Episteme: an online interdisciplinary, multidisciplinary & multi-cultural journal

Bharat College of Commerce, Badlapur, MMR, India

Volume 2, Issue 2 **September 2013**

PLASTIC CARD FRAUDS

SUBMITTED BY:

PROF. REEMA PANJWANI

QUALIFICATIONS: NET, MMS, M.COM

SMT. CHM COLLEGE

EMAIL: reemapanjwani1@gmail.com

Contact: 9890460604

INTRODUCTION

Card Fraud is a phenomenon when an individual uses another individuals' credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. Further, the individual using the card has no connection with the cardholder or issuer, and has no intention of either contacting the owner of the card or making repayments for the purchases made.

Card frauds are committed in the following ways:

- ✓ An act of criminal deception (mislead with intent) by use of unauthorized account and/or personal information
- ✓ Illegal or unauthorized use of account for personal gain
- ✓ Misrepresentation of account information to obtain goods and/or services

State-of-the-art thieves are concentrating on plastic cards. In the past, this type of fraud was not very common.

Today, it is a big business for criminals. Plastic cards bring new convenience to your shopping and banking, but they can turn into nightmares in the wrong hands.

Credit and Debit Cards

• ***ATM card****:* A card that allows the consumer to make purchases from a savings or transaction account using their own funds. An ATM card requires a Personal Identification Number (PIN) when making purchases or withdrawing funds

• ***Debit card:*** A card that allows a consumer to make purchases from a savings or transaction account both in Australia and overseas. A debit card requires the consumer to enter a PIN, provide a signature or quote the card details.

• ***Credit card:*** A card that allows the consumer to establish a line of credit with the card issuer for purchases both in India and overseas. Similar to a debit card, these cards require the consumer to

enter a PIN, provide a signature or quote the card details. There are also credit charge cards such as American Express and Diners Club.

Credit cards, debit cards, and other plastic cards such as "stored-value" cards may look alike. However, if a card is lost, stolen, or otherwise compromised, the similarities end there. Out-of-pocket loss could be nothing. Or, a thief could drain the entire bank account. It all depends on the kind of card one uses and the instances of reporting the loss.

Debit cards typically put consumers at much greater risk than credit cards because they offer less legal protection in the event of a loss. And because debit cards access funds directly from your bank account, your money will remain missing while you and your bank sort out any theft, which could mean bounced checks, late fees, and numerous other problems.

However, debit cards have the largest share of the retail point of sale market by purchase volume, followed closely by credit cards. It is also true that debit and credit cards will continue to dominate market share and will pull dollar volume from traditional paper-based payment options including cash and checks.

Personal desires and the specific situation may influence ones decision about how to pay. But, still, one needs to be sufficiently informed about various payment options to make a prudent decision.

Thieves have become increasingly sophisticated in gaining access to sensitive financial information. Databases of major retailers and restaurants have been compromised by hackers. Merchant card reading devices have been surreptitiously replaced with card skimmers. Restaurant employees have secretly captured card information on hand-held card readers. If you have a debit or check card and your account information is compromised, funds can quickly be withdrawn from your bank account without your knowledge. Your account can be emptied, resulting in overdrafts, fees, and an inability to pay your bills.

On the other hand, credit card will have an opportunity to dispute a fraudulent transaction before you have to pay the bill, so you will still retain access to the funds in your bank account.

Reporting misuse of ATM or debit card

The EFT Act requires the bank to investigate within the following timeline:

- The bank must investigate and resolve your complaint within **45 days**.
- For errors involving new accounts (opened in the last 30 days), point-of-sale transactions, and foreign transactions, the bank may take up to **90 days** to investigate the error.
- If the bank takes **longer than 10 business** days to complete its investigation, generally it must put back into your account the amount in question while it finishes the investigation. For new accounts, the bank may take up to **20 business days** to credit your account for the amount you think is in error.
- If it finds no error, the bank must explain in writing why it believes no error occurred and let you know that it has deducted any amount re-credited during the investigation. One may ask for copies of documents relied on in the investigation.

The important thing to note is that the bank is not obligated to restore the funds to a particular person's account for 10 or 20 business days while it investigates. During this time period, a person may not have funds available in bank account to pay mortgage, rent, loans, or other bills.

Episteme: an online interdisciplinary, multidisciplinary & multi-cultural journal

Bharat College of Commerce, Badlapur, MMR, India

Volume 2, Issue 2 **September 2013**

SOURCES OF CARD FRAUDS AND PREVENTIVE MEASURES

Although credit and debit card fraud can take many forms, the following examples explain some situations to watch for.

1. **Stolen Cards at the Office**

   Over the lunch hour when a person leaves the office for lunch, he could be the target of a credit card thief. Credit card thieves often gain illegal access to the offices of employees who are away in order to search unattended.

   Most times, they leave the offices and immediately go on a shopping spree, charge credit cards to their limits, and withdraw cash on debit cards.

   Protect your credit cards as you would cash. Never write your PIN number on your debit card. Instead, always commit your PIN number to memory.

2. **Extra Copies of Charge Slips**

   When processing your credit card, a dishonest merchant may decide to imprint a few extra copies of the charge slip. Later, the merchant can submit these copies to the issuing institution for payment on phony charges.

   Keep your eye on your credit card whenever it is in use. Watch clerks process your credit payments. Open your credit card bills promptly each month. Make sure that you made the listed purchases. Also, report any charges that you did not make to the credit card company.

3. **Discarded Charge Slips**

   Sometimes, people may collect copies of one's discarded charge slips from the wastebasket. Dishonest people could use the information from the copies to order merchandise by mail and ship it to a phony address. In addition, they could also sell the copies to counterfeiters who would take the account numbers and use them to alter cards or make new ones.

   After signing a credit card slip, ask for your receipt or duplicates. After you have compared them to the charges listed on your monthly credit card statement, tear them up and throw them away.

4. Unsigned Credit Cards

Stealing and using credit cards that have not been signed is another potential fraud. In other words, credit card thieves could steal unsigned credit cards and then sign a person's name on the card in their handwriting. By doing so, they take the name as an alias and they will never have a problem writing and verifying their own signature.

Protect your credit cards. When you receive a new or replacement card, sign the back of it as soon as it is activated.

Always be sure to store it in a safe place. Cut up expired cards before disposing of them.

5. Loss of Multiple Cards

While shopping, one can easily be targeted by pickpockets. If a person's purse or wallet is stolen, he may lose all your credit cards at one time.

Separate your cards. Only carry those cards with you that you plan to use. Also, check your cards from time to time and put aside those cards you don't use very often.

6. Strange Requests for Your PIN Numbers

This form of fraud involves thieves who find creative ways to steal credit or debit cards when one don't know about it. For example, sometimes people crawl behind rows in movie theaters and steal pocketbooks while one is watching a movie. When returning home they call you, identify themselves as bank security agents, and ask for PIN numbers. If one hesitates, they simply ask to phone their supervisor and give you an accomplice's phone number to call. By doing so, they are able to get PIN numbers and use the stolen debit cards to withdraw cash and make purchases.

Again, never reveal your PIN number to anyone. Also, never keep your PIN number in your purse or wallet. Don't write your PIN on your card either. Always try to memorize it.

CARD RELATED FRAUDS

- **APPLICATION FRAUD**

This type of fraud occurs when a person falsifies an application to acquire a credit card.

Application fraud can be committed in three ways:

- Assumed identity, where an individual illegally obtains personal information of another individual and opens accounts in his or her name, using partially legitimate information.
- Financial fraud, where an individual provides false information about his or her financial status to acquire credit.
- Not-received items (NRIs) also called postal intercepts occur when a card is stolen from the postal service before it reaches its owner's destination.

- **LOST/ STOLEN CARDS**

A card is lost/stolen when a legitimate account holder receives a card and loses it or someone steals the card for criminal purposes. This type of fraud is in essence the easiest way for a fraudster to get hold of other individual's credit cards without investment in technology. It is also perhaps the hardest form of traditional credit card fraud to tackle.

- **ACCOUNT TAKEOVER**

This type of fraud occurs when a fraudster illegally obtains a valid customers' personal information. The fraudster takes control of (takeover) a legitimate account by either providing the customers account number or the card number. The fraudster then contacts the card issuer, masquerading as the genuine cardholder, to ask that mail be redirected to a new address. The fraudster 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 poses highest threat in credit card frauds. Fraudsters are constantly finding new and more innovative ways to create counterfeit cards. Some of the techniques used for creating false and counterfeit cards are listed below:

1. Erasing the magnetic strip: A fraudster can tamper an existing card that has been acquired illegally by erasing the metallic strip with a powerful electro-magnet. The fraudster then tampers with the details on the card so that they match the details of a valid card, which they may have attained, e.g., from a stolen till roll. When the fraudster begins to use the card, the cashier will swipe the card through the terminal several times, before realizing that the metallic strip does not work. The cashier will then proceed to manually input the card details into the terminal.
This form of fraud has high risk because the cashier will be looking at the card closely to read the numbers. Doctored cards are, as with many of the traditional methods of credit card fraud, becoming an outdated method of illicit accumulation of either funds or goods.

2. Creating a fake card: A fraudster can create a fake card from scratch using sophisticated machines. This is the most common type of fraud though fake cards require a lot of effort and skill to produce. Modern cards have many security features all designed to make it difficult for fraudsters to make good quality forgeries.
Holograms have been introduced in almost all credit cards and are very difficult to forge effectively. Embossing holograms onto the card itself is another problem for card forgers.

3. Altering card details: A fraudster can 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 process where genuine data on a card's magnetic stripe is electronically copied onto another.
Skimming is fast emerging as the most popular form of credit card fraud.
Employees/cashiers of business establishments have been found to carry pocket skimming devices, a battery-operated electronic magnetic stripe reader, with which they swipe customer's cards to get hold of customer's card details. The fraudster does this whilst the customer is waiting for the transaction to be validated through the card terminal. Skimming takes place unknown to the

cardholder and is thus very difficult, if not impossible to trace. In other 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 until a statement arrives showing purchases they did not make.

5. White plastic: A white plastic is a card-size piece of plastic of any color that a fraudster creates and encodes with legitimate magnetic stripe data for illegal transactions. This card looks like a hotel room key but contains legitimate magnetic stripe data that fraudsters can use at POS terminals that do not require card validation or verification (for example, petrol pumps and ATMs).

- **MERCHANT RELATED FRAUDS**

Merchant related frauds are initiated either by owners of the merchant establishment or their employees. The types of frauds initiated by merchants are described below:

1. Merchant collusion

This type of fraud occurs when merchant owners and/or their employees conspire to commit fraud using their customers' (cardholder) accounts and/or personal information.

Merchant owners and/or their employees pass on the information about cardholders to fraudsters.

2. Triangulation

The fraudster in this type of fraud operates from a web site. Goods are offered at heavily discounted rates and are also shipped before payment. The fraudulent site appears to be a legitimate auction or a traditional sales site. The customer while placing orders online provides information such as name, address and valid credit card details to the site. Once fraudsters receive these details, they order goods from a legitimate site using stolen credit card details. The fraudster then goes on to purchase other goods using the credit card numbers of the customer. This process is designed to cause a great deal of initial confusion, and the fraudulent internet company in this manner can operate long enough to accumulate vast amount of goods purchased with stolen credit card numbers.

- **INTERNET RELATED FRAUDS**

The Internet has provided an ideal ground for fraudsters to commit credit card fraud in an easy manner. Fraudsters have recently begun to operate on a truly transnational level. With the expansion of trans-border or 'global' social, economic and political spaces, the internet has become a New World market, capturing consumers from most countries around the world. The most commonly used techniques in internet fraud are described below:

1. Site cloning: Site cloning is where fraudsters clone an entire site or just the pages from which you place your order. Customers have no reason to believe they are not dealing with the company that they wished to purchase goods or services from because the pages that they are viewing are identical to those of the real site. The cloned or spoofed site will receive these details and send the customer a receipt of the transaction via email just as the real company would. The consumer suspects nothing, whilst the fraudsters have all the details they need to commit credit card fraud.

2. False merchant sites: These sites often offer the customer an extremely cheap service. The site requests a customer's complete credit card details such as name and address in return for access to the content of the site. Most of these sites claim to be free, but require a valid credit card number to verify an individuals age. These sites are set up to accumulate as many credit card numbers as possible. The sites themselves never charge individuals for the services they provide. The sites are usually part of a larger criminal network that either uses the details it collects to raise 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 expiry dates. These generators work by generating lists of credit card account numbers from a single account number. The generators allow users to illegally generate as many numbers as the user desires, in the form of any of the credit card formats, whether it be American Express, Visa or MasterCard.

RECOGNISING FRAUDS

- **Legitimate Cards**

  Legitimate cards follow standard specifications as to color, tint, quality, and style. Stamped letters and numbers are spaced evenly and sized equally. The signature panel is uniform in size and is almost impossible to scrape off.

- **Altered Cards**

  Altered cards are made from actual cards. The original stamped data is melted down or pressed out. Then, the card is re-stamped with legitimate account numbers, names, and expiration dates, which have been illegally obtained. On altered cards, the letters do not line up well and are usually irregular in size. Some credit card companies help merchants identify altered cards by making an authenticator machine available to merchants.

  The machine authenticates or verifies certain information that is encoded on the back stripe on the back of the card.

- **Counterfeit Cards**

  Counterfeiters make most counterfeit cards by silkscreening or painting the card logo and issuing institution's name onto a blank piece of card plastic. Because they are silkscreened, the cards don't look exactly like the real thing. Real credit cards are printed. Also, the signature panel on silkscreened cards may be glued or painted on and can be easily lifted or chipped. This panel may also appear uneven in size or placement.

- **New Technology**

  New technology is making it more difficult for criminals to use, alter, or counterfeit credit and debit cards.

  Some of the innovations are already in use.

  These security features have been added to major credit cards:

1. **Holograph** – a three-dimensional, laser produced optical device that changes its color and image as the card is tilted.
2. **Fine-line printing** – a repeated pattern of the card company name positioned as background for the company logo.
3. **Ultra-violet ink** – special ink that is visible only under ultra-violet light, which will display the credit card company's logo.

"Smart Cards" may be the credit cards of the future. Each card has a built-in computer microprocessor. Signatures have been replaced with personal identification numbers and verification is handled only by computers.

Eventually these cards may provide information on investments, charge accounts, and money market accounts.

We may someday think of the credit card as a pocket-sized computer memory bank.

Improved verification methods are also being developed and tested. These include fingerprinting, retinal eye scanners, and computerized signature cards.

What is the Law?

The Credit Card Fraud Act imposes prison sentences and stiff fines on persons convicted of unauthorized or counterfeit use of credit cards and debit cards. Also, the law makes it a federal crime to use any unauthorized card, plate, code, or account number to obtain money, goods, or services. The Secret Service is authorized to investigate violations under this act.

Impact of Fraud on Cardholders

It's interesting to note that cardholders are the least impacted party due to fraud in credit card transactions as consumer liability is limited for credit card transactions by the legislation prevailing in most countries. This is true for both card-present as well as card not-present scenarios. Many banks even have their own standards that limit the consumer's liability to a greater extent. They also have a cardholder protection policy in place that covers for most losses of the cardholder. The

cardholder has to just report suspicious charges to the issuing bank, which in turn investigates the issue with the acquirer and merchant, and processes chargeback for the disputed amount.

Impact of Fraud on Banks (Issuer/Acquirer)

Based on the scheme rules defined by both MasterCard and Visa, it is sometimes possible that the Issuer/Acquirer bears the costs of fraud. Even in cases when the Issuer/Acquirer is not bearing the direct cost of the fraud, there are some indirect costs that will finally be borne by them. Like in the case of chargebacks issued to the merchant, there are administrative and manpower costs that the bank has to incur.

The issuers and acquirers also have to make huge investments in preventing frauds by deploying sophisticated IT systems for detection of fraudulent transactions.

SUGGESTED MEASURES

• Allow customers to select their own Personal Identification Numbers, to reduce the chance of their writing down their number in a document that is likely to be stolen or looked at (even perhaps by people in their own household) with their card.

• Reduce telecommunications and terminal costs, which are the key to increased on-line authorization.

• Encourage on-line card authorization mechanisms and technology to vary floor limits from remote terminals, making it more difficult for fraudsters (including store staff) to predict safe card expenditures.

• Introduce laser-engraved Payment Authorization Cards with photographs, which will reduce the number of people who can passoff cards as their own. We cannot be certain, however, that this will bring net benefits to financial institutions.

• Improve staff training and encourage the retaining of suspect cards. Setting 'charge-backs' from the banks for invalid signatures against the individual store manager's performance targets may encourage them to train staff properly. Staff also needs greater awareness of what aspects of the card are validated by the authorization process.

• Tighten controls over merchants by acquirers, checking them against collective 'terminated merchant' files and, if appropriate, obtaining merchants' photographs. Also, continuous monitoring of merchants' accounts to prevent them passing counterfeit vouchers (including those of numbers obtained by telemarketing) through their stores.

CONCLUSION

As card business transactions increase, so too do frauds. Clearly, global networking presents as many new opportunities for criminals as it does for businesses. While offering numerous advantages and opening up new channels for transaction business, the internet has also brought in increased probability of fraud in credit card transactions.

The good news is that technology for preventing credit card frauds is also improving many folds with passage of time. Reducing cost of computing is helping in introducing complex systems, which can analyze a fraudulent transaction in a matter of fraction of a second.

It is equally important to identify the right segment of transactions, which should be subject to review, as every transaction does not have the same amount of risk associated with it. Finding the optimally balanced 'total cost of fraud' and other measures outlined in this article can assist acquiring and issuing banks in combating frauds more efficiently.

REFERENCES:

1. 2002. Card Fraud Facts 2002, APACS (Administration) Ltd, Association for Payment Clearing
2. Services (APACS), April 2002. http://www.apacs.org.uk

3. 2002. Neural Network Basics Datasheet, IBEX Process Technology Inc, July 2002. http://www.ibexprocess.com/solutions/datasheeet_nn.pdf