking case is of Amit Viram Tiwari's case. India's Central Bureau of Investigation along with the help of federal Bureau of Investigation on 26th January, 2014 charged Amit Tiwari as hire hacker for hacking various bank accounts of customers and breaching over 1000 different emails. The website through which he was operating was called as www.hirehacker.ne. The charges of hiring the hacking services were around USD$250 to 500. Web jacking: Taking away the control over any website by cracking the password and later on changing it is called as web jacking. By doing so the owner of the website looses the control over the website and all the information loaded on website is also visible to the web hacker. Web hacker can even upload any data on the website which he has jacked. There are two kinds of popular password cracking attacks they are as follows: The first one is called as dictionary attack: Under the dictionary attack the software will try to attack almost all the words contained in the predefined dictionary of words. The second on is by using brute force: Under this attack software attempts to find out the password by trying all the various combinations of letters, number and symbols until and unless the correct password is found out.

Fake Websites: The most commonly now- a -days is the fake websites stating that they will provide assures job to the applicants. They state that the only requirement is the details given below in the link and they request to fill up the same. In this way the fraudster gets most of the information about

the person and the same is misused by the fraudster to commit the ebanking frauds. Same is in the case of fake online chat websites, the fake matrimonial websites and so on. The purpose of creating these websites is to get the data and information about the people which they use of committing the frauds.

Conclusion:

The detail information about the customer includes the name of the customer, permanent address, mailing address, telephone number, mobile number, e-mail address, pan card number, adher card number, birth date and other such details needed along with the photographs. The details given by the customer has to be verified by the banks by taking a copy of pan card, adher card, electricity, birth certificate and so on. The bank should also call for the original documents such as mentioned above from the customers and need to verify the same before opening the account of the customer. The most important is that if the person wants to open an account the bank should ask for the reference which means person has to get any other person who is already the existing the customer of the bank and also knows him personally from the number of years. This will help the bank to find out the reputation of the person to some extent before opening the account.

***Vice Principal**
Hans Law College
Kotputli (Raj.)

References:

1. Chakrabarty. K, 2013, Fraud in the banking sector causes, concerns and cures, National Conference on Financial Fraud organized by ASSOCHAM, New Delhi, Pg No. 3.
2. Chauhan. M, 2015, Problems and constraints in the bank frauds cases: A Study, International Journal of research, Vol. 2, Issue. No 2, Pg. No.472- 487.
3. Chavan. J, 2013, Internet Banking-Benefits And Challenges In An Emerging Economy, International Journal of Research in Business, Management (IJRBM) Vol. 1, Issue No.1, Pg. No.19-26. Chavda. V, 2014,
4. E-Banking System: Opportunities and Challenges – A Study, Research Hub – International Multidisciplinary Research Journal, Vol. 1, Issue No. 5, Pg. No.1-4.
5. Chiezey. U, Onu. A, 2013, Impact of fraud and fraudulent practices on the performance of banks in Nigeria, British Journal of arts and social sciences, Vol. 15, Issue No.1, Pg. No. 12-28. Dash.
6. M, Bhusan. P and Samal. S, 2014, Determinants of Customers adoption of Mobile Banking: An Empirical study by integrating diffusion of Innovation with attitude, Journal of Internet Banking and commerce, Vol. 19, Issue No.3, Pg. No. 1- 21