

Lab Systems services to Banks

A large part of the banking operations deal with sensitive individualized information which include personal customer information; information about specific transactions and in some cases the decisions of the bank's executives on investments and trades in security markets.

Leakages of such information can result in financial loss to the bank and also the risk of reputation loss and legal suits and regulatory issues.

Lab Systems' professional services can enable banks to detect such discrepancies and thus prevent any major data and information loss to the bank.

Using e-discovery computer forensics methodologies can help banks to adhere to regulators' frequent requests for older records and also to establish and verify them as being true and authentic. These records and archives are also important in fighting important legal disputes and, in case of a warranting situation, Lab Systems' experts can also testify in courts of law about the authenticity of cases involving e-discovery forensic methodologies.

Today, many public sector banks have computerized branches, but in spite of computerization, neither banks nor the customers have benefited, as expected.

Mentioned below are some case-studies that will enumerate how cyber scam occurs;

Mail Spoofing – E-Mail Forgery:

Kola Mohan's Case:

This was the first cyber crime case in Andhra Pradesh.

Kola Mohan, the perpetrator, was able to convince several gullible money lenders, top banks and the state's ruling Telugu Desam Party that he had won the euro lottery and was awaiting the completion of a few formalities before the money would be transferred to his account in India. He set the ball rolling in November 1998, just a few months after he actually picked up a euro lottery ticket in London, when a prominent Telugu daily received an e-mail (sent by Kola Mohan himself) saying that a Telugu man had won the multi-million dollar euro lottery but no one had taken notice of this great achievement.

The newspaper promptly published a report and followed it up with an interview without making any attempt to contact any euro lottery representative. Other newspapers soon picked up the story and Kola Mohan became a celebrity overnight.

Following this, he began calling up money lenders seeking short-term loans citing the excuse of payback as soon his *"money arrived from London where it was deposited in a bank."*

Kola Mohan's scammed dream run continued till creditors began putting pressure on him. By October 1999, word began to get out that his claims about his euro lottery win were untrue.

Cause of the above fraud:

1. Source Address Authenticity never verified:

The e-mail system was developed trying to imitate the postal mail and just like in postal mail, the "From Address" authenticity was never verified.

Though the new upgraded mail systems have that capacity, no one can actually stop any one from setting up a mail server to send fraudulent mail posing as an authentic source.

2. Reply can be sent to a different mail address as preferred by the sender instead of the Source Address:

Another major flaw in the e-mail system is that the sender can always set on which e-mail address to get the reply to his mail; i.e. the forger can send a mail with the forged source e-mail address and can set its reply address as his own e-mail address, so that the replies reach his actual e-mail address instead of the forged e-mail address.

Due to the above flaws, a forger can easily pose as any well-known personality, without the knowledge of that individual. The receiver always thinks that the mails were from the said address, and his replies go actually to the forger than to the real person.

In a similar fashion, even bank sites can be forged. The customers of the bank can be lured to log on to fake web site, which exactly looks and behaves as the original, at least till it captures the customers' username and password. Such forged web site owners, pose as the real customers of the bank and log on to the real site and do transactions with the already captured username and password.

The negative aspect of the whole issue is that the customers do not have any means of proving that it was not they who did those transactions, but someone unknown anonymous. This kind of fraud has been increasing lately to steal username, passwords and credit card information and other personal and valuable data.

Fraudsters can cheat even after deploying PKI

Even after employing all safety measures and efforts like PKI, fraudsters can still cheat the users, due to the following loopholes:

The browsers alert the user, only if they don't find the CA certificate that issued the digital certificate to the server/publisher. However, it still allows the user to go ahead with further communication. Anyone can set up a CA and issue digital certificate to them and make the browsers trust them.

Fraud by Insiders

Rogue traders:

A rogue trader is a highly placed insider nominally authorized to invest sizeable funds on behalf of the bank. This trader secretly makes progressively more aggressive and risky investments using the bank's money and if one investment happens to go bad, the rogue trader engages in further market speculation in the hope of a quick profit which would hide or cover the loss. It's more like window dressing in simple terms.

Unfortunately, when one investment loss is piled onto another, the costs to the bank can reach into the hundreds of millions of rupees and in recent times, there have even been several cases wherein a bank has gone out of business due to continuous and repeated piled-up market investment losses.

Wire fraud:

Wire transfer networks such as the international, interbank fund transfer system are tempting 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.

Demand draft fraud:

DD fraud is usually done by one or more dishonest bank employees also known as the Bunko Bankers. 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.

Fraud by Others

Forgery and altered checks:

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

Stolen checks:

Some fraudsters obtain access to facilities handling large amounts of checks, such as a mailroom or post office or the offices of a tax authority (receiving many checks) or a corporate payroll or a social or veterans' benefit office (issuing many checks). A few checks go missing; accounts are then opened under assumed names and the checks (often tampered or altered in some way) deposited so that the money can then be withdrawn by thieves. Stolen blank check books 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.

Banks have employed E Discovery techniques offered by Lab Systems to obtain the actual Books of Accounts; P & L statement & Balance Sheet which have revealed the Real Truth of such Companies and summarily rejected these Loan requests.

Bill discounting fraud:

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 certain 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.

Check kiting:

Check Kiting exploits a system in which, when a check is deposited to a bank account, the money is made available immediately even though it is not removed from the account on which the check is drawn until the check actually clears. Deposit 1000 in one bank, write a check on that amount and deposit it to your account in another bank; you now have 2000 until the check clears. In-transit or non-existent cash is briefly recorded in multiple accounts.

A check is cashed and, before the bank receives any money by clearing the check, the money is deposited into some other account or withdrawn by writing more checks. In many cases, the original deposited check turns out to be a forged check. Some perpetrators have swapped checks between various banks on a daily basis, using each to cover the shortfall for a previous check.

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.

Credit card fraud:

Credit card fraud is widespread as a means of stealing from banks, merchants and clients. A credit card is made of three plastic sheet of polyvinyl chloride. The central sheet of the card is known as the core stock. These cards are of a particular size and many data are embossed over it. But credit cards fraud manifest in a number of ways. They are: Genuine cards being manipulated genuine cards being altered Counterfeit cards being created Fraudulent telemarketing is done and consumer's credit card details are misused. Genuine cards are obtained on fraudulent applications in the names/addresses of other persons and used.

It is feared that with the expansion of e-commerce, m-commerce and internet facilities being available on massive scale the fraudulent fund freaking via credit cards will increase tremendously. Counterfeit credit cards are known as white plastics.

Booster checks:

A booster check is a fraudulent or bad check 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 check is credited to the card account by the bank as soon as the payment is made, even though the check has not yet cleared. Before the bad check 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 check 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.

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.

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*" programs 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 involves buying securities (stocks and bonds) for cash; the securities are 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 then defaults on the loan. The securities, however, are still worth their full amount. The transaction serves only to disguise the original source of the funds. It's as simple as black money becoming white.

Even though bank computer crimes have a typical feature, the evidence relating to crime is intangible. The evidences can be easily erased, tampered or secreted. More over it is not easily detectable as the evidence connecting the criminal with the crime is often not available.

Computer crimes are different from the usual crimes mainly because of the mode of investigation. There are no eyewitness, no usual evidentiary clues and no documentary evidences.

Modus operandi:

The method of alterations of checks, drafts, receipts and other fiduciary documents are comparatively simple both manually and with the help of technology. The following example will help simplify things.

A classic case is the recent loan racket busted by the Uppal police in State Bank of India (SBI)'s Chikkadpally branch. The modus operandi involved a gang of four members approaching the owner of a newly-constructed apartment building saying they were interested in buying flats.

The gang took photo copies of the building documents after entering into an oral agreement of sale with the builder by paying Rs. 2 lacs as advance. Later, they created forged documents in the name of building's owner establishing that the latter had sold five flats to five defense employees.

Incidentally, the salary slips and other documents submitted by the loan seekers were found to be genuine. *"This was made possible because the gang paid money to the defense employees to utilize their documents,"* says an investigator. The gang hired an impostor who executed the sale deed posing as the original building owner.

"We could not establish criminal negligence on the part of the bank manager and hence he was not arrested," say detectives. The police later learnt that the main lapse in the system is that the banks never asked for the original documents at any stage except for the sale deed for execution of which the offenders planted an impostor.

Bank rules:

After receiving photo copies of the documents (which were actually forged by the offenders) of the property, the bank passed the same on to the legal section. After scrutiny, the legal consultant told the bank that the photo copied documents were 'perfect' and to release loan after execution of sale deed.

The bank rules state that loan applications can be examined even with photocopies of documents. The alleged greediness of employees to give their salary slips and other documents on payment of some money made the job of the cheats easier.

This is not an isolated case. With a similar modus operandi, a gang cheated three banks to the tune of Rs. 1 Crore in Saroornagar police station area. The police opine that unless bankers evolve a foolproof system, the offenders continue to take advantage of the lapses.

A Better Alternative:

Though computer based banking crimes are yet limited but it is increasing with a huge pace. Their investigation is highly intricate and daunting. Prevention might be a solution but in terms of cost utilization, adopting preventive measures might prove a bit heavy on the purse strings of the bank.

A better solution would be the constant use of cyber forensic methodologies like e-discovery services to keep in tandem with the highly developing world of cyber financial development. Cost efficient yet highly effective, it will enable to revolutionize and elevate the standards of successfully nabbing the criminals and thus restoring the faith placed in the authorized financial institutions.