Tactful Management Research Journal
ISSN: 2319-7943
Impact Factor : 2.1632(UIF)

E-BANKING FRAUDS AND FRAUD RISK MANAGEMENT

Mr. Rupesh. D. Dubey and Dr. Anita Manna

Assistance professor , Dept. of Commerce , K.M. Agrawal College, kalyan .
Principal , HOD. Dept. of Commerce , K.M. Agrawal College, kalyan .

Abstract : Internet Banking Fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. Internet Banking Fraud is a form of identity theft and is usually made possible through techniques such as phishing, lottery fraud scam etc. Now internet banking is widely used to check account details, make purchases, pay bills, transfer funds, print statements etc. Generally, the user identity is the customer identity number and password is provided to secure transactions. But due to some ignorance or silly mistakes customer can easily fall into the trap of internet scams or frauds done by the fraudsters. The ways of E-banking frauds are like phishing, spam, spyware, card skimming, Hacking etc. The paper is focused to study and highlights the types and many ways of Internet banking frauds that take place in our banking systems nowadays, and also to understand and study the ways of Fraud risk management on the part of every individual bank. Fraud

INTRODUCTION

E-banking (or Internet banking)means any entity (banks) that permits the borderless banking facilities anytime, anywhere and anyhow banking. In simple meaning any user with a personal computer and a internet connection (browser) get connected to his bank -s website to perform any of I.T system, the banking services are delivered by way of a Computer-Controlled System. This system does involve direct interface with the customers. The customers do not have to visit the bank's premises. 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. Now a day's mostly all core banking facilities are performed though internet banking , every the virtual banking functions'-banking involves information technology based banking. Under this bank try to give their best core banking services through Electronic modes like mobile banking, Telephone banking, debit card, credits card, smart card, Automated teller machine (ATM), Electronic Funds transfer (EFT) system, Cheque Transaction payment system and mainly through Internet banking. Due to the internet banking, customer rarely visit to branch and he avoids using main branch banking. The traditional branch model of bank is now giving place to an alternative of E-Banking in broaderways.

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.

With the advances in information technology, most banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking, It leads to the creation of minds of frauds through online i.e internet banking frauds Fraudsters have also followed customers into this space. However, the response of most of the banks to frauds in these areas needs further improvement, thereby avoiding putting the entire onus on the customer. There is also a lack of clarity amongst banks on the reporting of these instances as

frauds.

There is need for all banking institute to have wide framework on fraud governance with particular emphasis on tackling electronic channel based frauds. This note endeavors to bring out the challenges and suggests a framework which can be implemented across banks to effectively tackle the electronic fraud menace. The definition of banking frauds is as follows

"A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank".

OBJECTIVE OF STUDY:

- To understand the E-Banking scope
- To highlight the various ways of E-Banking Frauds done by fraudsters.
- To understand and study the ways of E-Banking frauds Risk management.

RESEARCH METHODOLOGY:

This study is based on mostly on Primary data by interviewing the banking personnel who are working in the "Transaction Monitoring Team" and "Fraud and Prevention team" of Banks and Secondary Data are also used from various books, journals and websites.

WAYS OF E-BANKING FRAUDS TAKING PLACE:-

The following are some types of fraud are taking places in the recent time; these frauds mostly are performed by internet. Internet banking frauds or scams victims mostly, those customers who are an innocent customer and poor user of E-banking and they easily believe on banks and their personnel. Mainly internet banking fraud is targeted on dormant account (sleeping Account holder).

Phishing: A person's personal details are obtained by fraudsters posing as bankers, who float a site similar to that of the person's bank. They are asked to provide all personal information about themselves and their account to the bank on the pretext of database up gradation. The number and password are then used to carry out transactions on their behalf without their knowledge.

Phishing involves using a form of spam to fraudulently gain access to people's online banking details. As well as targeting online banking customers, phishing emails may target online auction sites or other online payment facilities. Typically, a phishing email will ask an online banking customer to follow a link in order to update personal bank account details. If the link is followed, the victim downloads a program which captures his or her banking login details and sends them to a third party.

Website cloning is the duplication of a website for criminal use. Often times websites cloning will take the form of known chat room or trade sites so that people will either unknowingly give information to the criminal or make a "fake" purchase, willingly giving money for a product that does not actually exist.

Spam: Spam is an electronic 'junk mail' or unwanted messages sent to your email account or mobile phone. These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details.

Spyware: Spyware such as Trojan Horse is generally considered to be software that is secretly installed on a computer and takes things from it without the permission or knowledge of the user. Spyware may take personal information, business information, bandwidth; or processing capacity and secretly gives it to someone else.

"Trojan Horse" scheme unfolds when malicious software (malware) embeds to a consumer's computer without the consumer being aware of it. Trojans often come in links or as attachments from unknown email senders. After installation the software detects when a person accesses online banking sites and records the username and password to transmit to the offender.

Card skimming: is the illegal copying and capture of magnetic stripe and PIN data on credit and debit cards. Skimming can occur at any bank ATM or via a compromised EFTPOS machine. Captured card and PIN details are encoded onto a counterfeit card and used to make fraudulent account withdrawals and

transactions.

ATM Skimming: Fraudsters can attach false casings and PIN pad overlay devices onto genuine existing ATMs, or they can attach a camouflaged skimming device onto a card reader entry used in tandem with a concealed camera to capture and record PIN entry details.

EFTPOS Skimming: Electronic Fund Transfer at Point of Sale. A foreign device is implanted into an EFTPOS machine that is capable of copying and capturing card and PIN details processed through the machine. A compromised EFTPOS terminal can only be detected by a physical inspection.

Hacking: Hacking includes gaining illegal entry into a PC system. Nowadays, the hacking of IP addresses is very universal as it permits the hackers to imagine a fake online character and carry out illegal dealings exclusive of using his factual individuality.

A identity theft: A large number of identity theft crimes occur over the internet. Criminals can get a hold of your personal information through your computer and then set up fake bank accounts or take put loans in your name.

FRAUD RISK MANGEMENT:

There is need for a proper and consolidated fraud governance standard. The fraud risk management and fraud investigation must be owned by the banks itself. Banks in India shifted to core banking business and have moved transactions to payments through the electronic channels like ATMS, Internet banking etc. Fraudsters have also playing an active role as customer into this electronic world banking. The response of the banks related the fraud needed further improvements to overcome through the E-banking fraud easily. The following are the some ways of fraud risk management.

- ❖ Every banking institute must have and maintain the strong “Transaction Monitoring Team”. The role of transaction monitoring team is to keep view on transaction taking place whether any suspicious transaction is going out or not as per the banking norms. If they found any suspicious transactions then necessary action should be taken against that account holder.
- ❖ Every banking institute must also have and maintain the strong “Fraud and Prevention team”. The role of Fraud and Prevention team is to keep trace out the fraud activity and preventing that from fraud before it actually performed.
- ❖ Banks can have dedicated email IDs for customers to report any fraudulent activity that they may notice. A dedicated team can be created to reply to customer queries and concerns through the above email IDs. Phone banking officers and branch staff should also be trained on response to customers’ queries and concerns on frauds.
- ❖ Banks may contemplate the setting up of a fraud helpline for customers and employees to enable them to report suspected frauds and seek tips on fraud prevention. By doing this, banks can make available one more avenue for early reporting and detection of frauds.
- ❖ Creation of fraud awareness among the customers and staff. Awareness on how to prevent and detect frauds is the basis of fraud management. Banks need to adopt various measures to create awareness amongst staff and customers.
- ❖ All banks have a dedicated team to take care of the security of the physical infrastructure. This team should conduct regular security audits of various offices to check for deviations/ lapses. It is the responsibility of this team to ensure that physical assets and data copied on magnetic/optical media do not go out of the offices of the bank without authorization.
- ❖ Banks can have dedicated email IDs for customers to report any fraudulent activity that they may notice. A dedicated team can be created to reply to customer queries and concerns through the above email IDs. Phone banking officers and branch staff should also be trained on response to customers’ queries and concerns on frauds.
- ❖ Creating and employee awareness and training about the various types of fraud and how to detect the frauds and their prevention ways. It is possible through proper mechanism and training program.
- ❖ A strong KYC(know your customer) process is the backbone of any fraud prevention activity. Know your customer , physical securitize of documents of old customers and as well as of new customer also.
- ❖ All banks must have separate Department to manage frauds, their role is monitoring, investigation, reporting and awareness creation.

CONCLUSION:

As electronic payment volumes grow, and more banking activity extends to the web and mobile devices, the ability to detect and prevent financial crime and reduce fraud risk exposure across the enterprise has become critical. Financial institution faces ever –increasing challenges around fraud. Malware, Trojans, Phishing, vishing, whaling, SMS sishing, hacking- criminals continually dream up new fraud schemes with the intention of staying one step ahead of those trying to combat such tactics. The burden on financial institutions is to protect their customers from fraud, protect themselves from losses due to financial crime. Due to the advancement of technology, the fraudsters are also uses technology to have fraud in new and innovative ways. The Banks institute must develop strong fraud risk management and fraud controlling mechanisms for the development of Banking services and customer trust.

REFERENCES:

1.Personal talk to those banking personnel who are working in the“Transaction Monitoring Team” and “Fraud and Prevention team”
2.B.P.Gupta, V.K.Vashistha, H.R.Swami, Banking and Finance, Ramesh Book Depot, Jaipur-New Delhi (2008).
3.http://www.mbaknol.com/business-finance/recent-trends-in-indian-banking-sector
4. http://www.worldjute.com/ebank.html
5.http://www.rbi.org.in/scripts/otherlinks.aspx