ISSN:0975-9646

N.Sivakumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1379-1386

Fraud Detection in Credit Card Transactions: Classification, Risks and Prevention Techniques

N.Sivakumar[#1], Dr.R.Balasubramanian[*2]

[#1]*Research Scholar,* [*2] *Research Supervisor,*

PG and Research Department of Computer Science,
J.J. College of Arts and Science, Bharathidasan University,
Tiruchirappalli, Tamil Nadu, India.

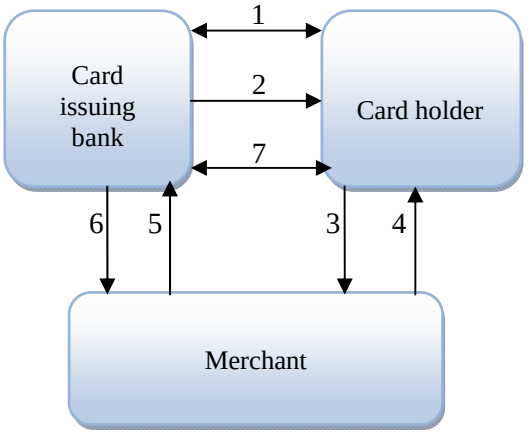
Abstract - Technological developments have changed the way we view money. 'Buy now and pay later, enjoy today and pay when able' with this in mind the Banks introduced the concept of credit cards. It provides cashless shopping at every shop in all countries. The advancement in the electronic commerce technology, the use of credit cards has increased and it becomes the popular mode of payment for both online and offline purchases. In spite of this enormous popularity the cards are not free of risk. Many FDS are exist but the efficiency of these system are in question only because they detect the fraudulent activity after the suspicious transaction is done. The role of banks and commercial organizations are important to develop an efficient FDS. This paper principally focuses the classification, numerous forms of fraud in the credit card by fraudsters and therefore the direction used to find the fraud in economical manner.

Keywords: FDS (Fraud Detection Systems), credit card.

I. INTRODUCTION:

Credit card is a plastic-card issued by a bank or non-banking financial company (NBFC) ready to lend money (give credit) to its customer. It is a suitable alternative for cash payment. It is used to execute transactions which are compiled through electronic devices like a card swapping machine, computer with internet facility, etc. Basically, it is a synthetic-card made from a laminated plastic sheet and other materials like paints, magnetic stripe, microchip (IC), gelatin, hologram, etc. It entitles (authorizes) the customers to buy goods and services, based on credit sanctioned to them. It shall be used among a prescribed credit limit. This limit relies on the earning capability. It gives a customer a suitable choice to plan payments for goods and services that may be most necessary to him on a day-to-day basis. By using it, customer promises the repayment of credit transactions executed by him. Such a repayment along with interest shall be paid to bank or NBFC at a later agreed date. Generally, repayments along with an applicable interest are made either after a period of 30-45 days or are done on a monthly billing basis.

Credit Card Operation:



1. Contract for credit card
2. Issue of Credit card
3. Purchasing goods
4. Deliver goods
5. Raising of bill
6. Payment for bills
7. Payment of Credit card

The credit card operation consists of the steps as follows:

1. Contract for credit card: there is a contract between cardholder and the cared issuing bank regarding limit etc.
2. Card issue: Once the contract is finished, the bank issues the credit card to their customer.
3. Purchasing goods: A Cardholder purchases goods/services and offers the credit card.
4. Deliver goods: A merchant establishment delivers goods once taking a valid credit card and noting the number and taking signatures.
5. Raising of bill: The merchant establishment raises the bill for the purchase and sends it to the credit card issuing bank for payment.
6. Payment for bill: The issuing bank pays the amount to the merchant establishment.
7. Payment of Credit card: The issuing bank raises bill on the credit cardholder and sends it for payment. The credit cardholder then pay the amount to the issuing bank.

Important basic terms and/or points associated with credit card are as follows:

1. Cardholder is somebody to whom a card is issued. The cardholder could also be a private or organisation. Here, issued suggests that licensed to create use of card.
2. I.S.O International standard Organization.
3. IEC is Electro-technical Commission.
4. NBFC could be a short-form of Non-Banking-Financial-Company.
5. ISO/IEC7810defines physical characteristics for identification cards.
6. ISO/IEC 7811 could be a set of 9 standards starting from 7811-1 to 7811-9. It specifies ancient knowledge recording techniques to be used on the magnetic stripe of ID-1 format identification cards.
7. ISO/IEC 7812-1 is specifies card listing system for identification cards. it's used to establish a card provision entity like a bank or NBFC.
8. ISO/IEC 7813 specifies structure and data content of Track1 and Track2. These tracks are placed on the magnetic stripe of an identification card and are used to begin money transactions.
9. Embossing could be a method within which raised numbers, letters, figures, etc., are adorned (i.e. craved) on an identification card.
10. Checksum could be a single-digit typically added at the end of a credit card number to visualize (validate) the legitimacy (genuineness) of it.
11. Credit Limit is that the maximum amount up to that a disposition entity like a bank or NBFC will lend (give) cash to its customers. it is further divided into 2 main varieties, viz., money withdrawal limit and credit-transaction limit.
12. Cash-withdrawal limit is that the most amount of money that may be withdrawn through a credit card.
13. Credit-transaction limit is that the most limit assail credit transactions (of purchases) that may be done through a credit card.
14. Usually, money withdrawal limit is a smaller amount than the credit transaction limit.

II. CLASSIFICATION OF CREDIT CARD:

1. Size of Credit Card

Standard size of credit card issued by a bank (or NBFC) is depicted below.

The average dimensions of a credit card in inches, mm and cm:

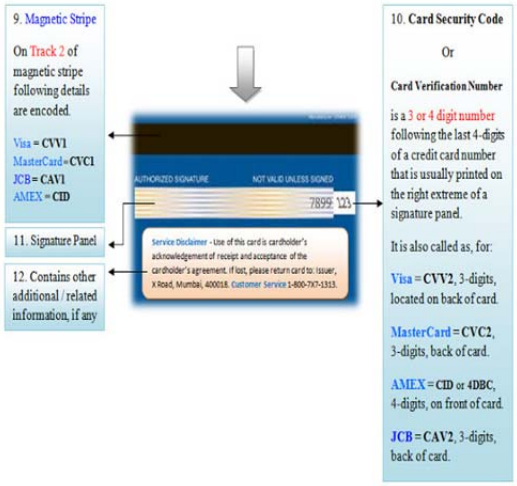
Credit card has a height of 2.125 inches (53.98 mm or 5.4 cm), width of 3.370 inches (85.60 mm or 8.5 cm). Its thickness is of 0.030 inch (0.76 mm or 0.076 cm). Its four corners (edges) are rounded with a circle of radius (r) measuring 0.125 inches (3.18 mm or 0.318 cm). The above measurements (sizes or dimensions) are averages of the maximum and minimum values defined for credit cards using ID-1 format of ISO/IEC 7810.

2. Anatomy of Credit Card:

Front side of a credit card is as follows:

1.Logo of issuing entity.
2.Logo of payment processor.
3.Hologram.
4.Expiration date.
5.Cardholder's name.
6.Card number.
7.Individual account identifier number.
8.Issuer identifier number (IIN).
9.Embedded microchip.
10.Major industry identifier (MII).
11.Issue date
12.Bank identification number (BIN).

Sample image of rear or back side of a credit card:



1.Security code (card verification number).
2.Magnetic stripe.
3.Signature panel.
4.Additional information.
5.Now let's discuss all details of credit card.

1. Logo of supplying entity

1. Logo is an emblem of the entity that issues a credit card so as to lend cash to its customers.
2. Its main purpose is to ease and aid instant public recognition of the issuer.
3. It's an emblem that helps folks quickly identify the name of bank or NBFC that has issued a credit-card.

2. Logo of payment processor

A bank issues a credit card unitedly with some payment process company. To point this tie-up, bank on its issued cards also puts a logo of its partnered card payment processor. Payment processor logo helps a cardholder to spot which payment processor will process and compile his credit card's transactions. It additionally helps him to decide on an applicable payment processor while shopping and filing payment forms. The below are some Credit card payment processor :

Visa, AMEX ,Credit card, JCB, Discover

3. Hologram

Hologram could be a 3D image either of an object, individual or some special image that has been projected and captured on a 2d flat surface.Important reasons why a photograph is employed on credit card:

1. hologram is principally used as a seal of originality.
2. It helps to authenticate a real brand from counterfeit one.
3. It aids in distinguishing an original credit card from pretend cards.
4. It acts as one of the protection measures to avoid and/or minimize forgery.

4. Card number

Card number may be a long and distinctive number assigned to a credit card. Often, it is raised (raised) on the face (front-side) of a card. Generally, it is 16-digits long and might be extended up to a maximum limit of 19-digits. an ISO/IEC 7812-1 card number is usually sixteen digits long and is grouped in four sets with four digits in every set.

Card numbering system consists of:

1. Major industry identifier (MII) digit value,
2. Bank identification number (BIN) now replaced with an issuer identifier number (IIN),
3. Individual account identifier, and
4. Checksum or check digit.

First single-digit (from left) of a credit card number could be a 'Major industry identifier (MII) digit value. It signifies the class or form of the entity that issued a card. MII value and issuer category is explained below:

0 is for ISO/TC 68 and other industry assignments, 1 is for Airlines, 2 is for Airlines and other future industry assignments, 3 is for Travel and entertainment and banking/financial, 4 is for Banking and financial, 5 is for Banking and financial, 6 is for Merchandising and banking/financial, 7 is for Petroleum and other future industry assignments, 8 is for Healthcare, telecommunications and other future industry assignment, 9 is for For assignment by national standards bodies.

First set of four-digits (which conjointly includes MII digit value) of a credit card range is referred as 'Bank positive identification (BIN)'. it\'s written in tiny fonts just under the cardboard range and is found on its front-left facet.

First-six digits of a credit card range (including the one MII digit value) represents an 'Issuer symbol range (IIN)' of a card issuance entity. it\'s needed to work within the world, inter-industry and/or intra-industry interchange.

As per ISO/IEC 7812-1, 'BIN is now replaced by IIN'. Following paragraph explains the explanation why IIN replaced BIN.

With the rising demand and recognition of credit cards, the monetary institutions opined the replacement of BIN with IIN. the aim of such replacement was to cover wider areas of monetary services, to bring various service suppliers under one roof and conjointly to ease their identification. The issuer identifier number consists of initial six digits when compared to Bank identification number , that consists of beginning four digits solely. The incorporated modification leads to a lot of prompt and proper help to compile and execute the credit card process.

Digits ranging from seventh position up to the second last position (7 to (n-1)) makes an IndividualAccountIdentifier. Here, n equals the total number of digits found in a credit card number.

For example, if n=16, then the individual account identifier number would begin from seven to (16-1) i.e. from seventh position to the fifteenth position.

The individual account identifier number may reach up to a most of 12-digits.

Final (last or ending) single-digit of a credit card number is understood as a 'Check Digit'. it's additionally referred to as as a 'Checksum'.

According to ISO/IEC 7812-1, the check digit or checksum may be a digit added to the end of a card number that helps to verify (confirm) its accuracy and/or validate its credibility (genuineness). Maximum of card numbers encoded with this digit use a LUHN Formula that depends on 'LUHN Algorithm'or a 'MOD-10 method'.

So ISO/IEC 7812-1 credit card numbering system offers details on the sort of industry, of an issuing entity, customer's data, check digit, etc.

5. Expiration date

Expiration date of a credit card is that the last date till that a card remains valid and might be used.

This final date of validity is additionally referred as 'VALID THRU' and is browse as 'valid through'.

It uses a mm/YY date format wherever MM implies a Month and YY stands for a Year.

For example, if 12/22 is mentioned on a credit card, then it's valid till twelfth month of year 2022 i.e. its 'VALID THRU' date is december 2022. In different words, we can|we are able to} say that the card will get expired and lose its usability on first january 2023.

6. Cardholder name:

Cardholder name is a given string of adorned or written alphabets on a credit card. It either mentions 1st and last name of an individual or specifies the registered name of a corporation, firm, or a corporation holding the account.

To complete on-line (the internet) transactions, it's necessary that name on the credit card should match its cardholder's name.

7. Embedded microchip

Embedded microchip is usually settled on the front side of a credit card.

Following are necessary features of microchip:

1. microchip is an electronic device that is often referred to as a semiconductor memory.
2. It acts as an increased protection shield of a card that safely stores confidential credentials of a cardholder. The credentials kept in an embedded microchip includes PIN details of a credit card supplying entity, etc.
3. It provides a comprehensive security to prevent cloning or duplication of a credit card.
4. It encrypts the sensitive information it stores. If hackers scan a credit card with some electronic spying device, then they'll solely fetch encrypted junk and not the initial info that microchip contains. This encrypted scrap is sort of useless to them as it is very troublesome to decode and misuse it intentionally.
5. it's a superior semiconductor memory and an honest processing capability.

Thus, it acts as a compulsory and essential security feature of a credit card.

8. Issue date

Issue date of a credit card is that the beginning date from when a card becomes valid and gets able to be used by cardholder.

This beginning date of card's validity is additionally referred as 'VALID FROM'.

As like an expiration date, issue date additionally uses a MM/YY date format.

For example, if 01/15 is mentioned on a credit card, then its validity started from the first month of year 2015 i.e. its 'VALID FROM' date is january 2015. In different words, we can say that the card became formally valid and got able to be used on first january 2015.

9. Magnetic stripe

Magnetic stripe is additionally sometimes known as as 'mag-stripe' or 'swipe card'. Generally, it's set on the rear side of a credit card. It comes in 3 completely different colors viz., black, brown, and silver. it's a storage device and is more internally divided into 3 horizontal stripes referred to as Track1, Track2, and Track3.

ISO/IEC 7811 specifies the traditional knowledge recording techniques to be used on the magnetic stripe of identification cards like credit cards.

According to this standard, the info recording density on track1, Track2, and Track3 should be 210bpi (bits per inch), 75bpi, and 210bpi, respectively. In different words, Track1, Track2, and Track3 should be 8.27bits per mm, 2.95bits per mm, and 8.27bits per mm, respectively.

The data recorded on track1 and Track2 of the magnetic stripe contains details of the cardholder's account. In different words, these tracks contain details of a credit card number, name of the cardholder, its ending date and also the issuer's country code.

1.Track1 largely contains record of an alphabetical value that is always a credit cardholder's name and his related data.

2. Track2 of magnetic stripe has CVV 1, CVC 1, CAV 1 and cid code.

3. Track3 is either non-existent or empty or might consist of some supplementary data regarding the credit cardholder and is hardly used for a few validation process.

Now with continuous improvement within the technology, magnetic stripes are getting obsolete as new contact-less credit cards are rising within the market.

10. Security code

Security Code is additionally referred as a card verification number or value. it's distinctive from any other number found on a credit card. Generally, it's a 3-digits number, however typically it may even be a 4-digits number.

Card security code offers an extra layer of security to the credit card. It helps to check and make sure the accessibility of the card. This stops an unauthorized card access and minimizes on-line frauds.

The card security code is named and abbreviated differently by various card payments processing corporations. Visa, Credit card, american express and JCB call it as CVV 2, CVC 2, CID, and CAV 2, respectively.

1. CVV 2 is an abbreviation of 'card verification value two'.
2. CVC 2 is an abbreviation of 'card validation code two'.
3. cid stands for a 'card identification number'.
4. CAV 2 is expanded as 'card authentication value two'.

In Visa, Credit card and JCB, card security code could be a 3-digits number and is mostly printed on the rear or back side of a credit card. However, just in case of american express, it's a 4-digits number that is typically printed on the face or front side of a credit card.

11. Signature panel

Signature panel may be a rectangular space located on the rear side of a credit card. because it name says, it's a reserved place wherever a cardholder should put or sign his approved signature. It should be signed by the holder with a decent permanent marker pen and a pen with blue or black should be used.

The below are something important for a signature panel:

1. it's an added feature for customization and security of a credit card.
2. It permits the merchants and/or traders to validate the credibility of person using a credit card. It helps them to cross check whether the physical-signature within the transaction invoice matches with the signature on the rear of a card.

It is necessary that signature panel should be signed properly else the credit card isn't thought-about as a legitimate. This message is warned on its top-right corner with written statement like,

"NOT VALID UNLESS SIGNED."

12. Additional information

Additional information is also printed on the rear side of a credit card. Mainly, it contains helpful details about; the

servicedisclaimer, official address of card issuing entity, and toll-free phone number for client service.

1. Service Disclaimer acts sort of a legal acknowledgement for an agreement on the terms and conditions between a credit card issuing entity and also the cardholder.
2. Address of an supplying entity provides official mailing or contact data of the bank or NBFC that issued a credit card to its client. If anyone is in possession of a lost and located card, then in such a case, this address helps a possessor to surrender the lost card to its original issuer.
3. client service is usually available via an official toll-free phone number. This service helps a cardholder to urge his card-related queries resolved, request an immediate further guidance (help) relating to usage of credit card, register complaints, alert frauds, and additionally to contact an issuer on numerous necessary matters arising on a every day basis.

III. CREDIT CARD RISKS:

Credit Card Fraud is one of the biggest threats to business institutions these days. However, to combat the fraud effectively, it is vital to initial perceive the mechanisms of executing a fraud. credit card fraudsters use a large variety of modus operandi to commit fraud. In simple terms, credit card Fraud is outlined as:

When a private uses another individuals' credit card for personal reasons whereas the owner of the card and also the card issuer are not aware of the actual fact that the card is getting used. Further, the individual mistreatment the card has no relation to the cardholder or establishment, and has no intention of either contacting the owner of the card or making repayments for the purchases created.

Types of Fraud:

Application Fraud:

This kind of fraud happens once someone falsifies an application to acquire a credit card. Application fraud is committed in 3 ways:

Assumed identity, wherever an individual illicitly obtains personal info of another person and opens accounts in his or her name, using partly legitimate info.

Financial fraud, wherever an individual provides false info regarding his or her
financial standing to acquire credit.

Not-received items (NRIs) additionally known as postal intercepts occur once a card is purloined from the postal service before it reaches its owner's destination.

Lost/ Stolen Cards:

A card is lost/stolen once a legitimate account holder receives a card and loses it or somebody steals the card for criminal functions. this sort of fraud is in essence the best way for a fraudster to get hold of alternative individual's credit cards without investment in technology. it is also maybe the toughest kind of ancient credit card fraud to tackle.

Account Takeover:

This type of fraud happens once a fraudster illicitly obtains a valid customers' personal info. The fraudster takes control of (takeover) a legitimate account by either providing the customers a/c.no or the cardnumber. The fraudster then contacts the card issuer, masquerading as the real cardholder, to ask that mail be redirected to a new address. The person who commit the fraud reports card lost and asks for a replacement to be sent.

Fake and Counterfeit Cards:

The creation of counterfeit cards, together with lost / stolen cards pose highest threat in credit card frauds. Fraudsters are perpetually finding new and additional innovative ways that to make counterfeit cards. a number of the techniques used for making false and counterfeit cards are listed below:

1. Erasing the magnetic strip: A fraudster can tamper an existing card that has been acquired illicitly by erasing the metallic strip with a powerful electromagnet. The fraudster then tampers with the details on the card so they match the details of a legitimate card, that they'll have earned, e.g., from a stolen until roll. once the fraudster begins to use the card, the cashier can swipe the cardboard through the terminal many times, before realizing that the metallic strip doesn't work. The cashier then proceed to manually input the card details into the terminal. this manner of fraud has high risk because the cashier will be viewing the card closely to read the numbers. Doctored cards are, like several of the traditional ways of credit card fraud, becoming an noncurrent technique of illicit accumulation of either funds or merchandise.
2. Making fake card: A fraudster will produce a fake card from scratch using sophisticated machines. This can be the foremost common variety of fraud although fake cards need lots of effort and talent to provide. Modern cards have several security measures all designed to create it troublesome for fraudsters to create good quality forgeries. Holograms are introduced in most credit cards and are terribly difficult to forge effectively. Embossing holograms on the card itself is another problem for card fraudster.
3. Altering card details: A fraudster will alter cards by either re-embossing them-by applying heat and pressure to the information} originally embossed on the card by a legitimate card manufacturer or by re-encoding them using computer software that encodes the magnetic stripe data on the card.
4. Skimming: Most cases of counterfeit fraud involve skimming, a method wherever real data on a card's magnetic stripe is electronically derived onto another. Skimming is quick rising because the most popular kind of credit card fraud. Employees/cashiers of business establishments are found to carry pocket skimming devices, a battery operated magnetic stripe reader, with that they swipe customer's cards to get hold of customer's card details. The fraudster does this while the client is waiting for the transaction to be valid through the card terminal. Skimming takes place unknown to the cardholder and is so terribly troublesome, if not impossible to trace. In alternative cases, the details obtained by skimming are used to carry out fraudulent card-not-present transactions by fraudsters. Often, the cardholder is unaware of the fraud till a statement arrives showing purchases they did not create.
5. White plastic: A white plastic may be a card-size piece of plastic of any color that a fraudster creates and encodes with legitimate magnetic stripe knowledge for illegal

transactions. This card looks like a chamber key however contains legitimate magnetic stripe knowledge that fraudsters will use at POS terminals that do not need card validation or verification.

Merchant related frauds are initiated either by owners of the merchant establishment or their workers. the kinds of frauds initiated by merchants are delineate below:

Merchant Collusion:

This type of fraud happens once merchant owners and/or their workers conspire to commit fraud using their customer's accounts and personal data. owners and/or their workers pass the information about customers to fraudsters.

Triangulation:

The fraudster in this kind of fraud operates from an internet website. product are offered at heavily discounted rates and also are shipped before payment. The dishonorable {site|website|web website} seems to be a legitimate auction or a traditional sales site. The client whereas inserting orders on-line provides info like name, address and valid credit card details to the site. when the fraudsters receive these details, they order product from a legitimate website using purloined credit card details. The fraudster then goes on to buy different product using the credit card numbers of the client. This method is designed to cause a good deal of initial confusion, and also the dishonorable internet company in this manner will operate long enough to accumulate vast quantity of products purchased with purloined credit card numbers.

The Internet has provided a perfect ground for fraudsters to commit credit card fraud in a straightforward manner. Fraudsters have recently begun to operate on a truly transnational level. With the enlargement of trans-border or 'global' social, economic and political areas, the web has become a brand new World market, capturing customers from most countries around the world. the foremost commonly used techniques in web fraud are delineate below:

1. Website cloning: web site cloning is wherever fraudsters clone a complete site or simply the pages from that you place your order. Customers haven't any reason to believe not handling the company that they needed to get merchandise or services from because the pages that they're viewing are identical to those of the real web site. The cloned or spoofed web site can receive these details and send the customer a receipt of the transaction via electronic mail just as the original company would. the consumer doubts nothing, while the fraudsters have all the details and to commit credit card fraud.

2. False merchant sites: These sites usually supply the client an especially low cost

service. the site requests a customer’s complete credit card details like name and address in return for access to the content of the site. Most of those sites claim to be free, however need a valid mastercard number to verify an people age. These sites are set up to accumulate as several credit cardnumbers as possible. The sites never charge individuals for the services they give. The sites are typically a part of a bigger criminal network that either uses little print|the main points} it collects to lift revenues or sells valid credit card details to small fraudsters.

3. Credit card generators: credit card number generators are computer programs that generate valid credit card numbers and ending dates. This generators work by generating lists of credit card a/c numbers from a single account number.this works by mishandling the mathematical Luhn algorithm that card issuers use to get alternative valid card number combos. The generators permit users to illicitly generate as several numbers because the user wishes.

IV. RECENT NEWS ABOUT FRAUDSTER:

1.4 Indians are among 10 people who have been charged in the US for their alleged participation in one of the largest credit card fraud schemes here, resulting in losses of $200 million.

2. The Reserve Bank of India (RBI) said that banks will have to bear the cost of fraudulent credit card transaction through point of sales that do not have prescribed security features.

3. Federal prosecutors said that they have charged five men responsible for a hacking and credit card fraud spree that cost companies more $300 million and 2 of the suspects in custody,in the biggest cyber crime case filed in the history of US.

4. A former BPO worker was arrested from his Southwest Delhi residence for allegedly using stolen credit card details to make purchases worth Rs 11 lakh from an e-commerce website — mydala.com.

5. Gurgaon Police said that they were looking for a third accused in a credit card fraud case. Police arrested 2 men, AkshitaAttri (27) and RahilArora(27).
   The 3 had allegedly misused the credit card of a United kingdom based man. Police said the trio conducted transactions cost Rs 10.85 lakh between October 2011 and April 2012.

6. 6 men were arrested for allegedly cheating people on the pretext of issuing them free credit cards and procuring loans on low interest rates. Police recovered fake account documents,driving licences,ATM cards,laptops,mobile phones and SIM cards from their possession.

7. 8 persons arrested by the Delhi Crime Branch for their criminal role in carrying out a credit card fraud operation from PrashantVihar. The accused men, divided into two groups,reportedly siphoned off close to Rs 35lakh from top private banks.

8. More or less half of the Indian plastic money coustomers are highly concerned about frauds in case,payments are done through credit/debit cards,while 73% are left shaken by media reports of such incidents said in a survey.
   With 46% respondents ‘extremely’ think about frauds related to payments through cards,consumers consider them as their biggest financial security regarding,according to the Visa Payment Card Security Study.

9. The West Delhi police arrested 7 men,including the assistant manager of a HDFC Bank branch,for their alleged involvement in cases of credit card fraud.
   The police received a complaint from the Rajouri Garden branch of the HDFC Bank regarding illegal use

of credit cards issued by the bank and withdrawal of Rs 9 lakh by unknown persons.

10. Two persons were arrested by the police for allegedly cheating showroom owners by using credit cards fraudulently. The two,Vicky Arora (28) and Vikas (25),are cousins and residents of Faridabad.

Police said the arrests were made following investigations into a complaint filed by Ritesh Chauhan,retail operation manager of Shoppers Stop showroom at Select Citywalk Mall in Saket on April 27. Chauhan told the police that two customers carrying American Express credit cards in the names of Mahender Ram and Pushpa Rani visited the store and purchased goods for Rs 2.77 lakh.

V. PREVENTION TECHNIQUES:

Keep all of your cards and financial details safe:

- look once your cards and card details at all times. attempt not to let your card out of your sight once making a transaction
- check receipts against statements rigorously. Contact your card company immediately if you discover an unfamiliar transaction
- Carry your cards separately from your pocketbook. It will minimize your losses if somebody steals your pocketbook or purse. And carry solely the card you need for that outing.
- Store your statements, receipts and financial documents safely and destroy them, preferably using a shredder, once you eliminate them
- Destroy expired cards through the magnetic strip and chip once replacement cards arrive.

Secure your PIN:

- Remember your PIN and destroy any paper notification.
- Ensure that you're the sole individual that is aware of your PIN. never write it or record it. Your bank/the police can never call you and raise you to disclose your PIN
- When entering your PIN, use your free hand and your body to defend the number from prying eyes or hidden cameras. If you think that somebody has seen your PIN or if you would like to change it to something a lot of memorable, you'll change it at a cash machine (ATM) or by contacting your bank.

Take care once using cash machines:

- Put your personal safety initial. If somebody causes you to feel uncomfortable, cancel the dealing and use a unique machine
- If you see something unusual in the cash machine, or if there are signs of damage, don't use it. Report it to the bank involved at once
- Be alert. If somebody is there and looking at you, delete the dealing and visit another machine. never accept help from seemingly well-meaning strangers and never permit yourself to be distracted
- Once you've completed a dealing, place your cash and card away before effort the cash dispenser. If the cash machine does not return the card, report it to your card company. Destroy or tear your cash receipt, mini-statement or balance enquiry.

Contact your bank as soon as possible if your card or personal info has been compromised.

- Never sign a blank receipt. Draw a line through any blank areas on top of the whole.
- Save your receipts to match together with your statement.
- Open your bills promptly — or check them on-line usually — and reconcile them with the purchases you've created.
- Report any questionable charges to the card establishment.
- Notify your card establishment if your address changes or if you'll be travel.
- You should not mention your account number on an envelope.

VI. CONCLUSION:

This paper presents classification of credit card the challenges faced by cardholder as well as the card issuer, verity of fraud implemented by the persons who commit that fraud, some latest news regarding credit card fraudster and provide some prevention techniques that should be followed by the cardholder against the fraudulent activity. In recent times credit cards becomes the most popular means of payment and if credit card transactions increase, so too do frauds. The good news is that technology for preventing credit card frauds is also increasing in recent times and reducing cost of computing helps in introducing complex systems, which can analyse a fraudulent activity in a matter of fraction of a second.

REFERENCES

[1]. Duncan M D G. 1995. The Future Threat of Credit Card Crime, RCMP Gazette, 57 (10): 25–26.

[2]. P Chan, W Fan, A Prodromidis & S Stolfo. 1999. Distributed data mining in credit card fraud detection, IEEE Intelligent Systems, 14(6): 67–74.

[3]. 2001. Fraud Prevention Reference Guide, Anonymous, Certegy, September 2001.

[4]. Bill Rini. 2002.White Paper on Controlling Online Credit Card Fraud, Window Six, January 2002. http://www.windowsix.com

[5]. Austin Jay Harris & David C Yen. 2002. Biometric Authentication- Assuring access to Information,Information Management & Computer Security, 10(1): 12–19.

[6]. Maguire S. 2002. Identifying Risks During Information System Development: Managing the Process, Information Management & Computer Security, 10(3): 126–134.

[7]. 2002. Card Fraud Facts 2002, APACS (Administration) Ltd, Association for Payment Clearing Services (APACS), April 2002. http://www.apacs.org.uk

[8]. 2002. Neural Network Basics Datasheet, IBEX Process Technology Inc, July 2002. http://www.ibexprocess.com/solutions/datasheeet_nn.pdf

[9]. 2002. ClearCommerce Fraud Prevention Guide, ClearCommerce Product Management, ClearCommerce Corporation, August 2002. http://www.clearcommerce.com

[10]. 2002. White Paper on Efficient Risk Management for Online Retail, ClearCommerce Product Management, ClearCommerce Corporation, September 2002. http://www.clearcommerce.com

[11] .N.Sivakumar, Dr.R.Balasubramanian "Credit Card Fraud Detection: Incidents, Challenges And Solutions" International Journal of Advanced Research in Computer Science and Applications.

[12]. Van Leeuwen. 2002. A Surge in Credit Card Fraud, H. Financial Review, 24 September, p.49.

[13]. 2002. Online Fruad Report – Online Credit Card Fraud Trends and Merchant's Response, Mindware Research Group, CyberSource. http://www.cybersource.com
[14]. Transnational Credit Card Frauds http://www.ex.ac.uk/politics/pol_data/undergrad/owsylves/index.html
[15]. Credit / Debt Management http://credit.about.com/cs/fraud/
[16]. Celent Communications http://www.celent.com
[17]. Recent news regarding fraud http://indianexpress.com/tag/credit-card-fraud/
[18] .N.Sivakumar, Dr.R.Balasubramanian "A Hybrid Algorithmic Approach for Fraud Detection in Online Transactions"International Journal of Advanced Research in Information and Communication Engineering.