ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 9, Issue, 06, pp.52198-52200, June, 2017

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

REVIEW ARTICLE

BANK FRAUD INVESTIGATIONS

[1]Dr. Anu Singla and *,[2]Baljeet Yadav

[1]Associate Professor, Institute of Forensic Science and Criminology, Bundelkhand University, Jhansi, India
[2]Research Scholar, Institute of Forensic Science and Criminology, Bundelkhand University Jhansi, Uttar Pradesh, India

ARTICLE INFO

Article History:
Received 12th March, 2017
Received in revised form
08th April, 2017
Accepted 26th May, 2017
Published online 20th June, 2017

Key words:

Forensic Science, Fraud Investigations, Forgery, Internet, Internal controls, Security measures.

ABSTRACT

When a crime is falsified committed and with intent to deceive is said to be forged. Such Crime is punishable under law. Fraud in banks is more often seen by false documentation, transactions, signatures and invalid KYCs which in turns convert into Fraud and further leads to fraud investigations. Fraud investigation in also adversely affected by the digitization in banks, from unsafe unsecure internet banking solutions which are more prone to fraud activities through Internet and there are still so many observation which on documents can be copied altered without any prior permission and further which could be fatal for customer or even sometimes to bank officials. So, there is an urgent need for the proper systematic investigation in Bank fraud examinations.

Citation: Dr. Anu Singla and Baljeet Yadav, 2017. "Bank fraud investigations", *International Journal of Current Research*, 9, (06), 52198-52200.

INTRODUCTION

In bank fraud investigations, forensic & its tools help in crabbing out the facts and in concluding, to unhide the clues and other important facts which are useful in fraud investigations. As there is a rapid increase in Frauds and white collar crimes, forensic accounting now days in India has come to a limelight because our law enforcement agencies do not have that much expertise which can uncover the hidden clues or frauds in banks. [1][Fraud is described under Section 17 of the Indian Contract Act, 1872, which includes any of the following acts committed by a party to a contract, or with his connivance, Fraud" means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto of his agent, or to induce him to enter into the contract:-

Sub Section (1) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true.

Sub Section (2) the active concealment of a fact by one having knowledge or belief of the fact.

Sub Section (3) a promise made without any intention of performing it.

Sub Section (4) any other act fitted to deceive.

Sub Section (5) any such act or omission as the law specially declares to be fraudulent.]$_1$

There are several types of bank frauds in general which particularly happens in common but these things should be noticed.

Category of frauds

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

1. KYC related (mainly in deposit accounts) or Fake Documentation
2. Technology related
3. Advances related

KYC related or Fake documentation

a. Physical Alterations

Most often happens in the issuing dates of cheque, or transcription of changing it to a latest date by altering the previous date already mentioned or written by the bank official or by customer itself which is unnoticed most often times by bank officials or by customer in issuing of those documents. Some other alterations may be the use of different ink or pen or erasure which may rise a question mark on document's authenticity.

Corresponding author: **Baljeet Yadav,**
Research Scholar, Institute of Forensic Science and Criminology, Bundelkhand University Jhansi, Uttar Pradesh, India.

b. Chemical Alterations

Sometimes there are bank tapes on cheque creates that overflow of adhesive can omit the words or figure which later on can create a problem for a customer or to bank official itself. Use of more inked seals also sometimes increases the work load of officials and may disprove the authenticity of the document. The use of low grade adhesive gums also create a problem document gets chapped with other document because of flow of adhesive gums during summers or after long time and ink gets dissolve with gum, and document looses its authenticity.

c. Conventional Method

Some of the documents also changes with the passage of time by handling and wear tear of the documents, At a point of time the documents may lose the authenticity of the documents and customer then tries to use of those document by editing it.

Technology Related Frauds

Internet Banking

More advanced facilities and easy banking steps, have somewhere opened the gate for more transitional crimes and fraudal activities, like [Internet banking in which banks have made very easy facilities and steps for transaction and withdrawal solution which can be done and proceed with the help of Internet with 24 hrs facilities, which is termed as Internet Banking. With the advantages of transferring money and successful transaction of bills and cheques and timely billing of different things and elements in one few minutes to one place to another in coversion of money into plastic money, leads to open a serious threat to the phishing, revealing information in secured pin numbers and unwanted transactions and ultimately deduction of money by unfair means.] There are more chances of fraudal activities in banks by providing a facility of internet banking. There are some frauds listed which are more prone to fraudal activities in bank by internet options

1. Identity theft
2. Credit/Debit card fraud
3. Cheque fraud
4. Electronic fraud
5. Card Skimming

Credit card & debit card frauds

[2][Credit card and debit card fraud is a crime whereby your credit or debit card can be reproduced in order to use the credit balance to obtain a financial advantage. The creation and/or alteration of a credit/debit card occur when the information contained on the magnetic strip is reproduced. This type of crime is known as 'skimming'.]$_2$Credit or debit card fraud can also occur when your card is lost or stolen and used by a third party to purchase goods with those cards or to remove cash from the cards. Credit or debit cards can also be intercepted in transit while being sent to you. Your cards can also be compromised by a dishonest merchant who undertakes unauthorized duplicate transactions on your card.

Cheque frauds

[2][Cheque fraud is the use of cheque to get financial advantage by altering the cheque (payee/amount) without authority. Theft of legitimate cheques and then altering them. Duplication and counterfeiting of cheques.]$_2$ Depositing a cheque into a third party account without authority Depositing a cheque for payment knowing that insufficient funds are in the account to cover the deposited cheque. (commonly called Cheque bounce).Fraud signature attempts on Cheques.

Identity Theft

When person tries to get or reveal the personal information about someone for benefits or financial credit information, leaving you the owner of that identity often in large debt with a negative credit history and in some cases with legal implications and further illegal trading purposes also.Information can be obtained in many ways such as Internet, Phishing of mails from your mailbox or account related fraud messages (commonly known as self initiating messages analog) which initiates as soon as message gets opened. Information can be revealed by going through our garbage bins Telephone, Fax and Mail scams all can be used to assume your identity details like Date of birth, Utilities bills (phone, gas, water and rates notices) and addresses.

Electronic Frauds

A number of customers from financial institutions have been targeted with hoax emails. These emails appear to be genuine bank emails. Some emails inform the customer that their security details and passwords need to be updated by logging into an authentic looking, but fake website. The purpose of these websites is to obtain your log on details and to access your bank accounts.

Card Skimming

[2][Card Skimming is the illegal copying of a card's magnetic strip that can later be used to access your account and make unauthorized purchases using those details. In the case of ATMs, this typically occurs when the would-be thief places a device over the card entry point that scans the cards as they enter and exit the ATM, combined with a hidden camera to record you while you enter your PIN. The scanning device and camera can be cleverly disguised so that you don't even notice the ATM has been modified]$_2$

Lack in advance securities

As per the new advancements in banks and for other facilities banks provides us some security measures for transacting money and withdrawal of money from ATM cum associated from Our Banks And transactions Machines. There are some securities options with ease provided by the banks are as follows, but there are more prone to fraud activities.

- ATM security
- Card Security
- Online security
- ATM Security

Forensic banking investigations

- Visualization
- Cross sectioning
- Forensic accounting

- Use of anti spyware software.
- Other techniques

Visualization

The investigation leads to proper visualization and analyzing the severity of the fraud has been committed, all the documents must be checked verified and its authenticity question should be rectified and solved and further precede to other its concerned documents. Carefully read the instructions of bank or of that contract which to be signed by the authorities and by customer itself.

Cross Sectioning

A investigator in bank fraud should have a sound knowledge of the terms and terminology and different aspect of KYC forms related to the bank, he should divide the mode of transactions like withdrawal from cheque or by slip or online transaction, issue and purchase of dates, Daily budget system laid down by the bank, employees involved in each work, A proper sectioning of work and accounts sections should be studied and evaluated and should have a look on DDR, Daily Dairy Registers and their Maintenance.

Forensic accounting

3[Forensic Accounting helps the conventional accounting and auditing with the help of different accounting tools like ratio technique, cash flow technique, a standard statistical tool examination of evidences are all part of forensic accounting.]$_3$ In cases involving significant amounts of data, the present-day forensic accountant has technology available to obtain or source data, sort and analyst data and even quantify and stratify results through computer audit and various other techniques.

Use of anti spyware software

The running of anti spyware software for computer safety is considered to be just as important as having antivirus. This is because good anti spyware software for our computer should have for its own safety in the online world. Anti spyware just like antivirus software is designed for one purpose. The one purpose that anti spyware was created for was to detect and get rid of any bad anti spyware that installs itself on our computer without our knowledge. It is a specialized form of software that has its own mission statement and that mission statement is the eradication of any anti spyware software that downloads on to our computer mysteriously. Good anti spyware software fully protects a computer on all fronts from the invasion of any spyware software that can pose a serious threat to our computer and our identity. By the use of antispyware software it enables us so many facilities and security during transaction of money for goods shopping and other things. It gives benefits of safe banking and secured with privacy by using different security modules inbuilt in antispyware. Some of the security modules for safe & secured for online Security in transaction of bills through internet banking are listed below.

Security Modules

a. Encryption

[5][Encryption is turning words and numbers into a coded language. Encryption prevents unauthorized users from being able to change or read our data. It encrypts our personal data using 256-bit SSL (Secure Socket Layer) encryption technology.]$_5$ It can identify whether the Internet Banking session is secure or encrypted.

b. Fraud Identification Systems

There must be a sophisticated technology to monitor Internet Banking transactions and identify suspicious activity. [4][A Fraud Detection System looks for patterns of transactions and new behavior which may indicate that a transaction is fraudulent. If it detects fraudulent activity, then there is a attempt to contact and temporarily freeze the personnel Internet Banking access in order to prevent further fraudulent transactions.]$_4$

c. Automatic Time outs

[5][Within the Internet Banking system, banking session can remain unattended for a maximum of 15 minutes. After this time, the system automatically 'logs off' and ends your session. Remember, if we are not using our computer for a period of time; make sure to 'log out' completely from the Internet Banking system so that sensitive banking information cannot be viewed by others.]$_5$

Conclusion

In the age of the internet, it is incredibly easy for fraudsters to commit crimes related to internet banking and con people out of a great deal of money. Whilst phishing emails have always been something to be cautious of, methods of committing internet banking fraud are becoming ever more sophisticated, and we can never be too careful with your bank transactions.
An increasingly popular method of committing fraud is the production of fake documentation. Fraudsters send letters notifying companies of changes to banking details, and they're able to make the letters look incredibly convincing. Company logos, personnel names, signatures and many more features can all be replicated to make a document look legitimate. These fake letters will usually be sent to companies notifying them of changes to bank details, tricking them into paying money into the criminal's account instead. So, to avoid such type of fraudulent activity affecting we should never trust any documentation which inform to concerned bank for a change in bank details without conducting further investigation. With a special contrast to banks must have dedicated staff with more versatility and a deep knowledge of fraud investigation and a good awareness among its customers. When using internet security modules and internet banking options, customers should be well aware of procedure and passwords confidentially with steps and avoid to be a part of phishing by more use of anti spyware software.

REFERENCES

1. http://indianlawcases.com/Act-Indian Contract.Act,.1872-2340
2. http://www.anz.com/personal/ways-bank/security/online-security/threats-banking-safety/fraud-types/
3. Shaheen I, *et al*. 2012 " Forensic Accounting and Fraud Examinations in india" published in International Journal of Innovative Research and Development, Vol 3 issue 12(ISSN 2278-0211)
4. https://www.fbi.gov/scams-safety/fraud/internet_fraud
5. Website Australia and New Zealand Banking Group Limited (ANZ) 2015 ABN 11 005 357 522

****