

### 1. INTRODUCTION

Bank fraud is a crime that has been around as long as banks themselves. Anytime there is a large amount of money floating around, there are going to be people trying to figure out ways to get to it. In the United States, and most other developed countries, bank fraud is a serious problem that causes billions of dollars in damages every year, and is considered a federal offense. In China bank fraud is even punishable by death. Bank fraud is defined as attempting to wrongfully take money or property from a Federally insured financial institution. That doesn't mean the banks are the only victims though. Millions of people every year fall victim to monetary damages that are caused by bank fraud.

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 is 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.

### 2. WHAT IS SCAM?

*“obtaining money by means of deception including fake personalities, fake photos, fake template letters, non-existent addresses and phone numbers, forged documents.”*

A scam is a dishonest attempt to trap you into parting with your money. Unfortunately we have all experienced being cheated in one way or another, and we all know how it feels.

A 'scammer' may make a personal approach, with an offer too good to be true. Someone may email you, phone, text-message or post an offer that they press you to take up.

They can often use persuasive techniques that can be hard to resist. They can sometimes make you feel that you are petty or inadequate if you resist or even question their offer.

But there are warning signs that you are being conned. There are patterns that you can learn to recognise. You can learn to spot a scam coming, and you can learn the skills to respond.

You can protect yourself, and your money, from the cheat.

### 3. BANKING SCAMS

Scam is defined as, *“any behavior by which one person intends to gain a dishonest advantage over another”. In other words , scam is an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other, either by way of concealment of facts or otherwise.”*

Bank fraud refers to the use of deliberate misrepresentation in order to fraudulently obtain money or other assets that are held by a bank or similar institution. Bank fraud is distinct from simple bank robbery or theft, because the perpetrator usually commits the fraud in secret, hoping that it will not be noticed until he has had ample time to move on. It usually requires some sort of technical expertise as well. For reasons like this, bank fraud is one of the offenses referred to as white-collar crime.

In most areas of the world, all types of bank fraud are illegal. One of the more prominent types of fraud is known as identity theft, where one person uses another person's private identifying information to obtain money, usually in the form of loans or credit. Somewhat related to identity theft is identity fraud, where credit is obtained by the use of an entirely fictitious identity. While identity theft and similar crimes receive a great deal of publicity, they are far from the only crimes involving bank fraud.

Fraud involving checks is quite common as well. Forging checks or signatures on them, as well as altering checks that have already been written are two ways in which check fraud is committed. In the case of the latter, it may be as simple as adding a few strokes of a pen to turn a check for \$100 US Dollars (USD) into one for \$1,000 USD. Another common type of fraud is check kiting. This is any kind of fraud that takes advantage of the fact that funds can be drawn on a deposited check before the money is actually removed from the check writer's account.

Check fraud has a history as long as that of checks themselves. Over the years, security features have been incorporated into many types of checks, especially payroll checks. These include unique watermarks, heat-sensitive ink, and extremely fine printed lettering that is not easily noticed or counterfeited. Technology has placed many barriers in the way of those

who would perpetrate bank fraud, but not all fraud can be completely prevented.

One kind of bank fraud that is still hard to detect or stop in time is that which is committed by bank employees themselves. In many cases, these acts are only discovered by careful auditing of the bank's accounting records, months down the road, by which time it is too late to recover lost funds. A complete description of the many possible ways to commit bank fraud would be impossible, but suffice it to say that criminals have gone to great lengths and used remarkable creativity in finding new and different ways to steal and defraud.

### **4. BANK FRAUDS: CONCEPT AND DIMENSIONS**

Banks are the engines that drive the operations in the financial sector, which is vital for the economy. With the nationalization of banks in 1969, they also have emerged as engines for social change. After Independence, the banks have passed through three stages. They have moved from the character based lending to ideology based lending to today competitiveness based lending in the context of India's economic liberalization policies and the process of linking with the global economy.

While the operations of the bank have become increasingly significant banking frauds in banks are also increasing and fraudsters are becoming more and more sophisticated and ingenious. In a bid to keep pace with the changing times, the banking sector has diversified its business manifold. And the old philosophy of class banking has been replaced by mass banking. The challenge in management of social responsibility with economic viability has increased.

#### **Mechanics of bank fraud against banks**

##### **Stolen checks**

Some fraudsters obtain access to facilities handling large numbers 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 checkbooks are also of value to forgers who then sign as if they were the depositor.

##### **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).

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.

### **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

### **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. Examples of accounting frauds: Enron and WorldCom. These two companies "cooked the books" in order to appear as they had profits each quarter when in fact they were deeply in debt

### **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 D.C. appeared in 2002 with no license and no affiliation to its seemingly apparent namesake; the real Chase Manhattan Bank is based in New York. Accounting fraud has also been used to conceal other theft taking place within a company.

### **Demand draft fraud**

Demand draft 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

### **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. Fraudulent loan applications

### **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.

### **Wire transfer 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.

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.

### **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 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.

### **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.

### **Empty ATM envelope deposits**

A criminal overdraft can result due to the account holder making a worthless or misrepresented deposit at an automated teller machine in order to obtain more cash than present in the account or to prevent a check from being returned due to non-sufficient funds. United States banking law makes the first \$100 immediately available and it may be possible for much more uncollected funds to be lost by the bank the following business day before this type of fraud is discovered. The crime could also be perpetrated against another person's account in an "account takeover" or with a counterfeit ATM card, or an account opened in another person's name as part of an identity theft scam. Later this decade, this scenario may become a thing of the past due to the emergence of ATM deposit technology that scans currency and checks without using an envelope.

### **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. However, 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 are all fictitious financial instruments intended to defraud individuals.

### **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.

### **5. FRAUD PRONE AREAS IN DIFFERENT ACCOUNTS**

The following are the potential fraud prone areas in Banking Sector. In addition to those areas I have also given kinds of fraud that are common in these areas.

#### **Savings Bank Accounts**

The following are some of the examples being played in respect of savings bank accounts:

- (a) Cheques bearing the forged signatures of depositors may be presented and paid.
- (b) Specimen signatures of the depositors may be changed, particularly after the death of depositors,
- (c) Dormant accounts may be operated by dishonest persons with or without collusion of bank employees, and
- (d) Unauthorized withdrawals from customer's accounts by employee of the bank maintaining the savings ledger and later destruction of the recent vouchers by them.

#### **Current Account Fraud**

The following types are likely to be committed in case of current accounts.

- (a) Opening of frauds in the names of limited companies or firms by unauthorized persons;
- (b) Presentation and payment of cheques bearing forged signatures;
- (c) Breach of trust by the employees of the companies or firms possessing cheque leaves duly signed by the authorized signatures;
- (d) Fraudulent alteration of the amount of the cheques and getting it paid either at the counter or through another bank.

### **Frauds In Case Of Advances**

Following types may be committed in respect of advances:

- (a) Spurious gold ornaments may be pledged.
- (b) Sub-standard goods may be pledged with the bank or their value may be shown at inflated figures.
- (c) Same goods may be hypothecated in favour of different banks.

### **6. RECENT TRENDS OF BANKING SYSTEM IN INDIA**

In the banking and financial sectors, the introduction of electronic technology for transactions, settlement of accounts, book-keeping and all other related functions is now an imperative. Increasingly, whether we like it or not, all banking transactions are going to be electronic. The thrust is on commercially important centers, which account for 65 percent of banking business in terms of value. There are now a large number of fully computerized branches across the country.

A switchover from cash-based transactions to paper-based transactions is being accelerated. Magnetic Ink character recognition clearing of cheques is now operational in many cities, beside the four metro cities. In India, the design, management and regulation of electronically-based payments system are becoming the focus of policy deliberations. The imperatives of developing an effective, efficient and speedy payment and settlement systems are getting sharper with introduction of new instruments such as credit cards, telebanking, ATMs, retail Electronic Funds Transfer (EFT) and Electronic Clearing Services (ECS). We are moving towards smart cards, credit and financial Electronic Data Interchange (EDI) for straight through processing.

### **BANK FRAUD RISE IN INDIA**

Crores of rupees are disappearing from bank accounts or are being used deceitfully everyday .The Reserve Bank of India has announced that bank frauds are on the rise. Moreover, it is the public sector banks, considered to be safer than private banks, that beat the latter in the swindling game, reports Economic Times.

Crores of rupees have been disappearing from bank accounts or are being used deceitfully everyday. According to Economic Times, recently, a bank branch manager recklessly sanctioned housing loans for the purpose of flats. On the behest of the bank's chief vigilance officer, an on spot verification by the Central Bureau of Investigation (CBI) was conducted, during which it transpired that the three storeyed building was constructed as a hotel.

On further probing it was found that the branch manager had sanctioned many other housing loans against fabricated agreements of sale in fictitious names. By the time, the investigation was completed the bank had been duped of ₹25 crore.

"This is an alarming scenario. After all, it is people's hard earned money.

Globally, banks keep a tight vigil as any slip can bring them down and even impact the economy," says Chairman of Indiaforensic Research Foundation, a Pune-based consultancy which conducts fraud examination and forensic accounting in India.

Information collated by the CBI has shown that, the central investigation body tracks frauds valuing only a crore or above - amount doubled in 2008-09 from ₹659 crore in 2007-08 to ₹1,404 crore.

"The focus is on expeditious completion of investigation, close follow up of under-trial cases to conclude them without delay," says a CBI spokesperson. The rising number of frauds has also got the central bank concerned. "It's high time banks strengthen their fraud management practices. In their bid to quickly expand and grow, they are losing focus on risk control," said a senior official of the bank.

### 7. NEWS RELATED TO BANK FRAUD

#### 4 held for bank fraud

Jan 25/ 2011

MUMBAI: A chartered accountant (CA) and her three accomplices were arrested by the MIDC police after they applied for loans against the same house from two banks. Anita Chaudhary, Anil Shelar, Shrisheila Sandimantri and Suresh Joshi have been booked on charges of cheating and forgery.

Chaudhary, a chartered accountant, had applied for a loan to buy a house which she already owned. She got the loan by submitting forged documents that were prepared by accomplices.

"Chaudhary submitted all necessary documents required for getting a home loan to the bank's MIDC, Andheri (East), branch. A loan of Rs 77 lakh was sanctioned for the flat in Kandivli. When the loan was disbursed, the accused opened a bogus account in a bank at Marine Drive and withdrew the money. Later, the four split the money between themselves," a police official said.

The MIDC bank's vigilance department soon found that Chaudhary had already taken a loan for the same flat from another bank by producing original documents.

The four were arrested on the basis of a complaint by the bank. They were produced before a metropolitan court which remanded them to judicial custody.

#### Bank fraud detected

Sep 16, 2001,

ahmedabad: the naroda police have detected a bank fraud worth rs 4.5 lakh involving the oriental bank of commerce and the rajkot branch of andhra bank. b. subbaramarao had filed a complaint with the naroda police that m k pathak, owner of sky skate paper mart, had deposited two demand drafts with counterfeit signatures at oriental bank of commerce's naroda branch

and withdrawn the money. pathak allegedly opened an account with the bank and deposited rs 5,000. he then presented two separate drafts from

andhra bank, one for rs 50,000 and another for rs 4 lakh, and withdrew the money. an inquiry by the bank officials, however, revealed that signatures in both drafts were counterfeit. the police have registered a case of cheating and forgery against pathak.

### **Woman alleges bank fraud**

May 26, 2011,

GURGAON: A woman has lodged a case against the branch manager and cashier of a nationalized bank for allegedly diverting Rs 5 lakh from her account. The case has been registered at Civil Lines police station.

According to the police, the woman has lodged an FIR alleging that she lost her savings due to the negligence of bank officials.

The victim, Pushpa Devi, has a savings account in the Gurdwara Road branch of the bank. She has alleged that few days back Rs 5 lakh had been transferred from her account to another account without her permission.

"When she filed a compliant with the bank, the branch officials investigated the case and found that the amount was transferred to the account of another customer," said a senior police officer.

### **2 convicted of bank fraud**

Nov 2, 2007,

BANGALORE: The proprietor of a private company and another man were convicted for fraud on Thursday. The 21st additional city civil and sessions court judge SudhakarPandit, sentenced B R Amarnath, a resident of 100 Ft Road, Jayanagar, to one-year rigorous imprisonment (RI) and imposed Rs-10,000 fine. B Kasinath, proprietor of the Bangalore Company, KH Road, has been sentenced to two-and-a-half years RI and has to pay Rs-50,000 fine. The case against another accused, P K Sharma, former branch manager of State Bank of Patiala, JP Nagar, was dropped as he is dead.

Kasinath opened a current account at State Bank of Patiala, JP Nagar. He conspired with Amarnath and issued four cheques amounting to Rs 27.50

lakh on March 10, 1993, and three other dates. This amount was deposited at Karnataka Bank, Sarakki.



Instead of returning the Bangalore Company's cheques for want of the requisite balance, P K Sharma cleared them by debiting the amount from the bank's clearing house account.

He later adjusted Rs 13.5 lakh to the current account and fraudulently created fixed deposits worth Rs 7.5 lakh in the company's name.

Kasinath's company also availed a Letter of Credit (LC) worth Rs 30 lakh and cash credit of Rs 70 lakh; he carried out accommodative LC transactions, thereby causing a loss of Rs 125 lakh to the State Bank of Patiala.

### **Software engineer held for bank fraud**

Nov 5, 2011,

- Punjab National Bank

GUWAHATI: Sleuths of CBI's anti-corruption wing on Friday arrested GautamThakuria, a software engineer of Birmati Software and Telecom Ltd, Ahmedabad, from a rented house at Dwaraka Nagar in the city for his involvement in a net-banking fraud case.

The CBI was in search of Thakuria for the last three months after the Boroma and Nityananda of Assam GraminVikash Bank filed a FIR against him in July, suspecting his involvement in swindling Rs 58,87,000.

"Thakuria was part of the net banking software installation programme at the bank. Thus he knew all the passwords and later forcefully cracked 10 bank accounts in the branches and swindled money. We finally we caught him from his rented house at 12.30 am today," said CBI DIG HirenNath.

Though the CBI wing arrested Thakuria for his involvement in two cases, AGVB officials said such frauds took place in more than 20 braches across the state. "The scam is worth Rs 2 crore. CBI cracked two cases but there are other cases lying in local police stations," said a top official of the bank.

"Thakuria has been charged under various sections of the PC Act. We produced him in the special court on Friday which sent him to five-day police remand," added Nath.

The CBI further said Thakuria is involved in many commissioned programmes of Doordarshan here. We found three bank accounts in

Thakuria's possession - one of Punjab National Bank, SBI (Tihu) and AGVB. We also found some documents which point to his involvement in Doordarshan commissioned programmes," said Nath.

Thakuria is an employee of the software firm and hails from Helena village of Patacharkuchi in Barpeta district of lower Assam.

### **NCP leader held in Rs 600cr bank fraud**

Apr 3, 2011,

MUMBAI: A Raigad police team on Saturday arrested senior NCP leader Shirish Dharkar for his alleged involvement in the Rs 600 crore fraud in the Pen urban cooperative bank. Dharkar heads the bank.

Dharkar and his wife Gulrainia were arrested from an Andheri flat. He was absconding for the last few days. As head of the bank, he, allegedly connived with 29 directors, forged documents and misled the administration to cheat account holders. During the financial years 2008-09 and 2009-10, Dharkar fabricated documents to establish that all was well with the bank. But the bank was facing a financial crisis. "Thus, he cheated 41,000 account holders of the bank," a senior police officer said

### **Banks lost Rs.2,289cr in scams**

The recent Rs.300-crore scam in the Gurgaon branch of Citi Bank is a pointer to a disturbing trend: the steady rise in the number of banks falling prey to such frauds.

According to the data compiled by the Reserve Bank of India (RBI), the money lost to such scams has doubled in the past four years. In the current financial year, banks lost Rs.2,289 crore (till December), while the loss was Rs.1,057 crore in 2007-08.

It's the state-of-the-art private banks, including foreign banks, that appear to be more prone to such frauds. The public sector banks, with their massive presence across the country, also reported an annual average of more than 3,000 cases of frauds and cheating during the past four years. Their better equipped counterparts in the private sector reported almost five times the number of cases.

ICICI Bank alone accounted for almost half of the total scams reported to the RBI. Of the total 21,244 cases reported in 2007-08, a whopping 10,976 were from ICICI.

Similarly, in 2008-09, ICICI reported 13,221 of the total 23,579 cases. The bank reported 15,074 of the total 24,788 fraud cases in 2009-10.

The second highest number of cases were reported by HSBC (3,770, 3,481, 2,741, 2028); followed by Citi Bank (1,647, 1,182, 1,277, 666); American Express banking (499, 703, 817, 637) and the distant fourth was State Bank of India (561, 745, 545, 615) during the past four financial years - 2007-08, 2008-09, 2009-10, 2010-11 respectively. The figures for the current fiscal are till December, 2010.

Maharashtra, with Mumbai being the country's financial capital, reported the maximum number of fraud cases: (1,006 in 2009-10 and 1,045 in 2010-11).

Delhi was second with 349 cases in 2009-10 and 338 in 2010-11.

Union minister of state for finance NamoNarainMeena presented these figures in the LokSabha on Friday.

The data has thrown up interesting trends in not just scams and frauds but also the way banks were being targeted by robbers and thieves.

Punjab reported the maximum number of dacoity and ATM thefts, followed by Uttar Pradesh and Haryana.

State Bank of India appeared to be the favourite for thieves and burglars.

SBI reported 114 such cases in 2009-10 and 79 this year, followed by State bank of Patiala - 41 and 39 respectively.

Overall, 582 cases were reported across the country in 2009-10 that resulted in a loss of Rs.21.22 crore, while a recovery of Rs.6.67 crore could be only made.

This year's figure stands at 392 cases, Rs.16.17 crore loss and Rs.4.98 crore recoveries.

### **More frauds and shocking loss**

1,045 bank fraud cases reported by Maharashtra reported in 2010-11

338 such cases were reported in Delhi in 2010-11

545 cases reported by SBI - highest by a public sector bank in 2009-10

15,074 cases reported by ICICI in 2009-10 - highest by a private bank

2,741 frauds reported by HSBC in 2009-10 - highest by a foreign bank

2,764 cases reported by public Sector banks in 2010-11 (till Dec)

Rs.1,497cr Loss incurred by public Sector banks in 2010-11 (till Dec)

9,175 cases reported by private banks in 2010-11

Rs.307 cr Loss to private banks in 2010-11

### **Robberies / thefts**

Rs.96 lakh Loss reported by banks in Punjab in 2009-10 because of 81 cases

Rs.21.22 cr Loss reported by banks in across the country in 2009-10

Rs.16.17 cr Loss reported by banks in the country in 2010-11 (till date)

### 8. Top 3 Financial Scams in India

- **Insurance Scam**

This scam had originated and prospered in the period immediately following Independence in 1947. At that time, the insurance sector was not nationalized, and a handful of private companies ruled the roost. These companies were more concerned with providing benefits to selected industrialists, and ignored the interests of the common man. The government responded by nationalizing the insurance sector, and the LIC was founded under an special Act passed by the Parliament. This scam laid the foundation of the nationalization culture in India.

- **Citibank Gurgaon**

A banking fraud which could run into a whopping Rs 400 crore was unearthed at Citibank's Gurgaon (Haryana) branch. Funds amounting to Rs 400 crore of 20 high networth customers was allegedly siphoned off by bank executive ShivrajPuri.

Puri is accused of selling investment products to high networth clients claiming that they would generate unusually high returns. It is also alleged that Puri, who is named in the FIR, showed a forged notification of market regulator Securities and Exchange Board of India for obtaining funds from customers. He is also accused of claiming that these products were authorised by the bank's investment product committee.

- **The UTI Scam**

UTI had purchased 40,000 shares of Cyberspace between September 25, 2000, and September 25, 2000 for about Rs 3.33 crore (Rs 33.3 million) from Rakesh Mehta when there were no buyers for the scrip. The market price was around Rs 830.

The CBI said it was the conspiracy of these four people which resulted in the loss of Rs 32 crore (Rs 320 million). Subramanyam, Kapur and Basu had changed their stance on an investment advice of the equities research cell of UTI.

The promoter of Cyberspace Infosys, Arvind Johari was arrested in connection with the case. The officials were paid Rs 50 lakh (Rs 5 million) by Cyberspace to promote its shares.

He also received Rs 1.18 crore (Rs 11.8 million) from the company through a circuitous route for possible rigging the Cyberspace counter.

Former UTI chairman P S Subramanyam and two executive directors - M M Kapur and S K Basu - and a stockbroker Rakesh G Mehta, were arrested in connection with the 'UTI scam'.

### 9. Case study :

#### ICICI Scam

#### ICICI Bank phishing scam hits again

Phishing is nothing but a technique used to commit online fraud to steal personal and confidential information (Identity Theft) which includes credit card number, bank details including password and account information, passport information etc. ICICI bank which is one of the most leading banks in India is being targeted more often than any other in the country. Today I too received an email which is part of the phishing scam and liked to share it with you guys.



I received a mail with the subject

***“ICICI Bank Alert: Please Re-Confirm Your Internet Banking Details”***  
with the links to the phishing or the fake ICICI site which looks similar to the ICICI login page. I clicked the link which was directed to the fake ICICI site where I was asked to input all personal information including my account password, card number, security code in the card to passport information. Please see the pictures below,



[Previous](#) | [Next](#) | [Back to Mailbox](#)

---

DeleteReplyForwardSpamMove...

ICICI Bank Alert: Please Re-Confirm Your Internet Banking Details

From: "ICICI BANK" <alerts@icicibank.com>  
To: undisclosed-recipients

---

ICICI Bank

---

We Are Upgrading Our Server's So Verify Your Login Details.  
Dear ICICI Bank Customer,

This is your official notification from ICICI Bank that the service(s) listed below will be deactivated and deleted if not renewed immediately. Previous notifications have been sent to the Billing Contact assigned to this account. As the Primary Contact, you must renew the service(s) listed below or it will be deactivated and deleted.  
SERVICE: ICICI Bank Online Banking Update  
EXPIRATION: JUL 30th 2009

<https://infinity.icicibank.co.in/login.jsp>

For Corporate Users Click Here  
<https://cib.icicibank.com>

Sincerely,  
ICICI Bank Account Review Department

Need help Use "Site Helper" or call customer service at 1.800.788.7000.

Please do not "Reply" to this Alert.

2007 ICICI Bank Financial Group. All rights reserved

DeleteReplyForwardSpamMove...

[Previous](#) | [Next](#) | [Back to Mailbox](#)



## Banking Scam



**Internet Banking Update - Billing Details**

Full Name	:	<input type="text"/>
Address	:	<input type="text"/>
City	:	<input type="text"/>
Postal Code	:	<input type="text"/>
State	:	<input type="text"/>
Date Of Birth	:	<input type="text" value="Month"/> <input type="text" value="Day"/> <input type="text" value="Year"/>
PAN Number	:	<input type="text"/>
Mother's Maiden Name	:	<input type="text"/>
Nominee Name	:	<input type="text"/>
Account Number	:	<input type="text"/>
ATM PIN	:	<input type="text"/>
Mode Of Account Statement	:	<input type="text" value="Choose Type of Statement"/>
Credit Card Number	:	<input type="text"/>
Expiration Date	:	<input type="text" value="Month"/> <input type="text" value="Year"/>
3 Digit Security Number (CVV)	:	<input type="text"/>
Passport Number	:	<input type="text"/>
Passport Expiration Date	:	<input type="text" value="Month"/> <input type="text" value="Year"/>



### Thanks For Upgrading Your Account.

Dear Customer,

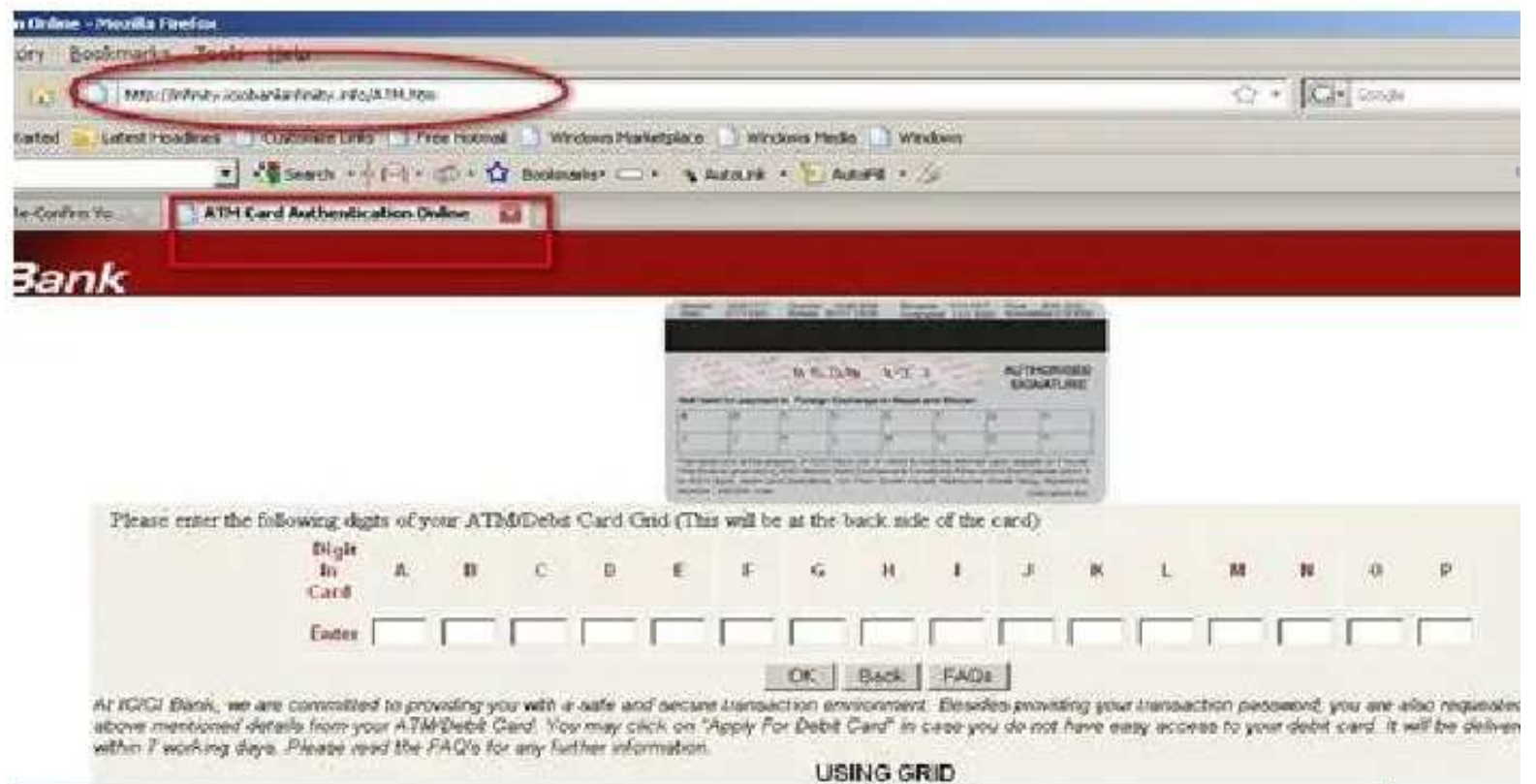
ICICI is constantly striving to provide you with more convenience, control, and security to assist in managing your finances. As part of our ongoing efforts to make it easier and more secure for you to use our online services, we have upgraded the ICICI E-Sign Consent and Online Access that you reviewed and accepted when you began to use ICICI Online® Banking service(s). No additional action is required by you to continue to use your online services.

We reiterate that ICICI Bank acts at all times with diligence, in good faith, and without any intent prejudicial to the interests of its customers.

Thank you for your cooperation.

Sincerely,

ICICI Bank Ltd.



### How to identify phishing scams?

- All mails that asks your password and other credentials are fake and no bank will send you a mail like that.
- The link you click from your mail will be re-directed to a different URL which looks completely different from the bank.
- The page URL will not have https:// and will be using http:// where HTTPS is secured browsing with the VeriSign certificate. Also you cannot find the padlock symbol at the right corner bottom of your browser which indicates the site you are browsing is a secured website.

### 10.LEGAL REGIME TO CONTROL BANK FRAUDS

Frauds constitute white-collar crime, committed by unscrupulous persons deftly advantage of loopholes existing in systems/procedures. The ideal situation is one there is no fraud, but taking ground realities of the nation's environment and human nature's fragility, an institution should always like to keep the overreach of frauds at the minimum occurrence level.

Following are the relevant sections relating to Bank Frauds

Indian Penal Code (45 of 1860)

(a) Section 23 "Wrongful gain".-

"Wrongful gain" is gain by unlawful means of property to which the person gaining is not legally entitled.

(b) "Wrongful loss"

"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.

(c) Gaining wrongfully.

Losing wrongfully-A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property, as well as when such person is wrongfully deprived of property.

(d) Section 24. "Dishonestly"

Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

(e) Section 28. "Counterfeit":A person is said to "counterfeit" who causes one thing to resemble another thing, intending by means of that resemblance to practice deception, or knowing it to be likely that deception will thereby be practiced.



### 11. PHYSICAL SECURITY MEASURES-CONCEPT

A large part of banks security depends on social security measures. Physical security measures can be defined as those specific and special protective or defensive measures adopted to deter, detect, delay, defend and defeat or to perform any one or more of these functions against culpable acts, both covert and overt and calamitous natural events. The protective or defensive measures adopted involve construction, installation and deployment of structures, equipment and persons respectively.

The following are few guidelines to check malpractices:

1. To rotate the cash work within the staff.
2. One person should not continue on the same seat for more than two months.
3. Passbook should not be written by the Cashier where an other person is available to the job
4. No cash withdrawal should be allowed within passbook in case of withdrawal by pay order.
5. The branch manager should ensure that all staff members have recorder their presence in the attendance registrar, before starting work.

#### Execution of Documents

1. A bank officer must adopt a strict professional approach in the execution of documents. The ink and the pen used for the execution must be maintained uniformly.
2. Bank documents should not be typed on a typewriter for execution. These should be invariably handwritten for execution.
3. The execution should always be done in the presence of the officer responsible for obtain them,
4. The borrowers should be asked to sign in full signatures in same style throughout the documents.

5. Unless there is a specific requirement in the document, it should not be got attested or witnessed as such attestation may change the character of the instruments and the documents may subject to ad volrem stamp duty.
6. The paper on which the bank documents are made should be pilfer proof. It should be unique and available to the banks only.
7. The printing of the bank documents should have highly artistic intricate and complex graphics.
8. The documents executed between Banker and Borrowers must be kept in safe custody,

### 12. Banking Fraud - Prevention and Control

In the present day, Global Scenario Banking System has acquired new dimensions. Banking did spread in India. Today, the banking system has entered into competitive markets in areas covering resource mobilization, human resource development, customer services and credit management as well.

Indian's banking system has several outstanding achievements to its credit, the most striking of which is its reach. In fact, Indian banks are now spread out into the remotest areas of our country. Indian banking, which was operating in a highly comfortable and protected environment till the beginning of 1990s, has been pushed into the choppy waters of intense competition.

A sound banking system should possess three basic characteristics to protect depositor's interest and public faith. These are:

- 1) a fraud free culture
- 2) a time tested Best Practice Code, and
- 3) an in house immediate grievance remedial system.

All these conditions are their missing or extremely weak in India. Section 5(b) of the Banking Regulation Act, 1949 defines banking... "Banking is the accepting for the purpose of lending or investment, deposits of money from the purpose of lending or investment, deposits of money from the public, repayable on demand or otherwise and withdraw able by cheque, draft, order or otherwise." But if his money has fraudulently been drawn from the bank the latter is under strict obligation to pay the depositor. The bank therefore has to ensure at all times that the money of the depositors is not drawn fraudulently. Time has come when the security aspects of the banks have to be dealt with on priority basis.

The banking system in our country has been taking care of all segments of our socio-economic set up. The Article contains a discussion on the rise of banking frauds and various methods that can be used to avoid such frauds.

A bank fraud is a deliberate act of omission or commission by any person, carried out in the course of banking transactions or in the books of

accounts, resulting in wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank. The relevant provisions of Indian Penal Code, Criminal Procedure Code, Indian Contract Act, and Negotiable Instruments Act relating to banking frauds has been cited in the present Article.

### **FRAUDS-PREVENTION AND DETECTION**

A close study of any fraud in bank reveals many common basic features. There may have been negligence or dishonesty at some stage, on part of one or more of the bank employees. One of them may have colluded with the borrower. The bank official may have been putting up with the borrower's sharp practices for a personal gain. The proper care which was expected of the staff, as custodians of banks interest may not have been taken. The bank's rules and procedures laid down in the Manual instructions and the circulars may not have been observed or may have been deliberately ignored.

Bank frauds are the failure of the banker. It does not mean that the external frauds do not defraud banks. But if the banker is upright and knows his job, the task of defrauder will become extremely difficult, if not possible.

### **Detection of Frauds**

Despite all care and vigilance there may still be some frauds, though their number, periodicity and intensity may be considerably reduced. The following procedure would be very helpful if taken into consideration

1. All relevant data-papers, documents etc. Should be promptly collected. Original vouchers or other papers forming the basis of the investigation should be kept under lock and key.
2. All persons in the bank who may be knowing something about the time, place a modus operandi of the fraud should be examined and their statements should be recorded.
3. The probable order of events should thereafter be reconstructed by the officer, in his own mind.



4. It is advisable to keep the central office informed about the fraud and further developments in regard thereto.

### **How to Avoid... Banking Scams**

- Protect your checking and other account numbers. Never give them to a someone you don't know
- Beware of phone calls from someone claiming to call from your bank. There are scams where someone poses as your bank and says they need to verify your account information
- Store your checks (new or cancelled) in a secure place. Use tamper proof checks.
- Guard your ATM information. Don't use obvious PINs, don't write the PIN on the card or leave the PIN on paper in your wallet or purse.
- Try swiching to electronic billing and statements.

### **Safety first**

"Sadly, some people have given out or confirmed account details not realising that they are not actually talking to someone from the bank," plz do not to give any personal information out over the phone, especially bank details.

the police also advice, that customers “should never disclose or confirm any personal banking details over the phone”, reiterating that banks will

never call customers and ask for personal details.

If you think that you’ve been a victim of a bogus banking call, contact your bank straight away – but it’s not just telephone bankers that are at risk of fraud.

1. Check your statements
2. Buy a shredder
3. Secure important documents
4. Safeguard your PC
5. Safeguard sensitive information
6. Report thefts

7. Guard your mail Watch your emails
8. Register to vote
9. Check your credit report

### 11.CONCLUSION

The Indian Banking Industry has undergone tremendous growth since nationalization of 14 banks in the year 1969. There has an almost eight times increase in the bank branches from about 8000 during 1969 to mote than 60,000 belonging to 289 commercial banks, of which 66 banks are in private sector.

It was the result of two successive Committees on Computerization (Rangarajan Committee) that set the tone for computerization in India. While the first committee drew the blue print in 1983-84 for the mechanization and computerization in banking industry, the second committee set up in 1989 paved the way for integrated use of telecommunications and computers for applying technogical breakthroughs in banking sector.

However, with the spread of banking and banks, frauds have been on a constant increase. It could be a natural corollary to increase in the number of customers who are using banks these days. In the year 2000 alone we have lost Rs 673 crores in as many as 3,072 number of fraud cases. These are only reported figures. Though, this is 0.075% of Rs 8,96,696 crores of total deposits and 0.15% of Rs 4,44,125 crores of loans & advances, there are any numbers of cases that are not reported. There were nearly 65,800 bank branches of a total of 295 commercial banks in India as on June 30, 2001 reporting a total of nearly 3,072 bank fraud cases. This makes nearly 10.4 frauds per bank and roughly 0.47 frauds per branch.

An Expert Committee on Bank Frauds (Chairman Dr.N.L.Mitra) submitted its Report to RBI in September 2001. The Committee examined and suggested both the preventive and curative aspects of bank frauds.

The important recommendations of the Committee include

- o A need for including financial fraud as a criminal offence;
- o Amendments to the IPC by including a new chapter on financial fraud;
- o Amendments to the Evidence Act to shift the burden of proof on the accused person;
- o Special provision in the Cr. PC for properties involved in the Financial Fraud.

- o Confiscating unlawful gains; and preventive measures including the development of Best Code Procedures by banks and financial institutions.

Thus it can be concluded that following measures should necessarily be adopted by the Ministry of Finance in order to reduce cases of Fraud.

- o There must be a Special Court to try financial fraud cases of serious nature.



- o The law should provide separate structural and recovery procedure. Every bank must have a domestic enquiry officer to enquire about the civil dimension of fraud.

- o A fraud involving an amount of ten crore of rupees and above may be considered serious and be tried in the Special Court.

The Twenty-ninth Report of the Law Commission had dealt some categories of crimes one of which is offences calculated to prevent and

obstruct the economic development of the country and endanger its economic health. Offences relating to Banking Fraud will fall under this category. The most important feature of such offences is that ordinarily they do not involve an individual direct victim. They are punishable because they harm the whole society. It is clear that money involved in Bank belongs to public. They deposit there whole life's security in Banks and in case of Dacoity or Robbery in banks the public will be all lost. Thus it is important that sufficient efforts should be taken in this regard.

There exists a new kind of threat in cyber world. Writers are referring it as Salami Attack under this a special software is used for transferring the amount from the account of the individual. Hence the culprits of such crimes should be found quickly and should be given strict punishment. Moreover there is requirement of more number of IT professionals who will help in finding a solution against all these security threats.



**SAFE BANKING**

# Beware of fraud

## Protect yourself from Phishing!

Dear Customer,

Fraudsters continuously find new ways to steal identity parameters from unsuspecting customers to carry out fraudulent transactions. **'Phishing'** is an online method used by fraudsters to capture customers' online personal identity details (like User ID, Password, Date of Birth and CVV number etc.). So far, requests for these sensitive and personal details have been made through links in e-mails which are misunderstood to be authentic bank requests by unsuspecting users.

In recent times, a new form of 'Phishing' called **'In-session Phishing'** has emerged. Through this new method, a pop-up appears requesting you to enter your personal online identity details, while you are logged-in to the bank's website. The pop-up emerges during the session and so can be easily mistaken to be from the bank. The pop-up may also ask you to take part in a survey or inform you that your session has expired and hence requests you to re-enter your details.

**We would like to bring to your notice that ICICI Bank will never ask you to update or validate your account information through links given in an e-mail or pop-up window. Hence, we request you to please ignore any such requests.**

Sincerely,

ICICIBank

### How to protect yourself from phishing?

- Always type the address of your bank (URL) in the browser bar while banking online.
- Do not open multiple browser windows when you are banking online.
- Do not give your Account Details, User ID, Password etc. on any pop-ups that appear in a web session.
- Always log off and close the browser window after you have finished your online banking session.
- Use reputed anti-virus and anti-spy ware tools to keep your computer in good health.

To unsubscribe from e-mailers please visit [www.icicibank.com](http://www.icicibank.com) and register yourself under the "Do not call" registry.

## BIBLIOGRAPHY

- 1) [www.wikipedia.com](http://www.wikipedia.com)
- 2) [www.bankingfrauds.com](http://www.bankingfrauds.com)
- 3) [www.thinkbanking.com](http://www.thinkbanking.com)
- 4) [www.icicibank.com](http://www.icicibank.com)
- 5) [www.google.com](http://www.google.com)