Audit of Fraud
Fraud Detection Techniques
& Forensic Audit

Reading Material
Vol. II
Cyber Crimes

Indian Audit & Accounts Department

Regional Training Institute

26/1, Civil Lines, Nagpur

E-mail : rtiaadnr_ngp@sancharnet.in

Phone : (0712) - 2545420, 2545816, 2545829

Fax : 0712-2562577

CONTENTS

Sr.No	Topic	Page No.
1.	Full guide on cyber crimes in India- *Mayur Joshi*	1
2.	Internet Fraud	15
3.	Bank frauds and approach to avoid them	25
4.	Computer Crime and Computer Forensics- *Investigative Techniques*	35
5.	Credit card frauds	42
6.	Occupational frauds and money laundering- *Mayur Joshi*	46
7.	Computer print outs can be admitted in the Courts as evidence- A judgment	48

Full Guide on Cyber Crimes in India

Mayur S.Joshi-C.A.,CFE(USA)

Introduction

The invention of the computers has opened new avenues for the fraudsters. It is an evil having its origin in the growing dependence on computers in modern life. Though there is a great talk about the cyber crimes there is nothing called cyber crime. The crimes such as frauds, forgery are traditional and are covered by the separate statutes such as Indian *Penal Code or alikes. However the abuse of computer and the related electronic media* has given birth to a gamut of new types of crimes which has some peculiar features.

A simple yet sturdy definition of these crimes would be "unlawful acts wherein the equipment transforming the information be it a computer or a mobile is either a tool or a target or both". In India the information Technology Act deals with the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Some examples are:

Financial crimes

Wipro Spectramind lost the telemarketing contract from Capital one due to an organized crime. The telemarketing executives offered fake discounts, free gifts to the Americans in order to boost the sales of the Capital one. The internal audit revealed the fact and surprisingly it was also noted that the superiors of these telemarketers were also involved in the whole scenario

Sale of illegal articles:

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'. The clip of the DPS students was kept for selling on the *site called Bazee.com by a student from IIT Kharagpur*

Online gambling (Cyber Lotto an Effective Tool of Frauds)

"It is a classic case of cyber crime, the first of its kind in Andhra Pradesh," was how Vijayawada Police Commissioner Sudeep Lakhtakia summed up the case of cheating and fraud registered against Kola Venkata Krishna Mohan, the self-styled winner of the multi-million dollar Euro lottery. Mohan admitted that he did not win the 12.5 million pound Euro lottery in November 1998, as he had claimed, but merely played fraud to make good his losses in gambling.

"With the help of computers, the accused took the people for a ride," the Vijayawada police commissioner pointed out. Mohan, using the Internet and forged documents, allegedly cheated banks and several persons to the tune of 60 million rupees.

Kola Mohan was arrested by the Vijayawada city police on Monday in connection with cases of fraud and forgery registered against him. He was remanded to judicial custody till December 13 by Fifth Metropolitan Magistrate K B Narsimhulu. He was shifted to the district jail at Gandhinagar in Vijayawada. Mohan was accused of cheating the Andhra Bank to the tune of Rs 1.73 million.

By perpetrating the multi-million rupee fraud, Mohan has achieved the dubious distinction of allegedly committing the first and biggest cyber crime in Andhra. The state, incidentally is making rapid strides in information technology, thanks to the initiative of cyber-savvy Chief Minister N Chandrababu Naidu.

A compulsive gambler who played cards regularly at high stakes in various clubs in the coastal city, Mohan told newsmen at the police commissioner's office at Vijayawada on Monday that he had lost as much as Rs 30 million in 1998 when a gambling syndicate led by a real estate dealer and a restaurant-owner cheated him.

"I was on the look-out to make good the losses by hook or crook. During a visit to London, I learnt about the Euro lottery. I staked some money on it in vain. Then, I invented the story that I won the lottery. I created a website and an email address on the Internet with the address 'eurolottery@usa.net.' Whenever accessed, the site would name

me as the beneficiary of the 12.5 million pound (that is, $ 19.8 million or Rs 840 million) Euro-lottery," Kola Mohan recalled.

A Telugu newspaper in Hyderabad received an email that a Telugu had won the Euro lottery. The website address was given for verification. The newspaper sent the query and got the "confirmation" since Kola Mohan had himself created and manipulated the website.

The Telugu daily published the story and other newspapers and the media in general followed suit. Nobody tried to verify the claim at the genuine address of Euro-lottery. "It was surprising that no newsman asked me either for any proof," Mohan quipped.

Taken for a ride by his claim, people made a beeline to Krishna Mohan for deposits, partnerships, donations etc. He became a celebrity overnight and began leading a luxurious life. He purchased a posh house and cars. He was provided gunmen by the police for his security.

Mohan collected millions of rupees from several individuals and financiers at four to nine per cent interest per month. Some nationalised banks also lent him money in a bid to attract the Euro deposit. He used this money to pay interest to some creditors to retain their confidence. To repay one loan, he took another.

However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs 1.73 million bounced. Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

After the cheque bounced, Andhra Bank authorities verified the authenticity of the bond certificate with the Midland Bank. They were shocked to learn that the bond certificate was fake. Thereupon, on November 25, the Andhra Bank Eluru Road branch officials lodged a complaint with Governorpet police station against Mohan for "cheating and forgery." The police registered a case against him under sections 420, 468 and 471 of the Indian Penal Code.

In the meantime, Chief Minister N Chandrababu Naidu also ordered the Crime Branch-Criminal Investigation Department of the state police to probe into the antecedents of Mohan who had joined the Telugu Desam Party in May this year and even donated one million rupees to the NTR Memorial Trust set up by the TDP.

Mohan claimed that the manager of a London-based company had collaborated with him in realising his plans to defraud people. The police confiscated a laptop, worth Rs 1,40,000, from his possession and also seized some incriminating documents.

Source: rediff.com 30.11.1999

Intellectual Property crimes

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. In other words this is also referred to as cybersquatting. Satyam Vs. Siffy is the most widely known case. Bharti Cellular Ltd. filed a case in the Delhi High Court that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with Network solutions under different fictitious names. The court directed Network Solutions not to transfer the domain names in question to any third party and the matter is sub-judice. Similar issues had risen before various High Courts earlier. Yahoo had sued one Akash Arora for use of the domain name 'Yahooindia.Com' deceptively similar to its 'Yahoo.com'. As this case was governed by the Trade Marks Act, 1958, the additional defence taken against Yahoo's legal action for the interim order was that the Trade Marks Act was applicable only to goods.

e-mail spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g. Gauri has an e-mail address gauri@indiaforensic.com. Her enemy, Prasad spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Gauri, her friends could take offence and relationships could be spoiled for life.

Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Recently, a branch of the Global Trust Bank experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. It was revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. Unfortunately this information proved to be true in the next few days.

But the best example of the email spoofing can be given by the Gujarat Ambuja Executive's case. Where he pretended to be a girl and cheated the Abu dhabi based NRI for crores by blackmailing tactics.

Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners.

Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high quality scanners and printers. In fact, this has becoming a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.Some of the students are caught but this is very rare phenomenon.

Cyber Defamation:

This occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

India's first case of cyber defamation was reported when a company's employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company.

The company was able to identify the employee with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

Cyber stalking

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

Ritu Kohli has the dubious distinction of being the first lady to register the cyber stalking case. A friend of her husband gave her telephonic number in the general chat room. The general chatting facility is provided by some websites like MIRC and ICQ. Where person can easily chat without disclosing his true identity. The friend of husband also encouraged this chatters to speak in slang language to Ms. Kohli.

Now, let us examine some of the acts wherein the computer is the target for an unlawful act. It may be noted that in these activities the computer may also be a tool. This kind of activity usually involves sophisticated crimes usually out of the purview of conventional criminal law. Some examples are:

Unauthorized access to computer systems or networks

This activity is commonly referred to as hacking. The Indian law has, however, given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking". However, as per Indian law, unauthorized access does occur, if hacking has taken place.

An active hackers' group, led by one "Dr. Nuker", who claims to be the founder of Pakistan Hackerz Club, reportedly hacked the websites of the Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and United Nations (India).

Theft of information contained in electronic form

This includes information stored in computer hard disks, removable storage media etc.

Email bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

In one case, a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

Data diddling

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in he bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

Salami attacks

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been supposedly mistreated by his employers the man first

introduced a logic bomb into the bank's systems. Logic bombs are programmes, which get activated on the occurrence of a particular predefined event.

The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters. Then he went and opened an account in the name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither any of the account holders nor the bank officials noticed the fault.

It was brought to their notice when a person by the name of Zygler opened his account in that bank. He was surprised to find a sizeable amount of money being transferred into his account every Saturday. Being an honest person, he reported the "mistake" to the bank authorities and the entire scheme was revealed.

Denial of Service attack

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread.

It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay!

Virus / worm attacks

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate.

In May 2000, this deadly virus became the world's most prevalent virus. It struck one in every five personal computers in the world. When the virus was brought under check the

true magnitude of the losses was incomprehensible. Losses incurred during this virus attack were pegged at US $ 10 billion.

VBS_LOVELETTER utilized the addresses in Microsoft Outlook and e-mailed itself to those addresses. The e-mail which was sent out had "ILOVEYOU" in its subject line. The attachment file was named "LOVE-LETTER-FOR-YOU.TXT.vbs". People wary of opening e-mail attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file. The message in the e-mail was "kindly check the attached LOVELETTER coming from me".

In addition, the Love Bug also uses the Internet Relay Chat (IRC) for its propagation. It e-mails itself to users in the same channel as the infected user.

VBS_LOVELETTER first selects certain files and then inserts its own code in lieu of the original data contained in the file. This way it creates ever-increasing versions of itself.

Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

Logic bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Trojan attacks

A Trojan as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

There are many simple ways of installing a Trojan in someone's computer. To cite an example, two friends Rahul and Mukesh (names changed), had a heated argument over one girl, Radha (name changed) whom they both liked. When the girl, asked to choose, chose Mukesh over Rahul, Rahul decided to get even. On the 14th of February, he sent

Mukesh a spoofed e-card, which appeared to have come from Radha's mail account. The e-card actually contained a Trojan. As soon as Mukesh opened the card, the Trojan was installed on his computer. Rahul now had complete control over Mukesh's computer and proceeded to harass him thoroughly.

Internet time theft

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In May 2000, the economic offences wing, IPR section crime branch of Delhi police registered its first case involving theft of Internet hours. In this case, the accused, Mukesh Gupta an engineer with Nicom System (p) Ltd. was sent to the residence of the complainant to activate his Internet connection. However, the accused used Col. Bajwa's login name and password from various places causing wrongful loss of 100 hours to Col. Bajwa. Delhi police arrested the accused for theft of Internet time.

On further inquiry in the case, it was found that Krishan Kumar, son of an ex army *officer, working as senior executive in M/s Highpoint Tours & Travels had used Col* Bajwa's login and passwords as many as 207 times from his residence and twice from his office. He confessed that Shashi Nagpal, from whom he had purchased a computer, gave the login and password to him. The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cyber crimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under *his directions raided and arrested Krishan Kumar under sections* 379, 411, 34 of IPC and section 25 of the Indian Telegraph Act. In another case, the Economic Offences Wing of Delhi Police arrested a computer engineer who got hold of the password of an Internet user, accessed the computer and stole 107 hours of Internet time from the other person's account. He was booked for the crime by a Delhi court during May 2000.

Web jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more *control over what appears on that website. In a recent incident reported in the USA the*

owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her. The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail.

It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'. In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'.

Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured!

Theft of computer system

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

Physically damaging a computer system

This crime is committed by physically damaging a computer or its peripherals.

This is just a list of the known frauds in the cyber world. The unknown frauds might be far ahead of these since the lawbreakers are always one step ahead of lawmakers.

****

Case of Cyber stalking

Little did Seema Khanna (name changed), an employee with an embassy in New Delhi, know that web surfing would lead to an invasion of her privacy. In an apparent case of cyber stalking, Khanna (32) received a series of e-mails from a man asking her to either pose in the nude for him or pay Rs 1 lakh to him. In her complaint to Delhi Police, the woman said she started receiving these mails in the third week of November.

The accused threatened Khanna that he would put her morphed pictures on display at sex websites , along with her telephone number and address. He also allegedly threatened to put up these pictures in her neighborhood in southwest Delhi. "Initially, she ignored the mails , but soon she started receiving letters through post, repeating the same threat. She was forced to report the matter to the police," said an officer with cyber crime cell.

That, however, was not the end of her ordeal. The accused mailed the woman her photographs . The woman claimed these were the same photographs which she had kept in her mail folder. The police said the accused had hacked her e-mail password which enabled him to access the pictures.

A preliminary inquiry into the complaint has revealed that the mails were sent to the victim from a cyber cafe in south Delhi. "We hope to trace the accused soon," said deputy commissioner of police (crime) Dependra Pathak.

The police feel the accused might be known to the victim as he seemed to know a lot about her.

The cyber stalker can be booked under Section 509 of the IPC for outraging the modesty of a woman and also under the Information Technology Act, 2000.

Net crime

• Woman threatened by cyber stalker who managed to get her photographs from her mail folder

• In another case, a housewife started receiving obscene calls from across the world after a hacker flashed her details on the Net

• Delhi Police set up two computer training centres this year to enable its staff to investigate cyber crime

• The police admit IT Act, 2000 is not enough to deal with cyber

Source: Times of India 26.12.2003

Case of Cyber Extortion

He does not know much about computer hacking, yet 51-year-old cyber criminal Pranab Mitra has stunned even the cyber crime investigation cell of Mumbai police with his bizarre fraud on the Net. Mitra, a former executive of Gujarat Ambuja Cement, was arrested on Monday for posing as a woman and seducing online an Abu Dhabi-based man,

thereby managing to extort Rs 96 lakh from him. Investigating officer, Assistant Commissioner of Police, J.S. Sodi, said Mitra has been remanded to police custody till June 24, and has been booked for cheating, impersonation, blackmail and extortion under sections 420, 465, 467, 471, 474 of the IPC, read with the newly formed Information Technology Act.

Mitra posed as a woman, Rita Basu, and created a fake e-mail ID through which he contacted one V.R. Ninawe. According to the FIR, Mitra trapped Ninawe in a ''cyber-relationship'' sending emotional messages and indulging in online **sex** since June 2002.Later, Mitra sent an e-mail that ''she would commit suicide'' if Ninawe ended the relationship. He also gave him ''another friend Ruchira Sengupta's'' e-mail ID which was in fact his second bogus address. When Ninawe mailed at the other ID he was shocked to learn that Mitra had died. Then Mitra began the emotional blackmail by calling up Abu Dhabi to say that police here were searching for Ninawe. Ninawe panicked on hearing the news and asked Mitra to arrange for a good advocate for his defence. Ninawe even deposited a few lakh in the bank as advocate fees. Mitra even sent e-mails as high court and police officials to extort more money. Ninawe finally came down to Mumbai to lodge a police case

Internet fraud

(From Wikipedia, the free encyclopedia)

The term "**Internet fraud**" generally refers to any type of fraud scheme that uses one or more online services - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Overview

Internet fraud is committed in several ways. The police agencies worldwide have people assigned to combat this type of fraud; according to figures from the FBI, U.S. companies' losses due to Internet fraud in 2003 surpassed US$500 million. In some cases, fictitious merchants advertise goods for very low prices and never deliver. However, that type of fraud is minuscule compared to criminals using stolen credit card information to buy goods and services.

Bank Fraud Statistics in India

Year	Amount	Cases
2002	599.53 cr.	1744
2003	653.5 cr.	2207
2004	600.16 cr.	2663

The Internet serves as an excellent tool for investors, allowing them to easily and inexpensively research investment opportunities. But the Internet is also an excellent tool for fraudsters.

Geographic origin

In some cases Internet Fraud schemes originate in the US and European countries, but a significant proportion seems to come from Africa, particularly Nigeria, and sometimes from Ghana and Egypt. Some originate in Eastern Europe, Southwest Asia and China. For some reason, many fraudulent orders seem to originate from Belgium, from Amsterdam in the Netherlands, from Norway, and from Malmö in Sweden.

Geographic targets

Europe and the US are the leading targets of this type of fraud.

Popular products

Fraudsters seem to prefer small and valuable products, such as: watches, jewelry, laptops, digital cameras, and camcorders. These items are usually commodities that are easily sellable and have a broad range of appeal. However, fraud in hosted marketplaces such as Ebay covers a broad range of products from cellular phones to desktop computers. The craft has continually evolved in sophistication. In some instances, a picture of the product is sent in place of the actual product. Other times, products are outright never sent after the bill is charged to credit card accounts. Victims are left to deal with credit card companies for chargebacks.

Identity theft schemes

Stolen credit cards

Most Internet fraud is done through the use of stolen credit card information which is obtained in many ways, the simplest being copying information from retailers, either online or offline. There have been many cases of hackers obtaining huge quantities of credit card information from companies' databases. There have been cases of employees of companies that deal with millions of customers in which they were selling the credit card information to criminals.

Despite the claims of the credit card industry and various merchants, using credit cards for online purchases can be insecure and carry a certain risk. Even so called "secure transactions" are not fully secure, since the information needs to be decrypted to plain text in order to process it. This is one of the points where credit card information is typically stolen.

Get wire transfer info

Some fraudsters approach merchants asking them for large quotes. After they quickly accept the merchant's quote, they ask for wire transfer information to send payment. Immediately, they use online check issuing systems as Qchex that require nothing but a working email, to produce checks that they use to pay other merchants or simply send associates to cash them.

Purchase scams

Direct solicitations

The most straightforward type of purchase scam is a buyer in another country approaching many merchants through spamming them and directly asking them if they can ship to them using credit cards to pay.

An example of such email is as follows:

From: XXXXXX XXXXXX [XXXXXXX@hotmail.com] Sent: Saturday, October 01, 2005 11:35 AM Subject: International order enquiry

Goodday Sales, This is XXXXXX XXXXXXX and I will like to place an order for some products in your store, But before I proceed with listing my requirements, I will like to know if you accept credit card and can ship internationally to Lagos, Nigeria. Could you get back to me with your website so as to forward you the list of my requirements as soon as possible. Regards, XXXXXX XXXXXX, XXXXXXXX Inc. 9999 XXXXX street, Mushin, Lagos 23401, Nigeria Telephone: 234-1-99999999, Fax: 234-1-9999999, Email: XXXXXXXXX@hotmail.com

Most likely, a few weeks or months after the merchant ships and charges the Nigerian credit card, he/she will be hit with a chargeback from the credit card processor and lose all the money.

Counterfeit Postal Money Orders

According to the FBI and postal inspectors, there has been a significant surge in the use of Counterfeit Postal Money Orders since October 2004. More than 3,700 counterfeit postal money orders (CPMOs) were intercepted by authorities from October to December of 2004; and according to the USPS, the "quality" of the counterfeits is so good that ordinary consumers can easily be fooled.

On March 9, 2005, the FDIC issued an alert [1] stating that it had learned that counterfeit U.S. Postal Money Orders had been presented for payment at financial institutions.

On April 26, 2005, Tom Zeller Jr. wrote an article in *The New York Times*[2] regarding a surge in the quantity and quality of the forging of U.S. Postal Money Orders, and its use to commit online fraud. The article shows a picture of a man that had been corresponding with a woman in Nigeria through a dating site, and received several fake postal money orders after the woman asked him to buy a computer and mail it to her.

Who has received Counterfeit Postal Money Orders (CPMOs):

- Small Internet retailers.
- Classified advertisers.
- Individuals that have been contacted through email or chat rooms by fraudsters posing as prospective social interests or business partners, and convinced to help the fraudsters unknowingly.

Geographical origin:

- Mostly from Nigeria
- Ghana

- Eastern Europe

The penalty for making or using counterfeit postal money orders is up to ten years in jail and a US$25,000 fine.

Online automotive fraud

There are two basic schemes in online automotive fraud:

1. A fraudster posts a vehicle for sale on an online site, generally for luxury or sports cars advertised for thousands less than market value. The details of the vehicle, including photos and description, are typically lifted from sites such as eBay Motors and re-posted elsewhere. An interested buyer, hopeful for a bargain, emails the seller, who responds saying the car is still available but is located overseas. He then instructs the buyer to send a deposit via wire transfer to initiate the "shipping" process. The unwitting buyer wires the funds, and doesn't discover until days or weeks later that they were scammed.

2. A fraudster feigns interest in an actual vehicle for sale on the Internet. The "buyer" explains that a client of his is interested in the car, but due to an earlier sale that fell through has a certified check for thousands more than the asking price and requests the seller to send the balance via wire transfer. If the seller agrees to the transaction, the buyer sends the certified check via express courier (typically from Nigeria). The seller takes the check to their bank, which makes the funds available immediately. Thinking the bank has cleared the check, the seller follows through on the transaction by wiring the balance to the buyer. Days later, the check bounces and the seller realizes they have been scammed. But the money has long since been picked up and is not recoverable.

In another type of fraud, a fraudster contacts the seller of an automobile, asking for the vehicle identification number, putatively to check the accident record of the venhicle. However, the supposed buyer actually uses the VIN to make fake papers for a stolen car that is then sold.

Cash the check system

In some cases, fraudsters approach merchants and ask for large orders: $50,000 to $200,000, and agree to pay via wire transfer in advance. After brief negotiation, the buyers gives an excuse about the impossibility of sending a bank wire transfer. The buyer then offers to send a check, stating that the merchant can wait for the check to clear before shipping any goods. The check received, however, is a counterfeit of a check from a medium to large U.S. company. If asked, the buyer will claim that the check is money owed from the large company. The merchant deposits the check and it clears, so the goods are sent. Only later, when the larger company notices the check, will the merchant's account be debited.

In some cases, the fraudsters agree to the wire but ask the merchant for their bank's address. The fraudsters send the counterfeited check directly to the merchant's bank with a note asking to deposit it to the merchant's account. Unsuspecting bank officers deposit the check, and then the fraudster contacts the merchant stating that they made a direct deposit into the merchant's account.

Re-shippers

Re-shipping scams trick individuals or small businesses into shipping goods to countries with weak legal systems. The goods are generally paid for with stolen or fake credit cards.

Nigerian version

In the Nigerian version, the fraudsters have armies of people actively recruiting single women from western countries through chat & matchmaking sites. At some point, the fraudster promises to marry the lady and come to their home country in the near future. Using some excuse the fraudster asks permission of his "future wife" to ship some goods he is going to buy before he comes. As soon as the woman accepts the fraudster uses several credit cards to buy at different Internet sites simultaneously. In many cases the correct billing address of the cardholder is used, but the shipping address is the home of the unsuspecting "future wife". Around the time when the packages arrive, the fraudster invents an excuse for not coming and tells his "bride" that he urgently needs to pick up most or all the packages. Since the woman has not spent any money, she sees nothing wrong and agrees. Soon after, she receives a package delivery company package with pre-printed labels that she has agreed to apply to the boxes that she already has at home. The next day, all boxes are picked up by the package delivery company and shipped to the fraudster's real address (in Nigeria or elsewhere). After that day the unsuspecting victim stops receiving communications from the "future husband" because her usefulness is over. To make matters worse, in most cases the fraudsters were able to create accounts with the package deliverer, based on the woman's name and address. So, a week or two later, the woman receives a huge freight bill from the shipping company which she is supposed to pay because the goods were shipped from her home. Unwillingly, the woman became the fraudster re-shipper and helped him with his criminal actions.

East European version

This is a variant of the Nigerian Version, in which fraudsters recruit people through classified advertising. The fraudsters present themselves as a growing European company trying to establish a presence in the U.S. and agree to pay whatever the job applicant is looking to make, and more. The fraudsters explain to the unsuspecting victim that they will buy certain goods in the U.S. which need to be re-shipped to a final destination in Europe. When everything is agreed they start shipping goods to the re-shipper's house. The rest is similar to the Nigerian Version. Sometimes, when the fraudsters send the labels to be applied to the boxes, they also include a fake cheque, as payment for the re-shipper's services. By the time the cheque bounces unpaid, the boxes have been picked up already and all communication between fraudster and re-shipper has stopped.

Chinese version

This is a variant of the East European Version, in which fraudsters recruit people through spam. The fraudsters present themselves as a growing Chinese company trying to establish a presence in the U.S. or Europe and agree to pay an agent whatever the unsuspecting victim is looking to make, and more. Here is an example of a recruiting email:

> *Dear Sir Madam, I am Mr: XXX XXX, managining XXXXXXXXXXX Corp. We are a company who deal on mechanical equipment, hardware and minerals, electrical products, Medical & Chemicals, light industrial products and office equipment, and export into the Canada America and Europe. We are searching for representatives who can help us establish a medium of getting to our costumers in the Canada America and Europe as well as making payments through you to us. Please if you are interested in transacting business with us we will be glad. Please contact us for more information. Subject to your satisfaction you will be given the opportunity to negotiate your mode of which we will pay for your services as our representative in Canada America and Europe. Please if you are interested forward to us your phone number fax and your full contact addresses. Thanks in advance. Mr. XXX XXX. Managing Director"*

Call tag scam

The Merchant Risk Council reported that the "call tag" scam re-emerged over the 2005 holidays and several large merchants suffered losses. Under the scheme, criminals use stolen credit card information to purchase goods online for shipment to the legitimate cardholder. When the item is shipped and the criminal receives tracking information via email, he/she calls the cardholder and falsely identifies himself as the merchant that shipped the goods, saying that the product was mistakenly shipped and asking permission to pick it up upon receipt. The criminal then arranges the pickup issuing a "call tag" with a shipping company different that the one the original merchant used. The cardholder normally doesn't notice that there is a second shipping company picking up the product, which in turn has no knowledge it is participating in a fraud scheme. The cardholder then notices a charge in his card and generates a chargeback to the unsuspecting merchant.

Business opportunity/"Work-at-Home" schemes

Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay anywhere from $35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

Often, after paying a registration fee, the applicant will be sent advice on how to place ads similar to the one that recruited him in order to recruit others, which is effectively a pyramid scheme.

Other types of work at home scams include home assembly kits. The applicant pays a fee for the kit, but after assembling and returning the item, it's rejected as sub-standard, meaning the applicant is out of pocket for the materials. Similar scams include home-working directories, medical billing, data entry at home or reading books for money.

Website scams

Click fraud

The latest scam to hit the headlines is the multi-million dollar Clickfraud which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via Spyware, the affiliate is then paid a commission on the cost-per-click that was artificially generated. Affiliate programs such as Google's Adsense capability pay high commissions that drive the generation of bogus clicks. With paid clicks costing as much as $100 and an online advertising industry worth more than $10 Billion, this form of Internet fraud is on the increase.

International modem dialing

Many consumers connect to the Internet using a modem calling a local telephone number. Some web sites, normally containing adult content, use international dialing to trick consumers into paying to view content on their web site. Often these sites purport to be free and advertise that no credit card is needed. They then prompt the user to download a "viewer" or "dialer" to allow them to view the content. Once the program is downloaded it disconnects the computer from the Internet and proceeds to dial an international long distance or premium rate number, charging anything up to US$7-8 per minute. An international block is recommended to prevent this, but in the U.S. and Canada, calls to the Caribbean (except Haiti) can be dialed with a "1" and a three-digit area code, so such numbers, as well as "10-10 dial-round" phone company prefixes, can circumvent an international block.

Another type of Click Fraud

This type of fraud involves a supposed internet marketing specialist presenting a prospective client with detailed graphs and charts that indicate that his web site receives (x) thousands of hits per month, emphasizing that if you pay for his services you will succeed in getting a number clicks converted to customers or clients.

When you receive no request for more information and no clients, the frauster responds that it must be something you web site is not doing right.

One recent experience resulted in the discovery that this fraudster's website had 176,000 pages, all with the same or very similar pages, they keywords included the days of the week and the months of the year, but nothing to do with any business except the fraudsters details. The experience resulted in the loss of £950 english pounds equivalent to US$1860.

Phishing

"Phishing" is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message). It is a form of social engineering attack.

The term was coined in the mid 1990s by crackers attempting to steal AOL accounts. An attacker would pose as an AOL staff member and send an instant message to a potential victim. The message would ask the victim to reveal his or her password, for instance to "verify your account" or to "confirm billing information". Once the victim gave over the password, the attacker could access the victim's account and use it for criminal purposes, such as spamming.

Phishing has been widely used by fraudsters using spam messages masquerading as large banks (Citibank, Bank of America) or PayPal. These fraudsters can copy the code and graphics from legitimate websites and use them on their own sites to create a legitimate-looking scam web pages. They can also link to the graphics on the legitimate sites to use on their own scam site. These pages are so well done that most people cannot tell that they have navigated to a scam site. Fraudsters will also put the text of a link to a legitimate site in an e-mail but use the source code to links to own fake site. This can be revealed by using the "view source" feature in the e-mail application to look at the destination of the link or putting the cursor over the link and looking at the code in the status bar of the browser. Although many people don't fall for it, the small percentage of people that do fall for it, multiplied by the sheer numbers of spam messages sent, presents the fraudster with a substantial incentive to keep doing it.

Anti-phishing technologies are now available.

Pharming

Pharming is the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the domain name for a site, and to redirect that website's traffic to another web site. DNS servers are the machines responsible for resolving internet names into their real addresses - the "signposts" of the internet.

If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to "phish" or steal a computer user's passwords, PIN or account number. Note that this is only possible when the original site was not SSL protected, or when the user is ignoring warnings about invalid server certificates.

For example, in January 2005, the domain name for a large New York ISP, Panix, was hijacked to a site in Australia. In 2004 a German teenager hijacked the eBay.de domain name.

Secure e-mail provider Hushmail was also caught by this attack on 24th of April 2005 when

the attacker rang up the domain registrar and gained enough information to redirect users to a defaced webpage.

Anti-pharming technologies are now available.

Auction and retail schemes online

Fraudsters launch auctions on eBay or TradeMe with very low prices and no reservations especially for high priced items like watches, computers or high value collectibles. They received payment but never delivers, or delivers an item that is less valuable than the one offered, such as counterfeit, refurbished or used. Some fraudsters also create complete webstores that appear to be legitimate, but they never deliver the goods. In some cases, some stores or auctioneers are legitimate but eventually they stopped shipping after cashing the customers' payments.

Sometimes fraudsters will combine phishing to hijacking legitimate member accounts on eBay, typically with very high numbers of positive feedback, and then set up a phony online store. They received payment usually via check, money-order, cash or wire transfer but never deliver the goods; then they leave the poor, unknowing eBay member to sort out the mess. In this case the fraudster collects the money while ruining the reputation of the conned eBay member and leaving a large number of people without the goods they thought they purchased.

Stock market manipulation schemes

These are also called investment schemes online. Criminals use these to try to manipulate securities prices on the market; for their personal profit. According to enforcement officials of the Securities and Exchange Commission, the 2 main methods used by these criminals are:

Pump-and-dump schemes

False and/or fraudulent information is disseminated in chat rooms, forums, internet boards and via email (spamming), with the purpose of causing a dramatic price increase in thinly traded stocks or stocks of shell companies (the "pump"). As soon as the price reaches a certain level, criminals immediately sell off their holdings of those stocks (the "dump"), realizing substantial profits before the stock price falls back to its usual low level. Any buyers of the stock who are unaware of the fraud become victims once the price falls. When they realize the fraud, it is too late to sell. They lost a high percentage of their money. Even if the stock value does increase, the stocks may be hard to sell because of lack of interested buyers, leaving the shareholder with the shares for a far longer term than desired.

Short-selling or "scalping" schemes

This scheme takes a similar approach to the "pump-and-dump" scheme, by disseminating

false or fraudulent information through chat rooms, forums, internet boards and via email (spamming), but this time with the purpose of causing dramatic price decreases in a specific company's stock. Once the stock reaches a certain low level, criminals buy the stock or options on the stock, and then reverse the false information or just wait for it to wear off with time or to be disproved by the company or the media. Once the stock goes back to its normal level, the criminal sells the stock or option and reaps the huge gain.

Avoiding Internet investment scams

The US Security Exchange Commission have enumerated guideline on how to avoid internet investment scams. The summary are as follows:

- The Internet allows individuals or companies to communicate with a large audience without spending a lot of time, effort, or money. Anyone can reach tens of thousands of people by building an Internet web site, posting a message on an online bulletin board, entering a discussion in a live "chat" room, or sending mass e-mails.
- If you want to invest wisely and steer clear of frauds, you must get the facts.
- The types of investment fraud seen online mirror the frauds perpetrated over the phone or through the mail. Consider all offers with skepticism.

Reference

1. ^ Counterfeit U.S. Postal Money Orders Counterfeit postal money orders are reportedly in circulation (FDIC) March 9, 2005

^ A Common Currency for Online Fraud Forgers of U.S. Postal Money Orders Grow by Tom Zeller Jr (NYT) April 26, 2005

Bank Frauds

Bank fraud is a crime in many countries, defined as planning to obtain property or money from any federally insured financial institution. It is sometimes considered a white-collar crime.

Most other countries like the United Kingdom, Australia and New Zealand declare this offence at a similar level of severity.

China has executed bankers for fraudulent activity; some recent cases (Sept '04) which ended in capital punishment include:

- Wang Liming, former accounting officer, China Construction Bank, Henan, with others stole 20 million yuan ($2.4 million) from the bank using fraudulent papers, executed.
- Miao Ping, an accomplice in the same case, executed.
- Wang Xiang, same bank in an unrelated case, also executed for taking 20 million yuan from the bank.
- Liang Shihan, Bank of China, Zhuhai, executed for helping cheat his bank out of $10.3 million.

Fraud by insiders

Rogue traders

A rogue trader is a highly placed insider nominally authorised to invest sizeable funds on behalf of the bank; this trader secretly makes progressively more aggressive and risky investments using the bank's money, when one investment goes bad, the rogue trader engages in further market speculation in the hope of a quick profit which would hide or cover the loss.

Unfortunately, when one investment loss is piled onto another, the costs to the bank can reach into the hundreds of millions of dollars; there have even been cases in which a bank goes out of business due to market investment losses.

Some of the largest bank frauds ever detected were perpetrated by currency traders John Rusnak and Nick Leeson.

Fraudulent loans

One way to remove money from a bank is to take out a loan, a practice bankers would be more than willing to encourage if they know that the money will be repaid in full with interest. A fraudulent loan, however, is one in which the borrower is a business entity controlled by a dishonest bank officer or an accomplice; the "borrower" then declares bankruptcy or vanishes and the money is gone. The borrower may even be a non-existent

entity and the loan merely an artifice to conceal a theft of a large sum of money from the bank.

Wire fraud

Wire transfer networks such as the international SWIFT interbank fund transfer system are tempting as targets as a transfer, once made, is difficult or impossible to reverse. As these networks are used by banks to settle accounts with each other, rapid or overnight wire transfer of large amounts of money are commonplace; while banks have put checks and balances in place, there is the risk that insiders may attempt to use fraudulent or forged documents which claim to request a bank depositor's money be wired to another bank, often an offshore account in some distant foreign country.

Forged or fraudulent documents

Forged documents are often used to conceal other thefts; banks tend to count their money meticulously so every penny must be accounted for. A document claiming that a sum of money has been borrowed as a loan, withdrawn by an individual depositor or transferred or invested can therefore be valuable to a thief who wishes to conceal the minor detail that the bank's money has in fact been stolen and is now gone.

Uninsured deposits

There are a number of cases each year where the bank itself turns out to be uninsured or not licensed to operate at all. The objective is usually to solicit for deposits to this uninsured "bank", although some may also sell stock representing ownership of the "bank". Sometimes the names appear very official or very similar to those of legitimate banks. For instance, the "Chase Trust Bank" of Washington DC appeared in 2002 with no licence and no affiliation to its seemingly apparent namesake; the real Chase Manhattan Bank is based in New York.

There is a very high risk of fraud when dealing with unknown or uninsured institutions.

The risk is greatest when dealing with offshore or Internet banks (as this allows selection of countries with lax banking regulations), but not by any means limited to these institutions. There is an annual list of unlicensed banks on the US Treasury Department site which currently is fifteen pages in length.

Theft of identity

Dishonest bank personnel have been known to disclose depositors' personal information for use in theft of identity frauds. The perpetrators then use the information to obtain identity cards and credit cards using the victim's name and personal information.

Demand Draft Fraud

This fraud is usually done by one or more dishonest bank employees. They remove few DD leaves or DD books from stock and write them like a regular DD. Since they are insiders they know the coding, punching of a demand draft. These Demand drafts will be issued payable at distant town/city without debiting an account. Then it will be cashed at the payable branch. For the paying branch it is just another DD. This kind of fraud will be discovered only when the head office does the branch-wise reconciliation, which normally will take 6 months. By that time the money is unrecoverable.

Bill Discounting Fraud

This particular method of fraud is currently in use in the banking sector. Essentially a confidence trick, a fraudster uses a company at their disposal to gain confidence with a bank, by appearing as a genuine, profitable customer. To give the illusion of being a desired customer, the company regularly and repeatedly uses the bank to get payment from one or more of its customers. These payments are always made, as the customers in question are part of the fraud, actively paying any and all bills raised by the bank. After time, after the bank is happy with the company, the company requests that the bank settles its balance with the company before billing the customer. Again, business continues as normal for the fraudulent company, its fraudulent customers, and the unwitting bank. Only when the outstanding balance between the bank and the company is sufficiently large, the company takes the payment from the bank, and the company and its customers disappear, leaving no-one to pay the bills issued by the bank.

Fraud by others

Forgery and altered cheques

Thieves have altered cheques to change the name (in order to deposit cheques intended for payment to someone else) or the amount on the face of a cheque (a few strokes of a pen can change $100.00 into $100,000.00, although such a large figure may raise some eyebrows).

Instead of tampering with a real cheque, some fraudsters will attempt to forge a depositor's signature on a blank cheque or even print their own cheques drawn on accounts owned by others, non-existent accounts or even alleged accounts owned by non-existent depositors. The cheque will then be deposited to another bank and the money withdrawn before the cheque can be returned as invalid or for non-sufficient funds.

Stolen cheques

Some fraudsters obtain access to facilities handling large amounts of cheques, such as a mailroom or post office or the offices of a tax authority (receiving many cheques) or a corporate payroll or a social or veterans' benefit office (issuing many cheques). A few

cheques go missing; accounts are then opened under assumed names and the cheques (often tampered or altered in some way) deposited so that the money can then be withdrawn by thieves. Stolen blank chequebooks are also of value to forgers who then sign as if they were the depositor.

Accounting fraud

In order to hide serious financial problems, some businesses have been known to use fraudulent bookkeeping to overstate sales and income, inflate the worth of the company's assets or state a profit when the company is operating at a loss. These tampered records are then used to seek investment in the company's bond or security issues or to make fraudulent loan applications in a final attempt to obtain more money to delay the inevitable collapse of an unprofitable or mismanaged firm.

Accounting fraud has also been used to conceal other theft taking place within a company.

Cheque kiting

Cheque kiting exploits a system in which, when a cheque is deposited to a bank account, the money is made available immediately even though it is not removed from the account on which the cheque is drawn until the cheque actually clears.

Deposit ¤1000 in one bank, write a cheque on that amount and deposit it to your account in another bank; you now have ¤2000 until the cheque clears.

In-transit or non-existent cash is briefly recorded in multiple accounts.

A cheque is cashed and, before the bank receives any money by clearing the cheque, the money is deposited into some other account or withdrawn by writing more cheques. In many cases, the original deposited cheque turns out to be a forged cheque.

Some perpetrators have swapped checks between various banks on a daily basis, using each to cover the shortfall for a previous cheque.

What they were actually doing was check kiting; like a kite in the wind, it flies briefly but eventually has to come back down to the ground.

Payment card fraud

Credit card fraud is widespread as a means of stealing from banks, merchants and clients.

Booster cheques

A booster cheque is a fraudulent or bad cheque used to make a payment to a credit card account in order to "bust out" or raise the amount of available credit on otherwise-legitimate credit cards. The amount of the cheque is credited to the card account by the bank as soon as

the payment is made, even though the cheque has not yet cleared. Before the bad cheque is discovered, the perpetrator goes on a spending spree or obtains cash advances until the newly-"raised" available limit on the card is reached. The original cheque then bounces, but by then it is already too late.

Stolen payment cards

Often, the first indication that a victim's wallet has been stolen is a 'phone call from a credit card issuer asking if the person has gone on a spending spree; the simplest form of this theft involves stealing the card itself and charging a number of high-ticket items to it in the first few minutes or hours before it is reported as stolen.

A variant of this is to copy just the credit card numbers (instead of drawing attention by stealing the card itself) in order to use the numbers in online frauds.

Duplication or skimming of card information

This takes a number of forms, ranging from a dishonest merchant copying clients' credit card numbers for later misuse (or a thief using carbon copies from old mechanical card imprint machines to steal the info) to the use of tampered credit or debit card readers to copy the magnetic stripe from a payment card while a hidden camera captures the numbers on the face of the card.

Some thieves have surreptitiously added equipment to publicly accessible automatic teller machines; a fraudulent card stripe reader would capture the contents of the magnetic stripe while a hidden camera would sneak a peek at the user's PIN. The fraudulent equipment would then be removed and the data used to produce duplicate cards that could then be used to make ATM withdrawals from the victims' accounts.

Impersonation and theft of identity

"I lived the life of Riley... well, until Riley reported his credit cards as missing."

Theft of identity has become an increasing problem; the scam operates by obtaining information about a victim, then using the information to apply for identity cards, accounts and credit in that person's name. Often little more than name, parents' name, date and place of birth are sufficient to obtain a birth certificate; each document obtained then is used as identification in order to obtain more identity documents. Government-issued standard identification numbers such as "social security numbers" are also valuable to the identity thief.

Information may be obtained from insiders (such as dishonest bank or government employees), by fraudulent offers for employment or investments (in which the victim is asked for a long list of personal information) or by sending forged bank or taxation correspondence. Some fictitious tax forms which purported to have been sent by banks to clients in 2002 were:

- W-9095 Application Form for Certificate Status/Ownership for Withholding Tax
- W-8BEN Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding
- W-8888

The actual origin of these forms is neither the bank nor the taxman - they're sent by would-be identity thieves and W-8888 doesn't exist, W-9095 is also fictitious (the real W-9 asks much less info) and W-8BEN is real but may have been tampered to add intrusive additional questions. The original forms on which these fakes were based are intended to collect information for income tax on income from deposits and investment.

In some cases, a name/SIN pair is needed to impersonate a citizen while working as an illegal immigrant but often the identity thieves are using the bogus identity documents in the commission of other crimes or even to hide from prosecution for past crimes. The use of a stolen identity for other frauds such as gaining access to bank accounts, credit cards, loans and fraudulent social benefit or tax refund claims is not uncommon.

Unfortunately for the banks, identity thieves have been known to take out loans and disappear with the cash, quite content to see the wrong persons blamed when the debts go bad or the police come calling.

Fraudulent loan applications

These take a number of forms varying from individuals using false information to hide a credit history filled with financial problems and unpaid loans to corporations using accounting fraud to overstate profits in order to make a risky loan appear to be a sound investment for the bank.

Some corporations have engaged in over-expansion, using borrowed money to finance costly mergers and acquisitions and overstating assets, sales or income to appear solvent even after becoming seriously financially overextended. The resulting debt load has ruined entire large companies, such as Italian dairy conglomerate Parmalat, leaving banks exposed to massive losses from bad loans.

Prime bank fraud

The "prime bank" operation which claims to offer an urgent, exclusive opportunity to cash in on the best-kept secret in the banking industry, guaranteed deposits in "prime banks", "constitutional banks", "bank notes and bank-issued debentures from top 500 world banks", "bank guarantees and standby letters of credit" which generate spectacular returns at no risk and are "endorsed by the World Bank" or various national governments and central bankers sounds too good to be true?

It is too good to be true.

These official-sounding phrases and more are the hallmark of the so-called "prime bank" fraud; they may sound great on paper, but the guaranteed offshore investment with the vague claims of an easy 100% monthly return simply does not exist... these are all fictitious financial instruments and your money is gone forever.

The fictitious 'bank inspector'

This is an old scam with a number of variants; the original scheme involved claiming to be a bank inspector, claiming that the bank suspects that one of its employees is stealing money and that to help catch the culprit the "bank inspector" needs the depositor to withdraw all of his or her money. At this point, the victim would be carrying a large amount of cash and can be targeted for the theft of these funds.

Other variants included claiming to be a prospective business partner with "the opportunity of a lifetime" then asking for access to cash "to prove that you trust me" or even claiming to be a new immigrant who carries all their money in cash for fear that the banks will steal it from them - if told by others that they keep their money in banks, they then ask the depositor to withdraw it to prove the bank hasn't stolen it.

Impersonation of officials has more recently become a way of stealing personal information for use in theft of identity frauds.

Phishing and Internet fraud

Phishing operates by sending forged e-mail, impersonating an online bank, auction or payment site; the e-mail directs the user to a forged web site which is designed to look like the login to the legitimate site but which claims that the user must update personal info. The information thus stolen is then used in other frauds, such as theft of identity or online auction fraud.

A number of malicious "Trojan horse" programmes have also been used to snoop on Internet users while online, capturing keystrokes or confidential data in order to send it to outside sites.

Money laundering

The term "money laundering" dates back to the days of Al Capone; Money laundering has since been used to describe any scheme by which the true origin of funds is hidden or concealed.

The operations work in various forms. One variant involved buying securities (stocks and bonds) for cash; the securities were then placed for safe deposit in one bank and a claim on those assets used as collateral for a loan at another bank. The borrower would then default on the loan.

But what of the securities themselves? Perfectly good and worth the full amount.

The transaction accomplished nothing except to disguise the original source of the funds.

Approach to avoid bank frauds

All the major operational areas in banking represent a good opportunity for fraudsters with growing incidence being reported under deposit, loan and inter-branch accounting transactions, including remittances.

A broad analysis of various frauds that have taken place throw up the following high-risk areas in committing frauds:

- Misappropriation of cash by fudging accounts.
- Unauthorized withdrawal or transfers of funds, mostly from long dormant accounts.
- Opening of fictitious accounts to misappropriate funds from illegal activities ie. Laundering through the fictitious accounts
- Use of interbank clearing for accommodation, kite-flying and misappropriation.
- Cheating in foreign exchange transactions by flouting exchange control provisions.
- Withdrawal from deposit accounts through forged documents.

Fraud in collusion with bank staff in emerging areas and services under the computerized environment. Frauds take place in a financial system only when safeguards and procedural checks are inadequate or when they are not scrupulously adhered to, leaving the system vulnerable to the perpetrators. Anecdotal evidence shows that whether the agency or individual committing the fraud works for the bank or deals with it, careful planning is done by the culprit before he attacks the system at its most vulnerable point.

The most effective defence banks could have against fraud is to strengthen their operational practices, procedures, controls and review systems so that all fraud-prone areas are fully sanitised against internal or external breaches. However, the huge expansion in banking transactions consequent to the transition of banks to mass banking and the large scale computerization have played a major role in the perpetration of the frauds.Hence mere reliance on the internal controls is of no use. The ten fold "*INDIA FORENSIC*" approach to tackle the bank fraud will definitely play a crucial role in coming days.

Expect fraud: Nowhere in the world the fraud can be avoided hence the banks can be no exceptions. It is a human tendency of taking the risk to commit the frauds if he finds suitable opportunities. So it is wise to expect the occurrence of the fraud. If the fraud is expected, efforts can be concentrated on the areas, which are fraud prone. Fraud is the game of two. The rule makers and rule breakers. Whoever is strong in the anticipation of the situations wins the game of frauds. Fraud is a phenomenon, which cannot be eliminated, but it needs to be managed.

Develop a fraud policy . The policy should be written and distributed to all employees, Borrowers and depositors. This gives a moral tension to the potential Fraudster. Maintain a zero tolerance for violations. The Indian bank needs to roar against the action that is taken against the Fraudsters. The media publicity against the fraudsters at all the levels is necessary. The announcement by US president George W. Bush that the "Corporate crooks will not be spared" gave the deep impact to the Corporate America. In India also we need to consider it as a sever problem and need to fight against it.

Assess Risk . Look at the ways fraud can happen in the organization. It is very important to study the trend and the style of frauds in the bank. Some of the big nationalized banks maintain the databases of the fraud cases reported in their banks. But the databases are dumb. They yield nothing unless they are analyzed effectively. Establish regular fraud-detection procedures. It could be in the form of Internal audit or it could also be in the form of inspections. These procedures alone discourage employees from committing fraud. In addition to this the Institute of Chartered Accountants of India has issued a "Accounting and Assurance standard on internal controls which is a real guideline to test internal controls . Controls break down because people affect them, and because circumstances change.

Segregate duties in critical areas . It is the absolutely basic principle of auditing a single person should not have the control of the books of accounts and the physical asset. Because this is the scenario which tempts the employee to commit the fraud. Hence it becomes essential to see that no one employee should be able to initiate and complete a critical transaction without involving someone else.

Most of the banks in India have the well-defined authorization procedures. The allocation of the sanctioning limits is also observed in most of the cases. But still the bankers violate the authorities very easily. They just need to collude with the outside parties. However the detection of the collusions is possible in most of the cases if the higher authorities are willing to dig the frauds.

Maintain the tone of Ethics at the top. The subordinates have the tendency to follow their superiors. When the signals are passed on to the middle management about the unethical behavior of the top management the fear of punishment gets reduced and the tendency of following the superior dominates. Fear vanishes when the tendency of "If I have to die I'll take along the superior and die" tendency rises.

Review and enforce password security . The incidences of hacking and the Phishing have troubled the Indian Private sector banks to a great extent. In addition to this most of the Indian banks are running behind the ATM and credit cards to compete with each other but have conveniently forgone the fact that ATM cards and the credit cards are the best tools available in the hands of the fraudsters. Inappropriate system access makes it possible to steal large amounts

of money very quickly and, in many cases, without detection. Hence the review and the enforcement of the security policy is going to be a crucial.

Promote the Whistle blowing Culture: Many of the surveys on Frauds have shown that the frauds are unearthed by the "TIPS" from insider or may be from outsiders. Internal audits and internal controls come much later. The message about contacting the vigilance officers is flashed in most of the branch premises. However the ethics lines are very rarely seen. The ethics lines are the help lines to the employees or the well-wishers of the bank which tells them whether a particular activity constitutes a fraud or not.

Conduct pre-employment screening: Since the raw material of the Banks is cash the banker needs to be more alert than any other employer before they recruit. Only testing the aptitude of a person is not of any use. Know whom you are hiring. More than 20 percent of resumes contain false statements. Most employers will only confirm dates of employment. Some times post employment condition might create the greed in the minds of employee,hence atleast the bankers should test check the characters of their subordinates by creating real life scenarios such as offering the bribes by calling on some dummy borrower.

Screen and monitor Borrowers: Bad borrowers cause the biggest losses to the banks. What are they ? Who they represent themselves to be? Look at their ownership, clients, references, and litigation history. In many cases the potential fraudsters have history of defaulting in some other bank or Financial Institution.

Though this is not the foolproof solution to the disease of the frauds to some extent it helps to combat the frauds.

****

Computer Crime and Computer Forensics

Investigative Techniques

Computer Power

Computer is a powerful tool in a limitless cyberspace. Power of one computer is the power of *'all connected computers'*.

Cyberspace is a new space with new risks. It is a Virtual Medium.

It has its own dark corners and alleys visited by Cyber Criminals.

Cyber Crime & Importance of Computer- Cyber crimes originate from the abuse of computer.

- The law has been able to recognize the computer as tool in criminal activity.
- A computer could be referred to as a 'weapon of offence' as well as a 'victim of crime'.

Advantages of Being a Cyber Criminal

- Complete Anonymity
- No Immediate Physical Risk
- Prevention Expensive and Uncertain
- Lag Between Action and Detection
- The Tools of Offence are Legitimate**Starting point of a Cyber Crime**
- Unauthorized access to computer programmes or data
- Unauthorized access with a further criminal intent
- Unauthorized modification of computer material

Establishing the Nature of the Offence

that the computer performed a function as a consequence of seeking or gaining access

•that the access was unauthorized

•that the person concerned knew that the access was unauthorized

•that the access was a preliminary to the commission or facilitation of a further serious offence

•that the intention behind the modification was to impair the operation of the computer in some way.

Investigation of Cyber Crimes:

Computer Forensics & Its Tools

Cyber Crime & Importance of Computer- Cyber crimes originate from the abuse of computer.

- The law has been able to recognize the computer as tool in criminal activity.
- A computer could be referred to as a 'weapon of offence' as well as a 'victim of crime'.

Advantages of Being a Cyber Criminal

- Complete Anonymity
- No Immediate Physical Risk
- Prevention Expensive and Uncertain
- Lag Between Action and Detection

- The Tools of Offence are Legitimate

Starting point of a Cyber Crime

- Unauthorized access to computer programmes or data
- Unauthorized access with a further criminal intent
- Unauthorized modification of computer material

Establishing the Nature of the Offence

•that the computer performed a function as a consequence of seeking or gaining access
•that the access was unauthorized
•that the person concerned knew that the access was unauthorized
•that the access was a preliminary to the commission or facilitation of a further serious offence
•that the intention behind the modification was to impair the operation of the computer in some way.

Classification of Cyber Crimes

Cyber crimes could be categorized as :
•Data-related theft and interception
•Network intrusion and sabotage
•Hacking and virus distribution
•Fraud, forgery and
•obscenity, breach of privacy etc.

Classification of Cyber Offences **contd.**

S. 65	Tampering with computer source documents Cognizable, Non-bailable
S. 66	Hacking with computer system Cognizable, Non-bailable
S. 67	Publishing of obscene information in electronic form Cognizable, Non-bailable
S. 70	Protected System Cognizable, Non-bailable

Power to Investigate Offences **(S.78)**

Notwithstanding anything contained in the Code of Criminal Procedure, a police officer not below the rank of DSP shall investigate any offence under this Act.

Power of police officers and other officers to enter, search, etc.

Any police officer, not below the rank of a DSP or any other officer of the Central Govt. or a State Govt. authorised by the Central Govt. in this behalf may enter any **public place** ***and search and arrest without warrant any person found therein who is reasonably***

under this Act. [S.80(1)]

Explanation. *For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.*

Computer Forensics

The Department of Justice (DoJ) of U.S. defines computer forensics as the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media.

It also includes the formalized and approved methodology to collect, analyze and present data in a court of law.

Computer forensics is all about `forensic processes`. It includes:

(a) Collection
(b) Preservation
(c) Examination and
(d) Analysis

of information (evidence) in an electronic form.

a. Collection of Evidence

It involves the search for, recognition, and collection of electronic information (evidence).

It requires precision and expertise. Any misstep and the crucial evidence is lost forever.

b. Preservation of Evidence

It primarily deals with storing the `collectables` in a storage media.

It requires knowledge and skills in preserving the `collectables` in a proper storage media with back ups.

c. Examination of Evidence

It helps to make the evidence visible and explain its origin and significance.

It is pain staking process, whereby an examiner `unlocks` both visible and invisible information.

d. Analysis of Evidence

It is more like an investigation process, where, a holistic view of `captured evidence` is taken into account.

The investigator recreates a scene of crime, by drawing inferences from the pieces of `electronic puzzle` presented to him.

Required Capabilities

- Data Protection
- Data Acquisition
- Imaging
- Extraction
- Interrogation
- Ingestion/Normalization
- Analysis
- Reporting**Data Protection**

Identifying the digital information source and protecting the said information from being destroyed or becoming unavailable.

Data Acquisition

Involves practice of transferring data from out of physical or administrative control of the investigator into a controlled location.

Imaging

The creation of a bit-for-bit copy of seized data for the purposes of providing an indelible facsimile upon which multiple analysis may be performed, without corrupting the original data sheet.

Extraction

The identification and separating of potentially useful data from imaged data set. This encompasses the recovery of damaged, corrupted, or destroyed data or data that has been manipulated algorithmically to prevent its detection.

Interrogation

The querying of extracted data to determine if a priori indicators or relationships exist in the data.Examples, include looking for known telephone numbers, IP Addresses and names of individuals.

Ingestion/Normalization

The storage and transfer of extracted data in a format or nomenclature that is easily or commonly understood by investigators. This includes the conversion of hexadecimal or binary information into readable characters etc.

Analysis

The fusion, correlation, graphing, mapping, or timelining of data to determine possible relationships within the data, and to develop investigative hypothesis**Reporting**

The presentation of analyzed data in a persuasive and evident form to a investigating authorities.

Presenting e-Evidence

It is obligatory to note that the evidence in electronic form is in 'intangible form' and the bottom line is – admissibility of such evidence in a court of law.**Analysis Tools**

EnCase Forensic Edition by Guidance Software

(Windows, Mac OS, Linux, Solaris etc)

•Can analyse computer media, HDD, Zip drive, USB device

•Create binary duplicate of original media

•Image is verified using MD-5

•DataLifter

•Disk2File

•LC-Tech – forensics tools developed to recover lost and deleted data

•SafeBack – Evidence Preservation Tool – Image backp

Evidence Capturing – Software

EnCase (www.guidancesoftware.com), SafeBack, SilentRunner, SnapBack, ByteBack, WinHex

Evidence Capturing – Hardware

ImageMaster Solo 2 – Hardware duplicator, Solitare, Forensic Steel Towers, Forensic AirLite

Important Certifications...

•www.cert.org

••www.giac.org

••www.cops.org

IACIS – International Association of Computer Investigative Specialists
www.Foundstone.com

Investigation of Cyber Crimes

Typically, an individual uses his computer to connect to Internet via an Internet Service Provider (ISP) by using either a dial-up connection or a leased line / broadband facility. There are two levels at which evidence of Internet usage exists:

I. Individual Level

(i) on an individual's own computer, computer system or computer network,

(ii) on the websites accessed by the individual using his own computer, computer system or computer network.

II. ISP Level

On the servers of individual's ISP.

Collecting Evidence @ Individual's Level

Computers usually store text, graphic, image files, emails messages etc. in the hard disk during its routine use.

User may keep on deleting the unwanted material regularly to free up disk space. Similarly, Chat rooms, Internet Relay Chat (IRC), Internet telephony sessions are real-time discussions happening on the Internet; it is optional for the user to maintain logging files of these sessions.

It is possible to determine what the user of a specific computer has been actually viewing / browsing; it may further give the date-and-time of viewing / browsing.

Collecting Evidence @ ISP Level

Logs maintained by the users using dial up connections to connect to ISP indicate the time and duration on Internet usage / connectivity.

It will corroborate other types of evidence that has already been gathered during investigation. Admissibility of such an evidence can not be questioned as it clearly highlights not only the time and duration of computer's Internet usage / connectivity, but also the fact that during a specific time period, the user's computer had been working as a sort of 'computer network'.

Problems with Preserving Computer Evidence

- *Some of the facilities within the browsers to save WWW pages to the disk are imperfect- as it may save the text but not the associated images.*

(b) In case of some very complex pages, involving "frames" and "templates", there could be perceptible difference in what is seen on screen and what is saved on the disk.

(c) It is difficult to tell when a specific page was last acquired, thanks to browser cache facility.

Thus if one examines a whole series of cached pages, it is not easy to pinpoint which page came first and which later.

Problems with Preserving Computer Evidence

(d) It should not be forgotten that many ISPs use proxy servers to speed up the delivery of popular pages. Thus a user of such an ISP may not be sure that what he has received on his computer is the latest version from the source computer (website) as opposed to an earlier cached version held by his ISP.

Common Computer Forensic Techniques

An understanding of common computer forensic techniques will go a long way to obtain and preserve - authentic, accurate and complete evidence:

- *Carrying out a pre-raid intelligence review to assess what types of hardware, software and back-ups might be expected.*

(ii) Photographing (video) the computer(s) **in situ**, *particularly any cabling of peripherals and ancillaries,*

Common Computer Forensic Techniques cont..

(iii) Every computer and its input and output devices carry a product number, it is thus advisable that these numbers be duly recorded

(iv) Careful identification and labeling of all items, including cables, peripherals, external data storage medium, like CDs, disks and tapes

(v)Precautions to prevent the data being destroyed by hostile individuals immediately prior to the raid,

Common Computer Forensic Techniques cont..

(vi) Proper handling of computers that are running, at the time of the raid,

(vii) Following proper procedures for safe shutting down,

(ix) Noting of the time on the computer's internal clock which provides date and time stamps on computer files

(x) Making of an exact sector-by-sector copy of every hard disk*

Common Computer Forensic Techniques cont..

The method consists of starting (or "booting") the computer not from the hard disk but through a floppy (Drive: A).

The operating system will make an "image" of the hard disk on the external device. The image is an exact copy, also referred as 'bit copy' or 'sector-by-sector copy' of the original.

It includes not only the visible files on the original hard disk but other which would not be seen, the parts of the disk that contain the information from which the directory details are obtained (file names, sizes, date and time stamp) and also certain other forensic segments from previously deleted files can sometimes be recovered.

****

Credit card fraud

(From Wikipedia, the free encyclopedia)

Credit card fraud is a kind of fraud where a merchant (business, service provider, seller, etc.) is "tricked" into releasing merchandise or rendering services, believing that a credit card account will provide payment for goods/services. The merchant later learns that they will not be paid, or the payment they received will be reclaimed by the card's issuing bank.

Typically, the fraudster causes a credit card of another person to be charged for a purchase. Today, half of all credit card fraud is conducted online, meaning that the fraudsters make online purchases with the credit card details of other people.

Types of Fraud

Stolen Card Fraud

When a card holder loses or has their credit card stolen, it is possible for the thief to make unauthorized purchases on that card up until the card is cancelled. Businesses that accept credit cards are not permitted to request supplemental ID from the cardholder, unless the credit card is not signed. A thief can potentially purchase thousands of dollars in merchandise or services before the card holder or the bank realize that the card is in the wrong hands. Self-serve payment systems such as gas stations are also highly prone to accepting a stolen credit card, as there is no verification of the card holder's identity, however many stations are trying to prevent this by adding a check requiring the user to key in a zip code. The zip code must match the code registered to the credit card or the transfer will fail.

Account Takeover Fraud

Fraud perpetrators call in and impersonate actual cardholders using stolen personal information. They have the address and other information of the cardholder changed to an address they control. Additional cards and possibly PIN mailers are requested and issued to the new address and used by the fraudsters to make purchases and/or obtain cash advances.

Sometimes the fraudster will attempt to add themselves or an alias that they control as an authorized user to the account in order to make it easier to commit the fraud.

Credit Card Mail Order Fraud

Using a stolen credit card number, or computer generated card number, a thief will order stolen goods.

Skimming

Skimming is the theft of credit card information by a dishonest employee of a legitimate merchant, manually copying down numbers, or using a magnetic stripe reader on a pocket-sized electronic device. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The skimmer will typically use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip.

Many instances of skimming have been reported where the perpetrator has put a device over the card slot of a public cash machine (Automated teller machine), which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pin-hole camera to read the user's pin number at the same time.

Cards in countries such as the UK are issued featuring a smart chip with public key encryption. The chip cannot be copied, but the card number, expiry date and security code can be, and this set of data is often sufficient to use the victim's credit card account for fraudulent purposes with so-called "card not present" transactions, e.g., manual input, over the telephone or internet.

Carding

Carding is a term used by fraudsters for a process they use to verify that sets of stolen credit card data are still valid. The fraudster will present each set of credit card details in turn on a website that has real-time transaction processing, making a purchase for a very small monetary amount so as not to use up the card's credit limit, and so as not to attract the attention of a human reviewer to the transaction.

Often, an online donation site for a charity is used instead of an eCommerce merchant, since there is no need to find an item of a suitable price to put in the virtual shopping cart, nor to supply shipping details. The carder may do this manually with a web browser, or may write automated software to interface to the website's checkout or billing forms.

In the past, carders used to use computer programs called "generators" to produce a sequence of credit card numbers, and then test them to see which were valid accounts. However, this process is no longer viable due to widespread requirement by internet credit card processing systems for additional data such as the billing address, the 3 to 4 digit Card Security Code and/or the card's expiry date. Nowadays, carding is more typically used to verify credit card data obtained directly from the victims by Skimming or Phishing.

A set of credit card details that has been verified in this way is known in fraud circles as a phish (see Phishing). A carder will typically sell data files of phish to other individuals who will carry out the actual fraud. Market price for a phish ranges from US$1.00 to US$50.00 depending on the type of card, freshness of the data and credit status of the victim.

Credit Card Crime Profits, Losses & Punishment

Losses

U.S. Federal Law can hold the cardholder victim responsible for up to $50. Merchants in high-risk industries, like unattended automated fuel pumps or Internet sales, anticipate a certain amount of credit card fraud, and set prices accordingly. These higher costs are then passed onto the customer.

Credit Card Companies

In 2003 the Wall Street Journal estimated that the credit card industry generated $500,000,000 in annual revenue in research and investigation fees paid by consumers and businesses. This additional revenue offsets some of the costs incurred by credit card issuing and processing companies' when investigating chargeback claims. Some merchants believe the high revenue generation by the banks from the crime victims, reduce the incentive for the credit card banks to implement procedures to reduce credit card crime. However, the companies which collect these fees are not capable of dictating fraud prevention policies to the rest of the world. Payment transfer associations, like Visa and Mastercard, receive profit from transaction fees calculated as a percentage of the amount of money they transfer. These associations are motivated to enact policies which increase the amount of money transferred by their systems. Credit card fraud has a chilling effect on merchant acceptance of credit cards, motivating merchants to not accept credit card payments to mitigate their risk of loss. These payment transfer associations are therefore motivated to enact policies and enforce regulations which reduce credit card fraud.

Merchants have begun to request changes in State and Federal Laws to protect consumers and merchants from fraud, but the credit card industry has opposed many of the requested laws.

Because all card-accepting merchants and card-carrying customers are bound by contract law, according to the agreements they sign with their processing / issuing banks, respectively, State and Federal law has a smaller role in preventing merchants from being tricked. Payment transfer associations enact regulatory changes, and issuing / acquiring banks, merchants, and cardholders are contractually bound to these new regulations.

The Criminals

In the US, persons that commit credit card crime largely go unpunished and repeatedly victimize consumers and businesses. The Secret Service handles crimes involving the US money supply, they have a limit of $2,000 before investigating each crime. Most credit card criminals know this and keep purchases from any one business below $2,000. With credit card crime occurring across state lines, criminals often are never prosecuted because the

dollar amounts are too low for local law enforcement to pay for extradition.

Reporting Credit Card Fraud

If you lose or have had your credit card stolen, you should immediately report it to your card issuer. Once you report the incident, you are no longer responsible for unauthorized charges made on your card.

In the US, credit card fraud can be reported to the Federal Trade Commission (FTC) and to local and regional authorities. It is the standing policy of the FTC not to investigate reports where the value of fraud does not exceed $2000. Local law enforcement may or may not further investigate a credit card fraud, depending on the amount, type of fraud, and where the fraud originated from.

Tips to help you avoid credit card fraud

- Don't carry credit cards you don't use and never leave them unattended in a purse, briefcase or wallet.
- Always make sure you get your credit card receipt because it just may include your credit card number. Never toss it in a public trash bin. You'll need that receipt later anyway to tally things up when your statement arrives.
- Shred all documents that might include your credit card number before disposing of them - old slips, credit card statements, bills, anything.
- Never give your number over the phone to someone that you do not know. It's OK if you initiate the call but if you get a call at home from anyone that you do not know by name do not give them your credit card number.
- Never respond to an e-mail asking for your number, no matter how official or legitimate it looks. These bogus e-mails are the #1 fraud right now on the Internet.
- Review your monthly statement as soon as it comes and report any problems right away. To insure your rights, follow-up by filing a written complaint form.
- If using a bank card where you have the option to use credit or debit, ALWAYS USE THE CREDIT OPTION as this may prevent the skimmer device from accessing your four digit pin number.

****

Occupational Frauds and Money Laundering

Mayur S. Joshi

Billing Scheme

The most fundamental scheme of an overstated expense occurs when an employee doctors an invoice or other supporting documentation to reflect a higher cost than what he actually paid. The employee may use whiteout, a ballpoint pen, or some other method to change the price reflected on the receipt, before submitting his expense report.

If the company does not require original documents as support, the perpetrator generally attaches a copy of the receipt to his expense report. Alterations are usually less noticeable on a photocopy than on an original document. For precisely this reason, business should require original receipts and ink signatures on expense reports. As with other expense frauds, overstated expense schemes often succeed because of poor controls.

In companies where supporting documents are not required, for example, fraudsters simply lie about how much they paid for a business expense. With no support available, it may be very difficult to disprove an employee's false expense claims

Case Study

The Maharashtra government employee was on Tamilnadu tour for 6 days. He had taken a huge sum as an advance from his employer. In reality his expenses were very much lesser than the total advance. He was allowed the lodging and boarding expenses. He adopted a simple method to siphon out the advance. He purchased tea worth Rs.5 and get the bill written in Tamil language. Tamil, telgu, malyalam and Kannad are the languages, which are not easily understood by the people residing in rest of India and so the accountant and cashier of the employer company. He collected some bills, which were written in the tamil characters and simply added a small digit-2. The bill of five became worth of Rs.25.In this fashion he inflated his bills to utilize the total advance

Negotiable Instruments Alteration

It is a general practice among the paper crashers to buy a small amount Draft or the Pay order from the bank. The initial buying becomes essential to know who is the authorized signatory. The banks clearing the draft reconcile the signature. Hence the signed draft or the pay order is obtained and scanned.

The amounts and the names of the payees are altered subsequently using the software tools.

What requires is simply the printout. However it is not sufficient enough to scan and alter the drafts. The banks also send the draft sold advices. These advices are very difficult to be obtained by the outsiders, which makes the forgery task a bit difficult.But to reiterate what Kautilya said "It is just as difficult to detect an appointed official's dishonesty,As it is to detect how much water the swimming fish drinks".

Case study

In the case of Mr.A.K.Shah, ingenious facts came out from the exposed fraud. Mr. A.K.Shah was the manager of the Pethapur Branch in Ahemdabad.He played rather simple technique to receive the proceeds of the draft. Just before he was transferred from Pethapur to another local branch, he stole the draft and draft sold advices book. With these weapons he forayed into the share market. He made exorbitant purchases of equity shares and very soon also booked the losses. Anyways he was not the loser. Whenever he incurred the losses he issued the demand draft. The draft issuing branch was not aware of the theft and the paying bank never had the doubt since the branch always received the draft sold advice beforehand and the signature on the draft tallied with the signature in the specimen signature book. In this fashion approximately 96 drafts worth Rs.88 lacs were issued to the brokers for compensating the losses. But looking at the serial numbers on the drafts the share broker in Mumbai had some doubts. He received all the drafts from the same Draft book. The CBI exposed the scam and the perpetrator was behind the bars. No forgery, No counterfeit still a big fraud.

Computer print-outs can be admitted as documentary evidence

In an unprecedented ruling, a TADA court at Mumbai has held that computer printouts can be admitted as documentary evidence. The ruling was delivered on 6.7.2000 by the Judge Shri Pramod Kode before whom the CBI examined an official of the Mahanagar Telephone Limited (MTNL), to corroborate its charges against film star Sanjay Dutt of having made an international call from his residence to Dubai - based Aneesh Ibrahim, brother of Dawood Ibrahim.

During the examination of the witness, computer print-outs containing the called numbers were produced as exhibits. These print-outs were taken from magnetic tapes on which the Bandra Telephone Exchange had recorded outgoing and incoming calls, to places within and outside India in the year 1993 . The investigating officer had collected only the print-outs and not the magnetic tapes. The tapes were preserved for a period of three years by MTNL and later destroyed following the usual practice.

The prosecution contended, that the computer print-out was primary evidence within the meaning of section 62 of the Indian Evidence Act, as print-outs were made by a uniform process and, therefore, deserved to be exhibited. These were the result of records contained in the magnetic tape automatically made at the exchanges regarding respective calls made or received. Such print-outs were not copies of the matters recorded on the magnetic tape and could, therefore, be exhibited. The defence argued that the print-outs produced in the court

were not original print-outs taken for the purpose of making bills. The primary evidence related to the alleged telephone call was the magnetic tape which had not been produced before the court. The defence also pleaded that the investigating agency had failed to collect the magnetic tape, and therefore, no case was made out under section 63 to permit secondary evidence. Hence, the document cannot be marked as exhibit.

The court observed that the print-outs are not a copy of the magnetic tape because the tape by itself cannot be termed as a document. It does not fall within the definition of a document under section 3 of Indian Evidence Act. Evidence is something which can be perceived by the human senses. Matter, which cannot be perceived by the human senses by a Judge cannot fall within the definition of the word 'document' or the word 'evidence'. Even if the magnetic tape had been produced before the court, the court would have been unable to directly perceive i.e. to read, hear or see the matter stored on it and consequently, would have been unable to act upon the said matter. The print-outs, on the other hand constitute the direct evidence of the matter. They were taken by technicians from the computer in the presence of the witness and after satisfying that at the relevant time the computer was properly working. It was therefore, ruled that the print-outs were primary evidence.

Source: http://cbi.nic.in