Overview of Fraud Prevention & Management

Rashmi G.Dukhi
G.H.Raisoni Institute of Information Technology
Nagpur,India

Sandhya Dahake
G.H.Raisoni Institute of Information Technology
Nagpur,India

ABSTRACT
Credit Card Fraud is one of the biggest threats to business establishments today. To combat the fraud effectively, it is important to first understand the mechanisms of executing a fraud. The purpose of this white paper is to study different types of frauds,how fraudsters attempt to take advantage of loopholes,impact of credit card fraud on card holders, merchants, issuers, fraud detection system could help maintain the cost of detecting fraud techniques, how skimming works & use of Neural networks in fraud detection.

Keywords
counterfeit ; doctored cards ; embossing holograms ; Redbox; kiosks

1. INTRODUCTION TO FRAUD TECHNIQUES
Visa has taken care security measures in building its cards, some criminals have still managed to make copies of legitimate credit cards by copying or "skimming" the data contained in a card's magnetic stripe.Using this "skimmed" information, criminals manufacture phony or counterfeit cards and use them for fraudulent purposes.There are many ways in which fraudsters execute a credit card fraud.

2. TYPES OF FRAUD
Frauds can be broadly classified into three categories, i.e., traditional card related frauds, merchant related frauds and internet frauds. The different types of methods for committing credit card frauds are described below:

A.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:

1.Assumed identity, where an individual illegally obtains personal information of another individual and opens accounts in his or her name, using partially legitimate information.

2.Financial fraud, where an individual provides false information about his or her financial status to acquire credit.

3.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.

B.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.

C.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.

D.Fake and Counterfeit Cards-The creation of counterfeit cards, together with lost / stolen cards pose 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.The details obtained by skimming are used to carry out fraudulent card-not-present transactions by fraudsters. 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).

3. FRAUD MANAGEMENT

Fraudsters are using sophisticated methods to gain access to credit card information and perpetrate fraud, new technologies are available to help merchants to detect and prevent fraudulent transactions. Fraud detection technologies enable merchants and banks to perform highly automated and sophisticated screenings of incoming transactions and flagging suspicious transactions[5].

A.Manual Review-This method consists of reviewing every transaction manually for signs of fraudulent
activity and involves a exceedingly high level of human intervention. This can prove to be very expensive, as well as time consuming. It is unable to detect some of the more prevalent patterns of fraud, such as use of a single credit card multiple times on multiple locations (physical or web sites) in a short span.

B.Address Verification System-This technique is applicable in *card-not-present* scenarios. Address Verification System (AVS) matches the first few digits of the street address and the ZIP code information
given for delivering/billing the purchase to the corresponding information on record with the card issuers. A code representing the level of match between these addresses is returned to the merchant. AVS is not much useful in case of international transactions.

C.Card Verification Methods-The Card Verification Method3 (CVM) consists of a 3- or 4-digit numeric code printed on the card but is not embossed on the card and is not available in the magnetic stripe. The
merchant can request the cardholder to provide this numeric code in case of *card-notpresent* transaction and submit it with authorization. The purpose of CVM is to ensure that the person submitting the transaction is in possession of the actual card, since the code cannot be copied from receipts or skimmed from magnetic stripe.CVM provides some protection for the merchant, it doesn't protect them from transactions placed on physically stolen cards. Fraudsters who have temporary possession of a card could, in principle, read and copy the CVM code.

D.Risk Scoring Technologies-Risk scoring tools are based on statistical models designed to recognize fraudulent transactions, based on a number of indicators derived from the transaction characteristics. These tools generate a numeric score indicating the likelihood of a transaction being fraudulent: the higher the score, the more suspicious the order. Risk scoring systems provide one of the most effective fraud prevention tools available. The primary advantage of risk scoring is the comprehensive evaluation of a transaction being captured by a single number. Individual fraud rules typically evaluate a few simultaneous conditions, a risk-scoring system arrives at the final score by weighting several dozens of fraud indicators, derived from the current transaction attributes as well as cardholder historical activities. E.g., transaction amounts more that three times the
average transaction amount for the cardholder in the last one year.

The second advantage of risk scoring is that, while a fraud rule would either flag or not flag a transaction, the actual score indicates the degree of suspicion on each transaction. Transactions can be prioritized based on the risk score and given a limited capacity for manual review, only those with the highest score would be reviewed.

E.Biometrics-Biometrics is the name given to a fraud prevention technique that records a unique characteristic of the cardholder like, a fingerprint or how he/she sign his/her name, so that it can be read by a computer. The computer can then compare the stored
characteristic with that of the person presenting the card to make sure that the right person has the right card.Biometrics, which provides a means to identify an individual through the verification of unique physical or behavioral characteristics, seems to supercede PIN as a basis for the next generation of personal identity verification systems.There are many types of biometrics systems under development such as finger print verification, hand based verification, retinal and iris scanning and dynamic signature verification.

4. SKIMMING

In credit card skimming schemes, thieves use a device to steal credit card information in an otherwise legitimate credit or debit card transaction[2]. For example, credit card skimming devices are often placed on ATMs or even held in the hands of waiters and store employees. When a credit card is run through a skimmer, the device stores the credit card information. Thieves use the stolen data to make fraudulent charges either online or with a counterfeit credit card. In the case of ATM and debit cards, thieves withdraw cash from the linked checking account. Credit card skimmers are even popping up on Redbox movie rental kiosks.Victims of credit card skimming are often unaware of the theft until they receive a billing statement or overdraft notices in the mail.

A.Detection of Credit Card Skimming-Credit card skimming incidents are difficult to detect since the credit cards are never lost or stolen. The best way to detect a skimmed credit card is to watch your accounts frequently. Monitor your checking and credit card accounts online daily and immediately report any suspicious activity.

Fig. 1 Skimming machine

5. DETECTION OF FRAUD USING NEURAL NETWORKS

Neural networks are used to solve a wide variety of problems, some of which have been solved by existing statistical methods, and some of which have not. These applications fall into one of the following three categories:

• *Forecasting*: predicting one or more quantitative outcomes from both quantitative and categorical input data,

• *Classification*: classifying input data into one of two or more categories, or

• *Statistical pattern recognition*: uncovering patterns, typically spatial or temporal, among a set of variables.

Problems of forecasting, pattern recognition and classification are not new.

Neural networks are an extension of risk scoring techniques. They are based on the 'statistical knowledge' contained in extensive databases of historical transactions, and fraudulent ones in particular. These neural network models are basically 'trained' by using examples of both legitimate and fraudulent transactions and are able to correlate and weigh various fraud indicators (e.g., unusual transaction amount, card history, etc) to the occurrence of fraud.

A neural network is a computerized system that sorts data logically by performing the following tasks:

1 Identifies cardholder's buying and fraudulent activity patterns.

2.Processes data by trial and elimination (excluding data that is not relevant to the pattern).

3.Finds relationships in the patterns and current transaction data.

The principles of neural networking are motivated by the functions of the brain – especially pattern recognition and associative memory. The neural network recognizes similar patterns, predicting future values or events based upon the associative memory of
the patterns it has learned.The advantages neural networks offer over other techniques are that these models are able to learn from the past and thus, improve results as time passes. They can also extract rules and predict future activity based on the current situation. By employing neural networks effectively, banks can detect fraudulent use of a card, faster and more efficiently.

6. FUTURE SECURITY ISSUES

Card security is itself another area that can be improved upon[1]. Criminal networks can and have produced fake credit cards that are of exceptional quality. Individuals can purchase both number embossing machines and hologram printing machines via the Internet. The future of actually card security lies with the hologram. These cards not only print the hologram on the entire surface of the card, but also print holograms that are semi-transparent as shown in figure 2. A combination of this type of card, along with greater electronic protection will be the likely appearance of cards in the future.

Fig. 2 Cards with hologram

7. REFERENCES

[1] Transnational Credit Card Frauds

http://www.ex.ac.uk/politics/pol_data/undergrad/owsylves/index.htm

[2].Credit / Debt Management http://credit.about.com/cs/fraud/

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

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

[5].2001. *Fraud Prevention Reference Guide*, Anonymous, Certegy, September 2001.

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

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

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

[9].2002. *White Paper on Efficient Risk Management for Online Retail*, ClearCommerce Product Management, ClearCommerce Corporation, September 2002. http://www.clearcommerce.com

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

[10].2002. Online Fruad Report – Online Credit Card Fraud Trends and Merchant's Response, Mindware Research Group, CyberSource. http://www.cybersource.com

[11] Hansen, J. V., McDonald, J. B., Messier, W. F., & Bell, T. B. A generalized qualitative – response model and the analysis of management fraud. *Management Science,* 42(7), 1022-1032, 1996.

[12] Martin, D. Early warning of bank failure: A logit regression approach. *Journal of Banking and Finance,* 1, 249–276, 1997.

[13] Ohlson, J.A. Financial ratios and probabilistic prediction of bankruptcy. *Journal of Accounting Research,* 18(1), 109–131, 1980.

[14] Quinlan J.R. C4.5 Programs for Machine Learning, *Morgan Kaufmann*, San Mateo, CA. 1993.

[15] Quinlan J.R. Introduction to decision trees. *Mach Learning;*1(1):81–106, 1986.

[16] Rumelhart D.E. McClelland J.L. Parallel Distributed Processing. *Experiments in the Microstructure of Cognition*, MIT Press, Cambridge, MA, 1986.

[17]M.J. Kim and T.S. Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," Proc. Int'l Conf.Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002.