RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF JURIDICAL SCIENCES

COURSE NAME : BALLB/BBALLB

SEMESTER : VIIIth

SUBJECT : Banking law

SUBJECT CODE: BAL -802/BBL-802

LECTURE : 24

FACULTY NAME: Mr JP Srivastava

Bank fraud prone areas in different accounts – Saving Bank Accounts, Current Accounts

Fraud is any dishonest act and behaviour by which one person gains or intends to gain advantage over another person. Fraud causes loss to the victim directly or indirectly. Fraud has not been described or discussed clearly in The Indian Penal Code but sections dealing with cheating. concealment, forgery counterfeiting and breach of trust has been discusses which leads to the act of fraud.

In Contractual term as described in the Indian Contract Act, Sec 17 suggests that a fraud means and includes any of the acts by a party to a contract or with his connivance or by his agents with the intention to deceive another party or his agent or to induce him to enter in to a contract.

Banking Frauds constitute a considerable percentage of white-collar offences being probed by the police. Unlike ordinary thefts and robberies, the amount misappropriated in these crimes runs into lakhs and crores of rupees. Bank fraud is a federal 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.

The number of bank frauds in India is substantial. It in increasing with the passage of time. 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.
Bank fraud is a big business in today's world. With more educational qualifications, banking becoming impersonal and increase in banking sector have gave rise to this white collar crime. In a survey made till 1997 bank frauds in nationalised banks was of Rs.497.60 crore.
This banking fraud can be classified as:
Fraud by insiders
Fraud by others

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, 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 rupees; there have even been cases in which a bank goes out of business due to market investment losses.

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, 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 license and no affiliation to its seemingly apparent namesake; the real Chase Manhattan bank, New York. There is a very high risk of fraud when dealing with unknown or uninsured institutions.

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

DD fraud is usually done by one or more dishonest bank employees that is the Bunko Banker. 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 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 cheque 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.

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.

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.

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 are manipulated
„« Genuine cards are altered
„« Counterfeit cards are created
„« Fraudulent telemarketing is done with credit cards.
„« 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 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

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, PAN numbers" are also valuable to the identity thief.

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.

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" 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. The securities, however, would still be worth their full amount. The transaction served only to disguise the original source of the funds.

Forged currency notes

Paper currency is the usual mode of exchange of money at the personal level, though in business, cheques and drafts are also used considerably. Bank note has been defined in Section 489A.If forery of currency notes could be done successfully then it could on one hand made the forger millionaire and the other hand destroy the economy of the nation. A currency note is made out of a special paper with a coating of plastic laminated on both sides of each note to protect the ink and the anti forgery device from damage. More over these notes have security threads, water marks. But these things are not known to the majority of the population. Forged currency notes are in full circulation and its very difficult to catch hold of such forgers as once such notes are circulated its very difficult to track its origin.

But the latest fraud which is considered as the safest method of crime without making physical injury is the Computer Frauds in Banks.

Computerization of banks had started since 1994 in India and till 2000 4000 banks were completely and 9000 branches have been partially computerised. About 1000 branches had the facilities for International bank Transaction. Reserve Bank Of India has evolved working pattern for Local area Network and wide area Network by instituting different microwave stations so that money transactions could be carried out quickly and safely.

The main banking tasks which computers perform are maintaining debit-credit records of accounts, operating automated teller machines, and carry out electronic fund transfer, print out statements of accounts create periodic balance sheets etc.

Internet facilities of computer have revolutionized international banking for fund transfer and for exchanging data of interest relating to banking and to carry out other banking functions and provides certain security to the customers by assigning different pin numbers and passwords.

Computer depredations have by some been classified as:
Computer frauds; and
Computer crimes
Computer frauds are those involve embezzlement or defalcations achieved by tampering with computer data record or proggramme, etc.Where as computer crimes are those committed with a computer that is where a computer acts as a medium. The difference is however academic only.

Bank computer crimes are committed mainly for money, however other motive or The Mens rea can be:
Personal vendetta;
Black mail;
Ego;
Mental aberrations;
Mischief

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. More over 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.

It is difficult to investigate for the following reasons:

Hi-tech crime

The information technology is changing very fast. the normal investigator does not have the proper background and knowledge .special investigators have to be created to carry out the investigations. the FBI of USA have a cell, even in latest scenario there has been cells operating in the maharashtra police department to counter cyber crimes.C.B.I also have been asked to create special team for fighting cyber crimes.

International crime

A computer crime may be committed in one country and the result can be in another country. there has been lot of jurisdictional problem an though the Interpol does help but it too has certain limitations. the different treaties and conventions have created obstructions in relation to tracking of cyber criminals hiding or operation in other nations"

No-scene crime:

The computer satellite computer link can be placed or located any where. The usual crime scene is the cyber space. The terminal may be anywhere and the criminal need not indicate the place. the only evidence a criminal leaves behind is the loss to the crime.

Faceless crime:

The major advantage criminal has in instituting a computer crime is that there is no personal exposure, no written documents, no signatures, no fingerprints or voice recognition. The criminal is truly and in strict sense faceless.

There are certain spy software's which is utilized to find out passwords and other vital entry information to a computer system. The entry is gained through a spam or bulk mail.

The existing enacted laws of India are not at all adequate to counter cyber crimes. The Indian Penal code, evidence act, and criminal procedure code has no clue about computers when they were codified. It is highly required to frame and enact laws which would deal with those subjects which are new to the country specially cyber law; Intellectual property right etc.

The Reserve Bank of India has come up with different proposals to make the way easier, they have enacted electronic fund transfer act and regulations, have amended, The Reserve Bank of India Act, Bankers Book Evidence Act etc., experience of India in relation to information and technology is limited and is in a very immature state. It is very much imperative that the state should seek the help of the experienced and developed nations.

Modus operandi:

The method of alterations of cheques drafts receipts and other fiduciary documents are comparatively simple both manually and with the help of technology.

Illustration:
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 adopted by the racketeers was interesting. A gang of four members approached owner of a newly-constructed apartment building saying they were interested in buying the flats.
The gang took xerox copies of the building documents after entering into an oral agreement of sale with the builder by paying Rs. 2 lakhs as an advance. Later, they created forged documents in the name of building's owner establishing that the latter had sold five flats to five defence 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 defence employees to utilise 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 the detectives. The police 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 xerox papers (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 xerox documents were `perfect' and to release loan after execution of sale deed.

The bank rules state that loan applications can be examined "even with xerox copies 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.

Though computer based banking crimes are yet limited but it is increasing with a huge pace. Their investigation is highly intricate and daunting. Prevention is the best alternative. It is comparatively easier, though even with the best laws, efficient investigation team the successful conclusion of most cyber crimes will remain a remote possibility .Therefore emphasis is more on prevention. In bank administration, one feels that not much attention is paid to preventive measures. Bank managements must direct their orientation towards preventive rather than detective or punitive measures. Preventive vigilance must be the prime agenda to bring down the occurrence of fraud in banks.