CYBER CRIMES AND BANK FRAUDS: NEED TO PROTECT INVESTORS

By Dr. Mariamma.A.K[242]

Invention of 'World Wide Web' has made the world a global village and cyber space has taken almost all the spheres of life ranging from NASA space mission to ordinary railway ticket booking, matrimony, pooja's and temple darshan, e-commerce including banking business and share markets. Core-banking, internet banking, e-payments and ECS, etc made human life so easy for the banking customers as they can make payments and transfer money with the click of a mouse. Availability of debit cards and credit cards reduced the risk of carrying money and ATMs provide any time money. Whereas internet banking business has become nightmare for the customers as it is to swipe and make the accounts dry within seconds from anywhere in the world and Nigerian online frauds are notorious and dangerous. There are several cases where depositors lost their money without their knowledge; hence there is an urgent need to protect the banking customers to help them keep their money safe.

Banking system in India:-The first bank in India was established in 1786. Since nationalisation of 14 banks in 1969, the public sector banks or nationalised banks, owned by Government have acquired a place of predominance and there has been tremendous progress. The need to become highly customer focused has forced the slow-moving public sector banks to adopt a fast track approach. Indian banks are now quoting all higher valuation as compared to banks in other Asian countries, viz. Hongkong, Singapore and the Philippines. An accountholder had to wait hours to get a draft or for withdrawal of money, but today things changed completely, thanks to the Internet.

Modern Banking: In the era of globalisation, banking sector also witnessed drastic changes both at the structural and organisational levels. Banking plays an important role in deciding the best business practises in developing new markets and clients with net based technologies. Faster technological developments have transformed human life into virtual mode, a reality that allows people to make purchases and payments online, without risking themselves to errors. The advent

[242] Faculty, Govt. Law College, Calicut

of the internet has revolutionalised the financial services with new business models to offer 24x7 online accessibility that has created a new business class of online bankers, online brokers and wealth managers. The mobile banking and Internet banking drive away the traditional customers from the conventional branch-based banking by offering them low-cost delivery and by core banking systems[243].

Hi-Tech Banking:-The Rangarajan Committee report in the early 1980s was the first step towards computerisation of banks in India. Indian banking is one of the largest in the world and is the second largest spender on IT. Private banks entered into banking business with huge IT budgets at their disposal to provide a whole new range of financial products and services at minimal costs and technology made this possible. The new generation banks showed the way and others had no option but to follow the tech infusion to retain and attract customers, hence banks are adopting core banking solutions for retaining customers and lowering costs to them[244].

Digital payments also termed as electronic cash, electronic currency, digital money, digital cash or digital currency, transfers money which is exchanged only electronically with the help of computer networks, the Internet and digital stored value systems. Technically electronic or digital money is a representation or a system of debit and credits used to exchange value within another system or itself as a standalone system, online or offline. Various companies now sell VISA, MasterCard or Maestro debit cards which can be recharged electronically are helpful even for people who do not have a bank account. Most money in today's world is electronic, and tangible cash is becoming less frequent. Banks offer many services whereby customer can transfer funds, purchase stocks, contribute to their pension plans and immediate transfer of funds from one account to another without actual paper transfer of money. This offers a great convenience to people and business alike[245].

Cross Border Payments:-Payment methods are the instruments, procedures and institutions which enable users to meet payments obligations. Traditionally payment methods are either paper based, electronic or a combination of both. Credit transfers are a vital means of payment of cross-border. At the retail level, payment cards, are prominent in cross-border payment. In countries like

[243] D. Muraleedharan, Modern Banking theory and Practice, PHI learning Pvt. Ltd, New Delhi, 2012,P.1
[244] Ibid p. 338
[245] Ibid P.319

France, cheques have been used in around 40% of non-cash transactions, in Germany they have constituted less than 5% of such transactions; credit transfers and directs debts have dominated. The sharp decline in the average value of cheques in Britain over the last decade reflects the encouragement for the commercial world to make wholesale payments by paperless credit transfer, rather than by cheques[246]. In, Indiaas on May, 2012, there are 10037761(NRI's) and 11872114(PIO's), total **21909875**Overseas Indians in 205 countries[247]and their remittances to India stood at $67.6 billion in 2012-13, accounts for over 4% of the country's GDP and this grew to $70 billion in 2013-14, the highest amongst the countries receiving remittances from overseas workers[248].The number of Keralites in the UAE is 409,000 and in Saudi Arabia 408,000. The total number of Non-Resident Keralites (NRK) abroad is 1.38 million. Of this, only 1.14 million are working. The remaining are dependents. The least number of Keralites (959) are in Australia[249] and In 2012, the Kerala was the highest receiver of overall remittances to India which stood at $66.13 billion (Rs. 3,42,884.05 crore), followed by Tamil Nadu, Punjab and Uttar Pradesh[250]. But most of these payments are online and there is a danger of cyber crimes or hacking.

Hacking: The information revolution has lead to the creation of 'information highways', operating across the globe through interconnected computer networks. The change has been unprecedented but without pitfalls, which resulted in the new computer cries like hacking which have transgressed national boundaries through cyber space by privacy violation and information theft. Hacking is a successful or unsuccessful attempt to gain unauthorised use or unauthorised access to a computer system[251]. Hackers are of different types, depends upon the technical skill, they can be classified into pirates, browsers, and crackers. Pirates, the least technically proficient hackers, confine their activities copyright violations through software piracy. The browsers, with a moderate technical ability gain unauthorised access to other people's files but usually do not usually damage or copy files. The crackers, the most proficient hackers, abuse their technical abilities by copying files or damaging programmes and systems. Another classification of hackers into White Hats and Black

[246] Ross Cranston, 'Principles of Banking Law', 2nd Edn, Oxford University Press, 2002, P.271
[247] http://moia.gov.in/writereaddata/pdf/NRISPIOS-Data(15-06-12)new.pdf visited on 16/3/2015
[248] http://en.wikipedia.org/wiki/Remittances_to_India visited on 16th March 2015
[249] http://www.bopionews.com/indians.shtml visited 15/3/2015
[250] http://en.wikipedia.org/wiki/Economy_of_Kerala visited on 16/3/2015
[251] Adamski, "Crimes Related to the Computer Network, Threats and Opportunities, A criminological perspective", http:www.ulapland.fi/home/oiffi/enlist/ resources/HeuniWeb.htm visited on 12/3/2015

Hats[252], wherein White Hats tend to finds flaws in security networks for security corporations and improve the sae for the computer users. Black Hats are ill-intentioned hackers who abuse their skills can again be classified into, angry hackers, script hackers, and agenda hackers. Angry Hackers, motivated by hatred for a particular company or group, dedicate their resources to harm them. Script Hackers creates mischief for fun and use hacking tools mad by others. Agenda hackers include those disillusioned by political or economic agenda or terrorist activities through large scale disruption of computer net works. Disgruntled employees or ex-employees who hack into or attack their employer's computer systems either by abusing their privileges or special knowledge constitute the internal group and conduct a 70% of all hacking activity. Professional criminals and cyber terrorists, the most dangerous hackers, are highly skilled, use the latest technology and ay act as mercenaries for corporate or political purpose[253].

Cyber Crimes:- Cyber crime is the most recent type of crime, which affects many people and is the biggest challenge for the police, prosecutors, and law makers. Cyber crime is one of the toughest one which the law enforcing agencies face. Computer crime is facilitated by the tools provided by the computer revolution, viz. Laser printers, scanners, modems, the Internet, the web and the programming tools that give people to have access to money, mail and data of others stored in the computer. The major computer crimes are:-

1. The sabotage of computer or computer networks; sabotage of operating systems and programmes;
2. Theft of data or information;
3. Theft of marketing information;
4. Blackmail based on information collected from computerized files such as personal as well as family information, sexual preferences, financial data, etc.
5. Unlawful access to criminal justice; and
6. Other Government records.

Generally, the targets of computer crime are military and intelligence computers, business houses targeted by competitors; banks and other commercial institutions targeted by white collar

[252] Fitch, Cynthia, Crime and Punishment, http://www.giac.org/practical/GSEC/Cynthia_Fitch_GSEC.pdf visited on 13/3/2015

[253]K.PrasannaRani, 'Cyber Jurisprudence', The ICFAI University Press, Hyderabad, 2008.

criminals. Information stored in computers of Government or service industries, commercial, industrial or trading companies, universities, scientific organisations, research institutions are also accessed illegally by unauthorised means. Some of the computer related bank frauds are:

1. **Credit Card Frauds**:- Credit Cards are stolen and signatures forged. Signatures and information on charge-slips are used for forging the cards.
2. **Automated Teller Machine Frauds** (ATM):- ATM cards are stolen and operated or use to swipe for payments. For many banks passwords are not required to swipe the cards. eg. SBI cards can be swiped only with passwords but Bank of Maharashtra cards can be swiped without any password.
3. **Electronic Funds Transfer Frauds:-** Transfer is effected by cable or telex or through computer network and various codes are used for transmitting bank code, receiving bank code, currency, data, amount, etc.
4. **Misappropriation of funds through manipulation of computerised bank accounts[254].**Bank accounts not maintained in such a way, so that the investor can easily check and understand the same. In *Central Bank of India v. Ravindra*[255], Supreme Court observed,

> *"Banking is an organised institution and most of the banks press into service long-running documents wherein the borrowers fill in the blanks, at times without caring to read what has been provided therein, and bind themselves by the stipulations articulated by the best of legal brains. Borrowers other than those belonging to the corporate sector, find themselves having unwittingly fallen into a trap and rendered themselves liable and obliged to pay interest the quantum whereof may at the end prove to be ruinous.... Statements of accounts supplied by banks to borrowers many a time do not contain particulars or details of debit entries and when written by hands, are worse than medical prescriptions putting to test the eyes and wits of the borrowers*." Hence banking customers fail to understand timely about the misappropriation of money from his accounts.

[254]Yogesh Barua &Denzyl P.Dayal, Cyber Crimes, 2001, Vol.1, P.246-267
[255] (2001) 107 Comp Case 416

Most computer crimes identified:-Criminal activity involving the perpetration of a fraud through the use of the computer or the internet can take many different forms. One common form includes "hacking," in which a perpetrator uses sophisticated technological tools to remotely access a secure computer or internet location. A second common criminal activity involves illegally intercepting an electronic transmission not intended for the interceptor. This may result in the interception of private information such as passwords, credit card information, or other types of so-called identity theft[256]. They are:

1. **Computer network break-in**:- Using software tools installed on computer in remote location, hackers break into the system to steal data, plant virus or Trojan horses or work mischief by changing password.
2. **Computer Virus**: Computer Virus is a computer programme and it is very common because the transfer or infected file from one computer to another causes the virus to replicate. There are thousands of different types of virus. A Trojan horse is the most common destructive type of virus.
3. **Industrial espionage**: These are used to spy the enemy.
4. **Software piracy**: Software illegally copied and distributed annually.
5. **Mail bombing**:- Software that will instruct computer to do everything. Terrorism has hit in the for mail bombings.
6. **Password sniffers**: Password sniffers re programmes that record the name and passwords of network users as they log in.
7. **Spoofing**: Spoofing is an act of disguising one computer electronically looks like another, computer in order to gain access to that system to access valuable documents stored in a computer.
8. **Credit Card Frauds**: In US, half a million dollars are lost annually due to credit card frauds. Frauds with online payments, ATM machines, electronic cards and net banking transactions have become a serious issue. Huge loss of money of people and institutions is caused every year due to these cyber frauds in banking firms, even after tight security measures in electronic transaction. Banks themselves have been found to be involved in fraudulent practices in a big way causing their customers enormous losses.

[256] https://www.law.cornell.edu/wex/computer_and_internet_fraud visited on 14/3/2015

9. **Banking Frauds in India**:-Online Banking Frauds and Cyber crimes in India are on rise the thanks to the growing use of information technology. With limited number of cyber law firms in India, these cyber crimes are not reported properly. Even the cyber security of India is still only catching up[257].

10. Cyber Crimes in Scheduled Commercial Banks in last 4 years[258]:-

Sl. No	Year	Total Cases Reported	Amount Involved (In Lakhs)
1	2009	21966	7233.31
2	2010	15018	4048.94
3	2011	9588	3672.19
4	2012	8322	5266.95

11. **Details of Cyber Frauds in Public Sector Banks in last 4 years.**(Amount in lakhs)

Sl. No	Name of Bank	2009		2010		2011		2012	
		No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved
1	Allahabad Bank	0	0	0	0	1	3.3	0	0
2	Andra Bank	0	0	1	31.85	1	0.52	0	0

[257] https://www.law.cornell.edu/wex/computer_and_internet_fraud visited on 14/3/2015

[258] Soni R.R, Sunrise University, & Soni Neena, Adinath Public School, Alwar, Rajasthan, India. http://www.isca.in/IJMS/Archive/v2/i7/4.ISCA-RJMS-2013-062.pdf visited 14/3/2015

3	Bank of Baroda	6	6.88	5	12.4	5	31.82	3	62.45
4	Bank of India	5	5.21	2	14.61	2	54.49	7	15.82
5	Bank of Maharashtra	4	3.55	4	4.69	2	2.9	3	105.26
6	Bank of Rajasthan	0	0	1	0.31	0	0	0	0
7	Canara Bank	6	1.39	0	0	1	0.6	1	10.24
8	Central Bank of India	2	0.84	2	2.15	0	0	0	0
9	Corporation Bank	2	0.72	2	6.21	5	6.44	47	21.69
10	Dena Bank	0	0	1	2.07	1	0.53	0	0
11	First Rand Bank	0	0	0	0	0	0	14	4.82
12	IDBI Bank	24	16.29	13	15.29	50	44.64	87	203.04
13	Indian Bank	0	0	1	1.41	1	0	4	20.9
14	Indian Overseas Bank	2	0.39	3	1.44	10	41	0	0
15	Oriental Bank	0	0	1	4.75	0	176.03	0	0
16	PNB	33	50.15	108	248.64	28	0	14	99.43

17	SBBJ	2	6.66	2	0.15	2	3.49	1	49.32
18	State Bank of Hyderabad	0	0	0	0	4	63.33	6	50.52
19	State Bank of India	0	0	0	0	2	14.62	0	0
20	State Bank of Indore	1	0.8	0	0	0	0	0	0
21	State Bank of Mysore	0	0	1	1.01	0	0	0	0
22	State Bank of Patiala	0	0	0	0	4	80.45	2	31.42
23	State Bank of Travancore	0	0	0	0	6	10.3	3	3.2
24	Syndicate Bank	2	0.53	1	2.32	1	0.56	2	7.87
25	UCO Bank	2	0.58	1	1.6	0	0	4	31.22
26	Union Bank	5	10.45	7	19.22	2	7.86	9	70.17
27	United Bank	1	1.37	0	0	0	0	6	32.86
28	Vijaya Bank	0	0	0	0	0	0	1	8.4
	Grand Total	97	105.81	156	370.12	128	672.48	214	828.63

12. **Details of Cyber Frauds in Private Sector Banks in last 4 years**.(Amount in lakhs)

Sl. No	Name of Bank	2009		2010		2011		2012	
		No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved	No. of Cases	Amount Involved
1	Axis Bank	20	110.58	14	44.59	23	209.59	85	1225.41
2	Development Credit Bank	2	0.96	2	0.3	0	0	0	0
3	Dhanlaxmi Bank	0	0	3	2.29	1	3.02	4	1.09
4	Federal Bank	0	0	2	20.5	0	0	3	83.69
5	HDFC	211	165.58	208	125.98	386	276.68	525	409.56
6	ICICI	15666	3731.95	9811	1920.28	6013	1096.67	3428	676.51
7	Industrial Bank	0	0	3	7.59	3	1.19	2	4.61
8	J& K Bank	1	4.51	2	6.58	0	0	1	13.88
9	KarurVysya Bank	0	0	1	23.14	0	0	0	0
10	Kotak Mahindra	57	75.26	31	29.63	52	33.11	78	67.64
11	Laxmi Vilas Bank	0	0	0	0	0	0	1	10

12	South Indian Bank	1	2.47	1	0.54	2	0.84	2	0.49
13	Tamilnad Mercantile Bank	0	0	0	0	1	0.27	1	1.49
14	Royal Bank of Scott.	142	141.3	51	44.52	46	49.35	14	12.1
	Grand Total	16100	4232.61	10129	2225.94	6527	1670.72	4144	2506.47

Cyber Security: Bank frauds arecommon**,** inprivate and foreign banks frauds relate to online banking, ATM, cards and other digital banking transactions. Banking cyber frauds in the country are the result of introductory phase of banking technology like ATM, online banking, mobile banking, EFT etc. which need time for people to learn the operations, market and technology to get matured. Regulatory framework also gets stronger by experience. Recently RBI has issued guidelines suggesting measures and reporting methods of cyber fraud cases to be followed by the banks[259]. Security devices should be applied and maintained depends upon the personal need of the customer. Security awareness programme is important for employees to maintain high level of security awareness. Latest devices and techniques need be imparted to regular users. For personal identification, need to limit user activities and unauthorised users. Passwords should be hard to guess, changed continuously and known only to the authorised user. System should keep records of actions taken by each individual to facilitate responsibility. Finger prints are a useful means of identification but not widely used for information systems.

Conclusion: The benefits of modern banking with latest technologies are very helpful to the banking customers. But at the same time there are so many traps through which their money can be transferred to some other accounts without their knowledge, causing financial loss and mental trauma to the bankers and customers alike. Hence it is necessary to take adequate precautions while

[259] Ibid.

making online transactions and there is need for awareness and safety mechanisms about the modern net banking business to help equip with latest banking techniques for beneficial use of its customers.

THE LAW BRIGADE