AN OVERVIEW OF PLASTIC CARD FRAUDS AND SOLUTIONS FOR AVOIDING FRAUDSTER TRANSACTIONS

Jangam Upendar[1], Etikala Gurumohan Rao[2]

[1, 2] *Asst. Prof., Dept. of CSE, SwarnaBharathi College of engineering, AP, INDIA*
uppi24sr@gmail.com**, **gurumohanrao@gmail.com

Abstract

Payment card fraud is causing billions of dollars in losses for the card payment industry. Besides direct losses, the brand name can be affected by loss of consumer confidence due to the fraud. As a result of these growing losses, financial institutions and card issuers are continually seeking new techniques and innovation in payment card fraud detection and prevention. Credit card fraud falls broadly into two categories: behavioral fraud and application fraud. Credit card transactions continue to grow in number, taking an ever-larger share of the US payment system and leading to a higher rate of stolen account numbers and subsequent losses by banks. Improved fraud detection thus has become essential to maintain the viability of the US payment system. Increasingly, the card not present scenario, such as shopping on the internet poses a greater threat as the merchant (the web site) is no longer protected with advantages of physical verification such as signature check, photo identification, etc. In fact, it is almost impossible to perform any of the 'physical world' checks necessary to detect who is at the other end of the transaction. This makes the internet extremely attractive to fraud perpetrators. According to a recent survey, the rate at which internet fraud occurs is 20 to25 times higher than 'physical world' fraud. However, recent technical developments are showing some promise to check fraud in the card not present scenario. This paper provides an overview of payment card fraud and begins with payment card statistics and the definition of payment card fraud. It also describes various methods used by identity thieves to obtain personal and financial information for the purpose of payment card fraud. In addition, relationship between payment card fraud detection is provided. Finally, some solutions for detecting payment card fraud are also given.

***Index Terms**: Online Frauds, Fraudsters, card fraud, CNP, CVV, AVS*

----------***----------

1. INTRODUCTION

In the modern world, plastic cards are becoming the primary payment method for in person and online purchases. Due to the popularity of payment cards, the market for credit and debit cards is continuously growing. According to the U.S. Census Bureau, the number of U.S. credit and debit cards is expected to reach 585 and 1,278 million respectively in 2011. However, as the use of payment cards has become more widespread, so has the amount of fraud related to these cards? Fraudsters are becoming more organized and are using increasingly sophisticated methods to obtain and misuse consumer personal and financial information. Payment card fraud is causing billions of dollars in losses for the card payment industry. Besides direct losses, the brand name can be affected by loss of consumer confidence due to the fraud. As a result of these growing losses, financial institutions and card issuers are continually seeking new techniques and innovation in payment card fraud detection and prevention.

2. PAYMENT CARDS FRAUD: OVERVIEW

Technological and financial innovations in the payment industry affect consumers' choice of payment vehicles by offering more convenient payment methods. Consumers now use electronic payment methods more extensively than in the past. A recent Federal Reserve payments study found that in 2009 electronic payments exceeded three-quarters of all noncash payments, with sixty percent attributed to payments made with payment cards, such as debit, credit and prepaid cards.

Source: Federal Reserve Payments Study [1]

Exhibit 1: Number of Noncash Payments

	2006	2009	CAGR*
Total (billions)	**95.2**	**109.0**	**4.6%**
Checks (paid)	30.5	24.5	-7.1%
ACH	14.6	19.1	9.4%
Credit card	21.7	21.6	-0.2%
Debit card	25.0	37.9	14.8%
Prepaid card	3.3	6.0	21.5%

Figures may not add due to rounding.
*CAGR is compound annual growth rate.

As consumer spending patterns are changing, the global card market has expanded rapidly in recent years. Cards are useful and convenient for consumers, widely accepted by merchants, and one of the most efficient ways of payments. They have replaced cash and checks to a great extent. It is estimated that there are 10,000 payment card transactions made every second around the world. [2] According to data from the U.S. Census Bureau, there were 176 million credit card holders and 181 million debit card holders in the United States in 2008. These numbers are projected to grow to 183 and 188 million respectively in 2011[3]. The number of U.S. credit and debit cards continues to grow and is expected to reach 585 and 1,278 million respectively in 2011[4]. On the one hand, innovation in payments has resulted in greater consumer convenience and efficiency. On the other hand, innovations and new technologies also created more complexity and introduced new risks factors presented by new products, new providers, and new technologies. Unfortunately, as cards have become the primary payment vehicle in retail transactions, they have also become an enticing target for criminals. Payment card fraud existed since the introduction of cards into the payment system. As the card market has expanded rapidly in recent years, the fraud level associated with payment cards has increased as well. Each year, card fraud costs billions of dollars, and figures continue to rise. According to a report released in January 2010 by Aite Group LLC, "card fraud costs the U.S. card payments industry about $8.6 billion per year. Although just 0.4% of the $2.1 trillion in U.S. card volume per year, this number remains a troubling area for the industry due to the volatile nature of fraud"[5]. In addition to actual financial losses, payment card fraud affects consumer confidence in electronic payments systems and card-issuers' reputations. For example, Visa stated in its annual performance report (10K) "an increase in fraudulent and other illegal activity involving our cards could lead to reputational damage to our brands and reduce the use and acceptance of our cards"[6]. In the U.S., credit and debit card fraud is the number one fear. Concerns about fraud are greater than that of terrorism, computer and health viruses and personal safety. [7]
Payment card fraud is related to identity fraud and its definition can be derived from the identity fraud definition. As defined in the Javelin identity fraud survey report [8], identity theft occurs when someone's personal information is taken by another individual without explicit permission. Identity fraud is the actual misuse of information for financial gain and occurs when illegally obtained personal information is used to make payments, create new accounts and attempt to obtain services such as employment or health care. Therefore payment card fraud can be defined as a misuse of personally identifiable information obtained by another individual without explicit permission for financial gain. Modern fraudsters are organized professionals using increasingly sophisticated methods to capture cardholder account information. Criminals continue to develop new attack methods, using all kinds of sophisticated techniques [9].

3. METHODS OF IDENTITY FRAUD FOR THE PURPOSE OF PAYMENT CARD FRAUD

As defined earlier, payment card fraud is a misuse of personally identifiable information obtained by another individual without explicit permission for financial gain. There are numerous methods of identity theft committed for the purpose of payment card fraud. Here are some methods commonly used by the criminals to obtain personal information:

3.1. Lost or Stolen Wallet

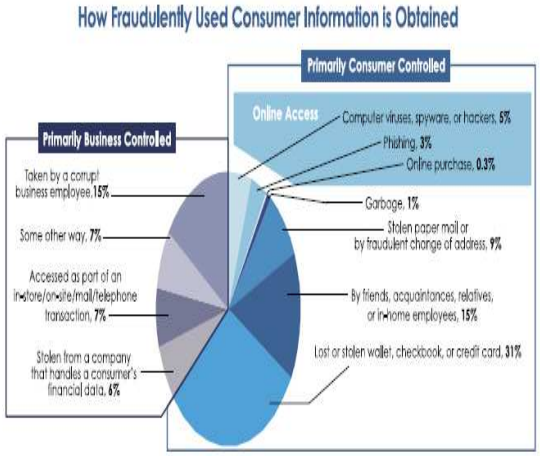
Most people carry bank cards and personal identification cards in their wallets. This information can be used to commit a fraud or it can be sold to criminals. As illustrated in Exhibit 2, payment card fraud is most often a result of a lost or stolen wallet or purse.

3.2. "Shoulder Surfing"

Identity thieves can simply use observation techniques, such as looking over someone's shoulder to obtain personal information when an unsuspecting individual fills out a form or uses a PIN number. Shoulder surfing is particularly effective in crowded places because it makes it easier to observe someone.

3.3. "Dumpster Diving"

Dumpster diving is one of the very popular methods used for identity theft. Thieves dig through trashcans or garbage dumpsters searching for pieces of personal information such as discarded trash for credit card offers, bank statements, medical statements and other papers that contain personal information. The average American uses 650 pounds of paper a year. Americans receive almost 4 million tons of junk mail every year [10] most of which goes to the landfill unopened. Carelessly thrown away documents, bills, credit card and banking statements, and other personal papers can make a public dumpster or a personal trash a goldmine of information for the identity thief. Besides consumers, businesses and organizations such as hospitals, accounting firms and profitable corporations discard millions of pounds of paper containing personal information. Not always are reasonable steps taken to destroy personal financial information and personal identification numbers issued by government entities. As a result, personal information ends up in the hands of criminals. The simple solution to the problem is to use a shredder to destroy documents and papers containing personal information that might be used by the fraudsters.



Note: The sample size was 182 respondents. The base was those who knew how their information was obtained.

Fig1: Javelin Strategy & Research

3.4. Mail Theft

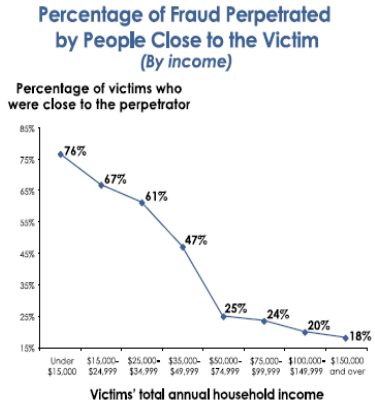
Fraudsters intercept mail to steal newly issued credit or debit cards, bank statements, credit offers, new checkbooks and tax forms. The theft of mail from businesses is also growing. Incoming and outgoing mail can contain checks, new checkbooks, financial records from the firm's CPA, bank cards and bank statements, employee payroll records and other important information.

3.5. Imposters

Thieves can pose as someone else to commit identity theft. For example, in a number of raids in California, discarded postal employee uniforms were found amongst bags of stolen mail, suggesting that impersonating mail carriers is an effective tactic for thieves. Another example is “pretesting” when criminals call a bank posing as a customer in order to find out personal information.

3.6. Home or Workplace

Unfortunately, family members, friends, co-workers and in-home employees can steal personal information in our homes and workplaces. As illustrated in Exhibit 3, Javelin Strategy & Research data indicates that quite often fraud victims personally knew the perpetrator, who was either a friend, relative, or in-home employee. This is especially true for fraud victims with less than $50,000 in annual household income. Such occurrences highlight the need for consumers to protect information not only at the point of transaction, but also in the home.



Note: The sample size was 182 respondents

Fig2: Javelin Strategy & Research

3.7. Inside Sources

As shown in Fig2, 15% of personal information obtained by identity thieves is received through corrupt and dishonest business employees with access to sensitive data such as personal records, payroll information, insurance files, account numbers, sales records, etc. Reports have shown that over 80% of financial institutions in the U.S. have been affected by employee fraud, and 65% recognize that the threat is becoming more serious.

3.8. Data Breaches

New technologies and the Internet have created new means for criminals to gain access to consumers’ personal information. One of the "high-tech" methods of identity theft is hacking. Some criminals have the ability to break into computer databases at e-commerce merchants, credit card processors, or payment gateway service providers to gain large scale access to customer personal information that can be used to commit payment card fraud. Databases at financial institutions, hospitals, retailers, government agencies, schools, libraries have all been breached, leaving millions of Americans potentially exposed to fraud involving compromised data. Several data breaches have been discussed in the media in the last few years. For example, in January 2007, the T.J. Maxx Company reported that 45.7 million credit and debit card numbers were compromised, along with 455,000 merchandise return records containing customers' driver's license numbers. In March 2007, nearly 8.6 million records of customer information were stolen from Dai Nippon printing company, including names, addresses, and credit card numbers. In January 2008, GE Money, which handles credit card operations for J.C. Penney and many other retailers, disclosed the loss of computer data backup tape containing 150,000 social security numbers and in-store credit card information from 650,000 retail customers. Heartland Payment Systems, one of the largest payment processors in the U.S., announced

that its processing systems were breached in 2008 by self-taught computer hacker, Albert Gonzalez. The breach impacted an estimated 130 million credit/debit cards - the largest such incident ever reported. The most recent massive data breach was experienced by Sony Corporation in 2011. The breach resulted in the theft of personal data for more than 100 million online accounts. Data breaches are not always a result of computer hacking. A significant number of data losses happen due to logistical difficulties in handling consumer information. For example, data can be misplaced by employees, exposed through an error, or lost in transport. Therefore, attention should be paid to how data is stored, transported and handled.

3.9. Skimming

The most commonly known type of payment card fraud involves skimming card details. Skimming is copying the data held in the magnetic strip on the back of the payment card. This data is then used to make purchases where the card itself is not present or to replicate the card. This type of crime is hard to detect, as victims may not be aware of fraudulent payments until their next statement arrives. Skimming can occur both at the point-of-sale (especially in restaurants, bars and gas stations where the card is often out of the cardholder's control for some time) as well as at ATM machines. A corrupted employee would use your card with an unauthorized device that records the data contained on the magnetic strip. Alternatively, the skimming device might be fitted around the card entry slot of a cash machine so that the card's data is copied when it is inserted into the ATM machine. A pinhole camera is placed above the PIN pad, so that the PIN is also recorded for use in a fraudulent transaction. Skimmed data is often collected from hundreds of cards and sold to criminal organizations who then manufacture the cloned cards. In 2010, a skimming ring was broken up in Boston, Massachusetts. Five men were accused of skimming bank cards from ATM machines and then withdrawing money. The men allegedly withdrew approximately $146,000 from customers of Citizens Bank, Wells Fargo Bank and BNY Mellon Bank, according to court papers. A T.G.I Friday's restaurant waiter in Coon Rapids, West St. Paul, Minnesota was arrested for skimming customers' payment cards. His skimming scam affected at least 15 victims with losses totaling in excess of $30,000

3.10. Phishing

More sophisticated criminals are "fishing" for personal and financial information through phishing schemes. Although the loss from phishing is relatively low, it is one of the fastest growing crimes on the Internet. Phishing involves creating authentic-looking emails that appear to be from legitimate businesses, such as an Internet service provider (ISP), bank, online payment service, or even a government agency. These e-mails might include official-looking logos and marketing slogans and other identifying information taken directly from legitimate websites. They also might include convincing details about your personal history that criminals found on your social networking page. The e-mail often describes a situation that requires immediate attention and includes threat of account closure unless the recipients "verify", "update", "validate," or "confirm" their account information immediately by clicking on a provided web link. Consumers then are re-directed to a bogus website, where victims are persuaded into providing sensitive information, including account information, usernames or passwords, Social Security numbers, credit/debit card number, CVV code, ATM card PIN, place of birth, mother's maiden name and other identifiable information. There are some new versions of phishing such as "smishing" and "vishing". A smishing scam involves SMS text messages instead of e-mail. As in traditional phishing, the victim is told that an urgent matter needs to be discussed. The text redirects the victim to a legitimate looking website that asks you to "confirm" your personal or financial information, or instructs the recipient to call a toll-free number for confirmation. A phone number normally directs victims to a legitimate sounding automated voice response system, similar to the voice response systems used by many financial institutions, which will ask for the same personal and financial information. Vishing is another form of phishing and uses a combination of e-mail and telephone, or just telephone. Just like with online phishing attacks, which direct consumers to phony web sites, recipients of the scam e-mails or recorded phone messages are instructed to call a toll-free number where victims are lured to provide personal and financial information. Because most people are more apt to trust text messages and phone messages than suspicious-looking emails, smishing and vishing provide fraudsters another area for attack.

3.11. Social Networking

Social networking websites such as Face book, Twitter, MySpace, LinkedIn and Flicker are growing in popularity. As of November 2009, more than half of all U.S. consumers indicated they have used or are using social networking sites. Social networking brings millions of people together around the world; however, it also creates new opportunities for cyber-crime. Banking and payments activity on the social networking web sites has attracted the attention of criminal hackers, fraudsters, spammers and scammers. There are many dangers in social networking. One of them is that personal pages can expose sensitive, personally identifiable information that can be used by fraudsters to commit identity theft. Identity thieves are spending a lot of resources and time on these networks and, because of this, the danger of social networking has taken a sharp increase in the last few years. Another danger is that most people use the same password to get into work computers, email accounts, online bank accounts, Face book and other social networking web accounts. "Crooks understand that most users use the same password for everything," says Tom Clare, head of product marketing at Blue Coat, an Internet security company that does annual

reports on web threats. "If they can get your user credentials for your Face book account, there is a good chance that they have the password for your bank account." People tend to trust social networking sites more than in any other online activities because these sites are built for helping people to make friends and to communicate. However, privacy and security controls are weak on these websites. Therefore, identity thieves will continue to target social networking sites to get personal information. Phishing scams are quite common on Face book. They appear as Face book games and quizzes.

4. CATEGORIES OF PAYMENT CARD FRAUD

Payment card fraud comes in a variety of forms. The most commonly known type involves skimming card details. However, as payment systems have experienced a number of changes and the use of credit and debit cards has risen, payment card fraud has become more sophisticated and more widespread. According to the Aite Group report on card data security "the greatest threats to the card industry are malware, counterfeit card fraud and CNP (card-not-present) fraud". Commonly known types of payment card fraud are:

4.1. Credit Card Application Fraud

Credit card application fraud is a form of identity fraud and occurs when a criminal uses victim's personal information to obtain a credit card in the name of a legitimate user and upon receiving the card uses it without the victim's knowledge. This may occur if a criminal can obtain enough personal information about the victim to completely fill out the credit card application, or is able to create convincing counterfeit documents. This form of fraud is difficult to detect and often results in large fraud amounts and serious difficulties for re-establishing the victim's credit history. Consumers can prevent this type of fraud by regularly monitoring their credit reports for activity or accounts that are not immediately recognized.

4.2. Account Takeover

Account takeover happens when fraudsters try to take over an existing account, first by obtaining personal information about the victim, and then contacting their card issuer while impersonating the legitimate cardholder to notify of address change and asking for mail to be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent. Bank statements also will be sent to this new address, making victims unaware of the fraud.

4.3. Lost or Stolen Cards

This type of fraud is the oldest form of payment card fraud used by criminals. When criminals obtain cards, either because they were lost or because they were stolen, they can impersonate the victim in order to buy goods and services, whether in person or online. As shown in Exhibit 4, the most common methods of fraud used by criminals are through making in□store and online purchases.

Identity Fraud Survey Report: Consumer Version.

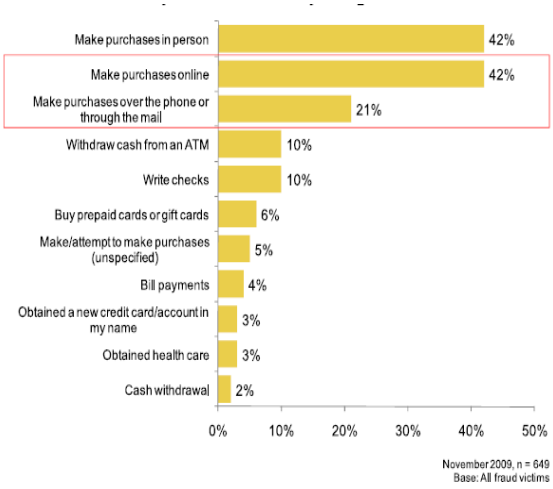


Fig3: Common Methods of Payment Card Fraud

4.4. Card-not-Received Fraud

Card-not-Received fraud occurs when legitimate cards are intercepted while in transit between manufacturer and cardholder. Losses attributable to card-not-received fraud have declined as a result of card activation programs, where cardholders must contact their financial institution to confirm their identity. The bank runs a series of security questions before the card is activated. These security questions aim to confirm certain details of the individual, such as date of birth, address, mother's maiden name and other personal details that the issuer may have on file regarding the account holder.

4.5 Counterfeit Cards

A counterfeit, cloned or skimmed card is one that has been printed, embossed or encoded with genuine card details. Card details are obtained from data breaches, card skimming, or purchased from other criminals. As described earlier, skimming is a process where card data on the agnatic strip is copied electronically onto another card. Organized criminals are now using the latest computer devices (embossers, encoders, and decoders often supported by computers) to read, modify, and clone magnetic strip information on counterfeit payment cards. Counterfeit cards can be used anywhere from ATM cash withdrawals to in-person transactions at a point-of-sale. In 2009, eight foreigners were indicted on charges of card fraud. Thieves hacked into computer system at RBS World Pay Inc., the U.S. payment processing division of Royal Bank of Scotland Group PLC, and stole account and PIN numbers for 44 prepaid payroll accounts, which were used by companies to distribute salaries to debit cards. Then they cloned prepaid ATM cards, which thieves then used to

withdraw $9.4 million cash from 2,100 ATMs in 280 cities around the world, including in the U.S. The unprecedented coordinated operation took no more than 12 hours.

4.6. ATM Fraud

According to Javelin Strategy & Research, in 2009, 10% of fraud victims in the U.S. were victims of fraudulent ATM withdrawals (Exhibit 4). This usually involves skimming devices being installed in the ATM machines. Besides skimming and using cloned cards at the ATM, there are other forms of card fraud that occur at ATM machines. One of them is called “Lebanese loop”. Lebanese loop is a deceptive tactic where the criminal inserts a device made of bent metal, plastic, or videotape sleeve into the ATM machine leaving only a tiny flap sticking out. When the victim uses the machine, the card becomes trapped when inserted. The criminal then tricks victim into entering the PIN in their presence, while they 'help' to fix the machine. When the victim leaves to report the broken ATM machine, the criminal returns to the ATM, disables the device, removes the card and using the PIN, withdraws funds. Another ATM fraud involves 'shoulder-surfing'. A criminal will watch a victim enter a PIN number at the machine by looking over the victim’s shoulder, then steal the card by distracting the victim or pick-pocketing and withdraw money from the victim’s account. The losses from these low-tech methods are usually limited to daily withdrawal amounts.

4.7. Card-not-Present Transaction

Card-not-present transaction (CNP) is a transaction made using a payment card that is not physically present at the point-of-purchase. It could be a mail order/telephone order (MOTO) or an online sale. As these types of transactions are becoming more popular with customers, they are also creating many opportunities for credit card fraud. In CNP transactions, perpetrators do not need a physical card to make a purchase. In transactions made in-person, customers using a credit card may authenticate themselves by providing a signature that also authorizes the transaction. Customers using a debit card can authenticate themselves and authorize the transaction by providing a personal identification number (PIN) or by providing a signature. In card-not-present transactions there is no opportunity to physically check the card to determine its authenticity or the identity of the cardholder, therefore there is always some risk of payment fraud. Fraud committed without the actual use of a card accounts for more than 60% of fraud cases according to Javelin Strategy & Research (Exhibit 4). To confirm the consumer’s identity in the CNP transaction, the merchant can require the customer to provide information such as name of card holder, billing address, account number, expiration date, and the card security code/verification value (CVV) that is imprinted on the card. In fraud committed in connection with card-not-present transactions, criminals are often using stolen account information resulting from security breaches of systems that store cardholder or account data, including systems operated by merchants, financial institutions and other third-party data processors. Underground payment card shops and illegal websites are set up by criminals to sell compromised payment card data. These shops are advertised in fraudsters’ forums and accessible to registered users. Initially, these shops were offering information obtained through data breaches or skimming devices. However, as “demands” grew, other information, such as full identities including SSN, addresses, account information, e-mail accounts, commonly used passwords, and mother’s maiden names became available. According to Symantec, stolen credit card information is available at a cost as low as 6 cents when they are purchased in bulk. Bank account credentials are sold at a cost of $10 to $1000 per account number. Vladislav Horohorin, arrested in 2009, was managing such underground websites for hackers. He used criminal forums such as “CarderPlanet” and “carder.su” to advertise stolen data and directed buyers in the buying process. "The network created by the founders of CarderPlanet, including Vladislav Horohorin, remains one of the most sophisticated organizations of online financial criminals in the world," Michael Merritt, assistant director for investigations at the Secret Service, said in a statement, "This network has been repeatedly linked to nearly every major intrusion of financial information reported to the international law enforcement community.”

5. DETECTION AND PREVENTION

5.1. Impact of Payment Card Fraud

Interestingly enough, cardholders are the least affected party in the card fraud. This is due to the fact that cardholder liability is limited. However, there are some differences in the liability amounts for credit and debit cards. Cardholder’s maximum liability under federal law for unauthorized use of their credit card is $50. The liability under federal law for unauthorized use of the ATM or debit card depends on how quickly the cardholder reports the loss. If a stolen/lost card was reported before it is misused, the card issuer cannot hold the cardholder responsible for any unauthorized transfers. If unauthorized use occurs before a stolen/lost card was reported, the liability under federal law depends on how quickly the loss is reported. For instance, if the loss is reported within two business days after the card went missing, the cardholder will not be responsible for more than $50 for unauthorized use. However, if the loss is not reported within two business days after the loss was discovered, the liability can be up to $500 because of an unauthorized transfer. There is a risk of unlimited loss in case a cardholder fails to report an unauthorized transfer within 60 days after the bank statement containing unauthorized use is mailed to him/her. Because debit cards, like checks, access checking accounts, in this unfortunate case, a cardholder can lose all the money in the checking account. However, for unauthorized transfers involving only debit card number (not the loss of the card), the liability occurs only for transfers that take place after 60 days

following the mailing of the bank statement containing the unauthorized use and before the loss was reported. Merchants are the most impacted party in payment card fraud, especially in CNP transactions where merchants cannot inspect cards for authenticity or confirm that a customer has possession of the card. According to a 2009 LexisNexis Risk Solutions report, U.S. merchants are incurring $100 billion in fraud losses due to unauthorized transactions and fees associated with charge backs, nearly 10 times the identity fraud cost incurred by financial institutions. Payment card issuer losses remain relatively well-contained despite the continuing evolution of card fraud. Loss of consumer confidence can be devastating. As fraud continues to grow, issuers are forced to increase their investments in new technology to better protect against fraud.

5.2. Fraud Prevention and Detection

Preventing fraud can be achieved by using a number of anti-fraud techniques and practices, such as card activation, card verification codes, consumer education, address verification services, and real-time POS authorization, to name but a few. In card-present transactions, the merchant can verify the validity of the payment information provided be the customer by verifying both the cardholder's identity and the card's authenticity. Payment card fraud becomes more difficult when point-of-sale (POS) is chip-enabled. The Chip and PIN verification should help to reduce card fraud. The chip on the card verifies the authenticity of the card and the PIN verifies the cardholder. Use of PIN number is more secure than using a signature. While solutions such as the EMV card standard or PIN technology have been introduced in most European countries, as well as in Canada and Mexico, it is not commonplace in the U.S. Chip and PIN cards have been proven to be successful in reducing certain types of fraud such as lost/stolen card and use of counterfeit cards. However, in card-not-present transactions, they are not useful. In CNP transactions, there can be signs that indicate that fraud is involved such as first time shopper; unusual quantities of order, items with high resale value, multiple transactions on one card over a very short period of time, etc.Merchants should train their personnel to recognize fraud indicators. Being able to recognize suspicious orders may be particularly important for merchants involved in telephone sales; therefore, employees should be given clear instructions on the steps to verify these transactions.

New techniques developed to reduce fraud in CNP transactions include Card Verification (CVV2/CVC2) and the Address Verification Service (AVS). Address Verification Service (AVS) verifies the cardholder's billing address on file with the card issuer. However, if a fraudster knows the victim's address, the address verification fails to prevent fraud. Card Verification Value/Code compares the card security value/code, the 3- or 4-digit numeric code on the payment card, with the issuer's value on file. This helps to verify that the customer is in physical possession of a valid card during a card-not-present transaction.

Visa and MasterCard offer 3D authentication such as "Verified by Visa" and "Secure Code". MasterCard Secure Code and Verified by Visa enable cardholders to validate themselves to their card issuers through the use of personal passwords they create when they register their cards with the programs. To address issue of data breaches and mass data compromise, the Payment Card Industry Security Standards (PCI DSS) have been developed. All organizations that transmit, store or process credit card data must be compliant with the requirements of the PCI standard, which sets the rules for data security management, policies, procedures, network architecture, software design and other protective measures.

5.3 Technology Solutions

Detecting fraud is essential once prevention mechanisms have failed. There are a number of algorithmic solutions for fraud detection. These include data mining techniques such as decision trees, clustering techniques, and artificial neural and Bayesian networks. For example, consider a decision tree-based classification approach. The goal is to train a decision tree to detect various types of fraud. In the simple case, the decision tree would learn to detect whether the patterns are a fraudulent activity or not. That is, the decision tree will be trained to recognize one of two classes: Yes to mean that it is a fraudulent activity and No to mean it is a benign activity. Then the decision tree is tested with the test data and it will detect whether the activity is fraudulent or not. More sophisticated decision trees can be built to detect multiple classes. That is, in the case of fraudulent activity, the tree would detect the type of fraud, such as credit card fraud or bank account fraud.

One issue with data mining solutions is the existence of false positives and negatives. Due to fact that the amount of data to be processed is often very large, the techniques have to extract only the useful features and carry out the training. This will likely result in false positives and false negatives. Therefore, a major goal of the data mining researchers and developers is to reduce the number of false positives and negatives.

CONCLUSIONS

This paper first provided an overview of payment card fraud which began with payment card statistics and the definition of payment card fraud. It then described various methods used by identity thieves to obtain personal and financial information for the purpose of payment card fraud. Next an overview of fraud types was given. This was followed by a discussion of payment card fraud as a type of terrorist financing. Finally, prevention and detection techniques including data mining solutions were discussed. As more and more of the financial and other data are digitized, the opportunities for payment card fraud will continue to increase exponentially. Furthermore, the thieves are also getting more and more

sophisticated and learning new fraudulent techniques. They are also trained to thwart the defensive mechanisms imposed. That is, the adversary will learn the patterns utilized by the solutions and attempt to develop methods to thwart the solutions. Therefore, in addition to the technological solutions, we also need to learn the behavior of the adversary. Appropriate game theoretic strategies have to be investigated so that we can win the games against the thieves. Ultimately, we need to develop and integrate solutions that will use data mining, risk analysis, game theory and adversarial learning so that we can be one step ahead of the thieves, hackers and the terrorists.

REFERENCES

[1]. 2010 Federal Reserve Payments Study. December 2010.
[2]. Sources: American Bankers Association, March 2009. Quoted at creditcards.com
[3]. U.S. Census Bureau's, Statistical Abstract on the United States: 2011.
[4] S.Benson Edwin Raj, A. Annie Portia, ―Analysis on Credit Card Fraud Detection Methods‖, IEEE March 2011
[5] M.Hamdi Ozcelik, Mine Isik, ―Improving a credit card fraud detection system using Genetic algorithm‖, IEEE 2010.
[6] Genetic algorithms for credit card fraud detection by Daniel Garner, IEEE Transactions May 2011.
[7].Kearns M. and Mansour Y., A fast, bottom-up decision tree pruning algorithm with near-optimal generalization, in J. Shavlik,ed., 'Machine Learning:
[8].Proceedings of the Fifteenth International Conference', Morgan Kaufmann Publishers, Inc., pp. 269-277, 1998.
[9].Kearns M. and Mansour Y., on the boosting ability of top-down decision tree learning algorithms. Journal of Computer and Systems Sciences, 58(1): 109-128, 1999.Kohavi R.
[10].Duncan M D G. 1995. The Future Threat of Credit Card Crime, RCMP Gazette, 57 (10): 25–26.

BIOGRAPHIES

J. Upendar Received M. Tech in Web Technologies from JNTU, Hyderabad and now presently working as Assistant Professor Dept of CSE, Swarna Bharathi College of Engineering, and Khammam. His research interests include Mobile Computing, Image Processing, Data Mining, Computer Networks and Software Engineering.

E. Gurumohan Rao Received M. Tech Computer Science and Engineering from JNTU, Hyderabad. B. Tech in Computer Science & Engineering from KU, Warangal. And now presently working as Associate Professor, Dept of CSE, Swarna Bharathi College of Engineering, Khammam .His research interests includes Mobile Computing, Image Processing, Data Mining and Computer Networks