BANKING FRAUDS AND WAYS TO PREVENT THEM

Amith Donald Menezes* & Dr. Prakash Pinto**
* Assistant Professor, Srinivas Institute of Management Studies, Pandeshwar, Mangalore, Karnataka
** Professor & Dean/ Research Guide, Department of Business Administration, St. Joseph Engineering College, Vamanjoor, Mangalore, Karnataka

Abstract:

Financial institutions face an ever-increasing range of challenges within the financial crime arena, both internal and external. Rapid technological and social changes combined with evolving consumer demands are creating numerous new opportunities for the perpetrators of fraud. Consumers want products that are quicker, faster and easier to use, delivered through the platforms of their own choosing. This paper discusses the various frauds that are in existence in the modern or the e-age banking system & the ways to overcome these frauds or be alert to avoid these frauds.

Index Terms: E-Age, Frauds & Challenges

1. Introduction:

Financial institutions face an ever-increasing range of challenges within the financial crime arena, both internal and external. All institutions/organisations which as part of their normal activities, engage themselves in financial transactions, run the risk of being put to loss sometime or through frauds perpetrated on them. The probability of being defrauded is more in the case of banks as the transactions which they handle involve monetary and financial dealings. Further, they are liable to be defrauded not only by their own employees and constituents but also by third parties. At times persons in two or even all the three of the aforesaid categories collude in perpetration of frauds. Hence the procedure and systems to prevent/expose frauds need adherence at all times and deserve attention and review on a priority and continuous basis.

2. Objectives:

The main objectives of the study are to know

- The meaning of fraud & the Categories of fraud in banking.
- Varieties of fraud associated with technology.
- Suggest Ways of preventing technological frauds.

3. Research Methodology:

Since this is a conceptual paper, the data is collected mainly through secondary sources and then analysed to meet the objectives.

4. Frauds in Banking:

Frauds, as they are popularly understood, are acts of criminal deception resorted to by persons singly or in collusion with others with a view to deriving gains to which they are not legally entitled. As per RBI in the Report of the Study Group on Large Value Bank Frauds

"Fraud is a deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of account 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."

Fraud impacts organizations in several areas including financial, operational, and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be staggering. The losses to reputation, goodwill, and customer relations can be devastating. As fraud can be perpetrated by any employee within an organization or by those from the outside, it is important to have an effective fraud management program in place to safeguard your organization's assets and reputation.

A year-wise break up of fraud cases reported by the banking sector together with the amount involved is given in Table 1 below:

Table 1: Year-wise no. and amount of fraud cases in the banking sector

(No. of cases in absolute terms and amount involved in Rs. crore) **Year**	**No. of cases**	**Total Amount**
2009-10	24,791	2,037.81
2010-11	19,827	3,832.08
2011-12	14,735	4,491.54
2012-13	13,293	8,646.00
Total frauds reported as of March 2013	1,69,190	29,910.12

It may be observed that while the number of fraud cases has shown a decreasing trend from 24791 cases in 2009-10 to 13293 cases in 2012-13 i.e. a decline of 46.37%, the amount involved has increased substantially from Rs 2037.81 crore to Rs. 8646.00 crore i.e. an increase of 324.27%.

5. Category of Frauds:

Broadly, the frauds reported by banks can be divided into three main sub-groups:

- Technology related
- KYC related (mainly in deposit accounts)
- Advances related

Frauds in the Modern era of Banking are mostly related with technology. A closer examination of the reported fraud cases has revealed that around 65% of the total fraud cases reported by banks were technology related frauds (covering frauds committed through /at internet banking channel, ATMs and other alternate payment channels like credit/ debit/prepaid cards). Hence we would be considering only technology related frauds in our present study.

Technology Related Frauds:

The substantially larger proportion of technology related frauds by number is only expected as there has been a remarkable shift in the service delivery model with greater technology integration in the financial services sector. Banks are increasingly nudging their customers to adopt newer service delivery platforms like mobile, internet and social media, for enhanced efficiency and cost-cutting. But while banks' customers have become tech-savvy and started using online banking services and products, evidence suggests that even fraudsters are devising newer ways of perpetrating frauds by exploiting the loopholes in technology systems and processes. There have been several instances of low value frauds wherein the fraudsters have employed hostile software programs or malware attacks, phishing, Vishing (voicemail), SMSishing (text messages), Whaling (targeted phishing on High Networth Individuals) techniques apart from stealing confidential data to perpetrate frauds.

Following are the various technology related frauds in the present generation banks;

ACH Fraud:

Is a generic term used to represent transfer of funds by a fraudster (usually a well connected gang operating across borders) using the login credentials of a victim.

The login credentials are obtained through phishing attacks or by using social engineering techniques.The fraudsters often go scot free leaving the banks and their customers to fight in courts and try to recoup whatever losses they can. The funds are usually transferred to accounts in the names of fictitious persons and then withdrawn as soon as the credit hits. Many of these beneficiary accounts are held in countries with weak law enforcement. Then there are unsuspected money mules lured by prospects of easy money. All this makes recovering the money difficult.

Identity Theft:

The most broadly defined of the types of online banking fraud, identity theft gets the most attention from the media and is of highest concern to consumers. Identity theft can be very simple or quite complex. Identity theft can be extremely difficult for its victims. It can take months or even years to correct the damage it can cause. If the thief has acquired enough information to satisfactorily answer the questions asked by the financial institution, he or she will be able use the information to commit fraud. Because the level and types of questions asked can determine whether or not an identity theft succeeds, those questions must be crafted so that only the true person will know the answers.

Your information can be obtained in any of the following ways:

- ✓ Theft, including theft of mail from your mailbox at home
- ✓ By going through your garbage bins
- ✓ Telephone, Fax and Mail scams
- ✓ Internet.

Friendly Fraud:

This kind of fraud, also known as “civil fraud” or “family fraud,” refers to fraud committed using information that belongs to a trusted friend or family member. As much as financial institutions, independent organizations and the media communicate to consumers that they should not share confidential data, many people do share their information with close friends and family. A growing number of identity theft cases indicate that some close friends and family members will pretend to be the customer and steal from that individual. These are very time-consuming cases to research, but they can present a lower risk to the institution if the case is referred back to the customer to handle in a civil (rather than criminal) manner. Because it can be devastating to an individual to learn that he or she has been deceived by a close friend or family member, these cases can be especially difficult for victims. The strongest defense against this type of fraud is to emphasize to customers the importance of keeping their passwords completely confidential.

Internal Fraud:

This type of fraud is not new, but online banking has added another channel through which an employee can steal. If a financial institution allows employees access to customer data, and that data is the same information needed to gain online access to customer accounts, an employee can easily commit fraud. Because of this, financial institutions should require a password or PIN for online banking, and the password or PIN should be stored in an encrypted format. Another option is to truncate account numbers and customer data and limit employee access to the full numbers.

Cross-Channel Fraud:

Customers – legitimate and otherwise – tend to see the institution as a single brand represented across various contact channels: phone, automated contact center, ATM, branch office and online. But the institution tends to see its customers as diverse entities based on product: mortgage, credit card, DDA, home equity, consumer banking, small business, etc. This disparity creates inefficiencies that fraudsters can exploit. Criminals know the above facts all too well. They know bank fraud systems rarely monitor customer behavior across multiple accounts, channels and systems. That weakness opens the door for cross-channel fraud, in which a fraudster gains access to customer information in one channel and uses that knowledge to commit fraud through another.

Credit Card and Debit Card Fraud:

- ✓ Credit or debit card fraud can also occur when your card is lost or stolen and used by a third party to purchase goods with those cards or to remove cash from the cards.
- ✓ Credit or debit cards can also be intercepted in transit while being sent to you.
- ✓ Your cards can also be compromised by a dishonest merchant who undertakes unauthorised duplicate transactions on your card. This type of crime is known as 'skimming'. It is a crime whereby your credit or debit card can be reproduced in order to use the credit balance to obtain a financial advantage. The creation and/or alteration of a credit/debit card occurs when the information contained on the magnetic strip is reproduced.

Email Scams and Fake Websites:

A number of customers from financial institutions have been targeted with hoax emails. These emails appear to be genuine bank emails. Some emails inform the customer that their security details and passwords need to be updated by logging into an authentic looking, but fake website. The purpose of these websites is to obtain your log on details to access your bank accounts. Others communicate security messages and advise you to install software from the email that checks and removes viruses. By downloading the software you are in fact tricked into downloading a virus.

Computer Threats:

Each and every time you log onto the internet your computer is at risk of various threats with the aim of getting your personal details and accessing your money. Here we describe the main threats to your computer and how to protect yourself from them.

- ✓ Phishing
- ✓ Spyware and Adware
- ✓ Viruses and Worms
- ✓ Trojans.

Phishing:

Phishing is a scam where hackers 'fish' for your personal details by using hoax emails claiming to be from financial institutions. This method continues to be favoured by online thieves. Hoax emails claiming to be from banks are often generated overseas and are sent in bulk. The email asks the recipient to provide sensitive information such as their username, password, customer registration number or PIN by providing a link leading to a fake website, enabling thieves to gather the details for later fraudulent use.

Spyware and Adware:

Spyware:

Spyware is a type of software that cleverly collects user information while on the Internet.

Adware:

Adware is a type of spyware used by marketers to track Internet user's habits and interests for the purpose of customising future advertising material. Adware can monitor information such as the types of sites visited, articles read or the types of pop-ups and banners the user clicks on. The information is then used to customize future advertisements directed to the user, or can be sold to a third party for the same purpose.

Viruses and Worms:

A computer virus is software that affixes itself to another program like a spread sheet or word document. Similar to a biological virus, it must attach itself to another program to survive and reproduce. Unlike Trojans, which are self-sufficient programs, viruses can only run if the infected program is running. While active, the virus attempts to reproduce and attach itself to other programs. This can tie up resources such as disk space and memory, causing problems on any home computer. An email virus is the latest type of computer virus. It is transported through email messages and usually replicates by automatically distributing itself out to all contacts on the victims email address book. A worm is similar to a virus. It exploits computers in a network that contain security holes. Once a security hole is found, the worm will attempt to replicate itself from computer to computer. Like viruses, worms can be equally destructive.

Trojan's:

A Trojan is a destructive program that poses as a harmless application. Unlike viruses, Trojans do not replicate themselves and do not needs a host program to attach to. Today's computer users often accept Trojan horses onto their computers, believing that the program is harmless or even helpful. Some Trojans will claim to get rid the computer of viruses or other harmful applications, but instead introduce viruses and leave it vulnerable to attacks by hackers and intruders. Trojans can appear as pop ups or some don't appear at all and silently in the background do damage.

6. Suggestions for Users to Prevent these Frauds:

- ✓ Ensure you know the person/entity you are giving information to over the Internet.
- ✓ At least once a year, order copies of your credit report from each of the three major credit bureaus, ensuring all of the information is accurate.
- ✓ Monitor your accounts and monthly statements thoroughly, ensuring that all the activity is accurate. If your account statements are late, immediately contact your banks to ascertain if and when they were mailed.
- ✓ Always thoroughly tear or shred personal information, such as pre-approved credit offers, that may contain account information, Social Security numbers, date of birth, etc.
- ✓ Check merchant privacy policies and only shop with those who have published privacy policies that you agree with.
- ✓ Only do business with Internet companies that use a secure form to capture private information, such as an account numbers or credit card numbers. (The key symbol on your browser status bar indicates whether or not a page is secure.)
- ✓ Avoid instant credit offers, ensuring they are properly shredded/discarded.
- ✓ Ensure your computer is equipped with anti-virus protection and firewalls to help keep trespassers out. Always back up your data.
- ✓ Never divulge personal information to anyone, as identity thieves often obtain information through social engineering.
- ✓ Avoid purchasing a product from a merchant or an auction site where the deal looks "too good to be true" because it usually is.

- ✓ Always protect your account information. Don't write your personal identification number (PIN) on your ATM/Debit Card. Don't write your Social Security number and/or credit card number on a check.
- ✓ When using your ATM, cover your hand when entering the PIN number to protect the information from shoulder surfers.
- ✓ Carry only those pieces of identification you absolutely need, and keep them secure.
- ✓ Always log off from your online banking session.
- ✓ If you suspect your identity has been stolen, contact your financial institution and the authorities immediately.

8. Conclusion:

With the advent of technology there have been positive as well as negative impacts to the banking industry. Positive is that technology has brought in lots of savings in terms of time and money to both the bankers as well as the customers. Similarly every good thing comes at a cost and the cost here is the growing amount of frauds that have mushroomed over the years. It is important for all the people involved in this system to be alert, follow rules and never takes things for granted. As Jodi Rell says “At the end of the day, the goals are simple: safety and security

9. References:

1. Soni R R and Soni Neena, 2013,”An investigative study of banking cyber frauds with special reference to private and public sector banks”, Research journal of management studies, Vol 2(7),22-27,July 2013.
2. Ashu Khanna and Bindu Arora, 2009,”A study to investigate the reasons for bank frauds and the implementation of preventive security controls in indian banking industry”, Volume 4, issue 3, 2009.
3. Ellen Joyner, 2011,”Detecting and preventing fraud in financial institutions”,SAS Global Forum 2011, Paper 029-2011
4. Fraud prevention strategies for internet banking, BITS Financial services round table, April 2003.
5. http://www.anz.com/personal/ways-bank/security/online-security/tips-protecting-yourself/
6. http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=8178
7. http://www.mondaq.com/india/x/250030/Financial+Services/Banking+Frauds+Prevent+Or+Lament
8. http://rbi.org.in/scripts/BS_SpeechesView.aspx?Id=826