Cards Business Review#2003–01

Understanding Credit Card Frauds

Tej Paul Bhatla, Vikram Prabhu &
Amit Dua

June 2003

CONTENTS

OVERVIEW

Introduction

Credit Card Fraud is one of the biggest threats to business establishments today. However, to combat the fraud effectively, it is important to first understand the mechanisms of executing a fraud. Credit card fraudsters employ a large number of modus operandi to commit fraud. In simple terms, Credit Card Fraud is defined as:

> 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.

Credit 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.

Contrary to popular belief, merchants are far more at risk from credit card fraud than the cardholders. While consumers may face trouble trying to get a fraudulent charge reversed, merchants lose the cost of the product sold, pay chargeback fees, and fear from the risk of having their merchant account closed.

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 12 to 15 times higher than 'physical world' fraud. However, recent technical developments are showing some promise to check fraud in the *card not* present scenario.

Purpose of this Paper

The purpose of this white paper is to study:

- State of the credit card industry,
- Different types of frauds,
- How fraudsters attempt to take advantage of loopholes,
- Impact of credit card fraud on card holders, merchants, issuers,
- How a comprehensive fraud detection system could help maintain the cost of detecting fraud, and
- Losses due to fraud, i.e., the total cost of fraud, under manageable levels.

While the focus of the document will be mostly on Visa and MasterCard type transactions, the concepts and ideas generally prove valid with other credit cards such as American

Express and Discover also.

Current State of the Industry

While the exact amount of losses due to fraudulent activities on cards is unknown, various research analyst reports concur that the figure for year 2002 probably exceeds $2.5 billion. Further, as the overall e-commerce volumes continue to grow and fraudsters adopt more complex schemes, the projected figure for losses to internet merchants in the US alone is expected to be in the range of $5–15 billion by the year 2005[1]. This again is dependent on how rapidly fraud prevention technology will be adopted by the industry. The incidence of fraud for credit card transactions taking place over the internet is according to Garner G2[2], nearly 15 times higher than face-to-face transactions.

The increased likelihood of fraud, in conjunction with the full economic liability for fraud losses makes risk management one of the most important challenges for Internet merchants worldwide.

How Fraud is Committed Worldwide?

While lost or stolen card is the most common type of fraud, others include identity theft, skimming, counterfeit card, mail intercept fraud and others. Table 1 summarises the modus operandi for credit card frauds and their percentage of occurrence.

Method	Percentage
Lost or stolen card	48%
Identity theft	15%
Skimming (or cloning)	14%
Counterfeit card	12%
Mail intercept fraud	6%
Other	5%

Table 1: Methods of Credit Card Fraud and their percentage of occurrence
Source: Celent Communications, January 2003

Amongst the high risk countries facing Credit Card Fraud menace, Ukraine tops the list with staggering 19% fraud rate closely followed by Indonesia at 18.3% fraud rate. Also in the list of high risk countries are Yugoslavia (17.8%), Turkey (9%) and Malaysia (5.9%). Surprisingly United States, with its high number Credit Card transactions, has a minimum fraud rate.

Over the last few years, the credit card industry in UK was subjected to maximum threat from increasing fraud losses. Table 2 shows the worrying trend in volume of credit card frauds in UK over the last few years.

[1] Source: Fighting Fraud on the Internet: An Advanced Approach, *Meridian Research*, September 1999

[2] Source: Online Transaction Fraud and Prevention Get More Sophisticated, *Garner G2,* January 2002

Fraud Category	2000	2001	% Change
Counterfeit	107.1	160.3	+50
Card-not-present	72.9	95.7	+31
Lost/stolen card	101.9	114.0	+12
Intercepted in post	17.7	26.7	+51
Fraudulent application	10.5	6.6	+37
Other	6.9	8.0	+15
Totals	317.0	411.4	+30
Losses as % of turnover	0.162	0.183	+13

Table 2: Trend of fraud categories in UK for 2000–2001 (in Pound Sterling millions)
Source: APACS, March 2002

Stolen and counterfeit cards together contribute to more than 60% of fraud losses according to figures published by both MasterCard and Visa in Figure 1.

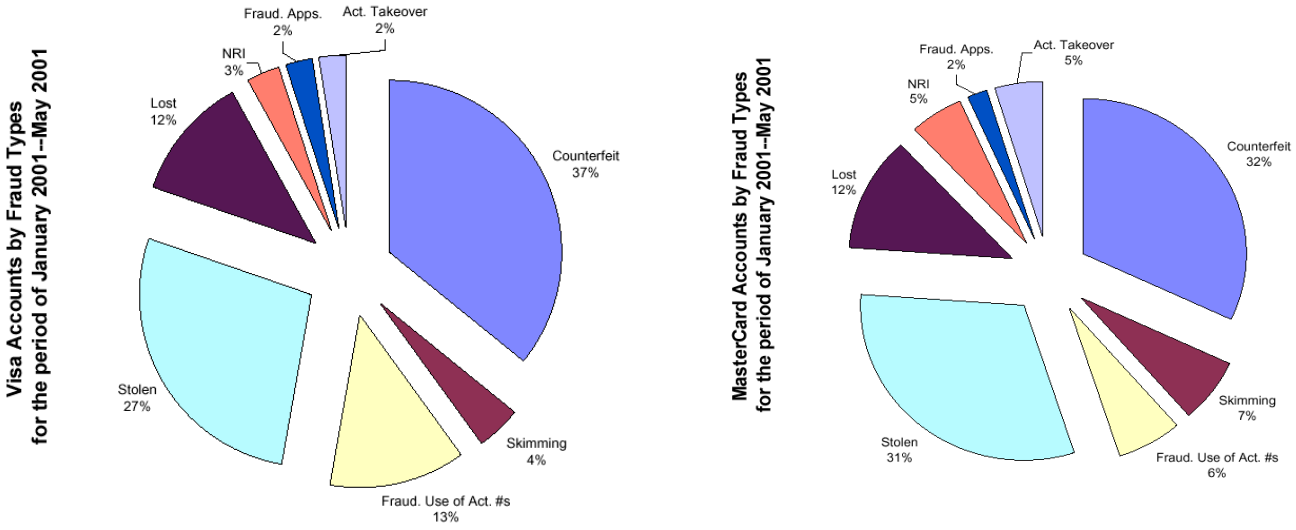

Figure 1: Visa & MasterCard accounts by fraud types for year 2001 (January to May)
Source: APACS, March 2002

FRAUD TECHNIQUES

As indicated above, there are many ways in which fraudsters execute a credit card fraud. As technology changes, so do the technology of fraudsters, and thus the way in which they go about carrying out fraudulent activities. 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:

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 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. 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:

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.

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 software works by using the mathematical Luhn algorithm that card issuers use to generate other valid card number combinations. 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.

IMPACT OF CREDIT CARD FRAUDS

Unfortunately, occurrences of credit card frauds have only shown an upward trend so far. The fraudulent activity on a card affects everybody, i.e., the cardholder, the merchant, the acquirer as well as the issuer. This section analyses the impact that credit card frauds have on all the players involved in transacting business through credit cards.

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 Merchants

Merchants are the most affected party in a credit card fraud, particularly more in the *card-not-present* transactions, as they have to accept full liability for losses due to fraud. Whenever a legitimate cardholder disputes a credit card charge, the card-issuing bank will send a chargeback to the merchant (through the acquirer), reversing the credit for the transaction. In case, the merchant does not have any physical evidence (e.g. delivery signature) available to challenge the cardholder's dispute, it is almost impossible to reverse the chargeback. Therefore, the merchant will have to completely absorb the cost of the fraudulent transaction. In fact, this cost consists of several components, which could add up to a significant amount. The cost of a fraudulent transaction consists of:

1. **Cost of goods sold**: Since it is unlikely that the merchandise will be recovered in a case of fraud, the merchant will have to write off the value of goods involved in a fraudulent transaction. The impact of this loss will be highest for low-margin merchants.
2. **Shipping cost**: More relevant in a *card-not-present* scenario. Since the shipping cost is usually bundled in the value of the order, the merchant will also need to absorb the cost of shipping for goods sold in a fraudulent transaction. Furthermore, fraudsters typically request high-priority shipping for their orders to enable rapid completion of the fraud, resulting in high shipping costs.
3. **Card association fees**: Visa and MasterCard have put in place fairly strict programs that penalize merchants generating excessive chargebacks. Typically, if a merchant exceeds established chargeback rates for any three-month period (e.g. 1% of all transactions or 2.5% of the total dollar volume), the merchant could be penalized with a fee for every chargeback. In extreme cases, the merchant's contract to accept cards could be terminated.
4. **Merchant bank fees**: In addition to the penalties charged by card associations, the merchant has to pay an additional processing fee to the acquiring bank for every chargeback.
5. **Administrative cost**: Every transaction that generates a chargeback requires significant administrative costs for the merchant. On average, each chargeback requires one to two hours to process. This is because processing a chargeback requires the merchant to receive and research the claim, contact the consumer, and respond to the acquiring bank or issuer with adequate documentation.
6. **Loss of Reputation**: Maintaining reputation and goodwill is very important for merchants as excessive chargebacks and fraud monitoring could both drive cardholders away from transacting business with a merchant.

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.

FRAUD PREVENTION AND MANAGEMENT

With all the negative impacts of fraudulent credit card activities – financial and product losses, fines, loss of reputation, etc, and technological advancements in perpetrating fraud – it's easy for merchants to feel victimized and helpless. However, technological advancements in preventing fraud have started showing some promise to combat fraud. Merchants and Acquirers & Issuers are creating innovative solutions to bring down on fraudulent transactions and lower merchant chargeback rates.

One of the main challenges with fraud prevention is the long time lag between the time a fraudulent transaction occurs and the time when it gets detected, i.e., the cardholder initiates a chargeback. Analysis shows that the average lag between the transaction date and the chargeback notification could be as high as 72 days. This means that, if no fraud prevention is in place, one or more fraudsters could easily generate significant damage to a business before the affected stakeholders even realize the problem.

Fraud Prevention Technologies

While 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.

While none of the tools and technologies presented here can by itself eliminate fraud, each technique provides incremental value in terms of detection ability. As it will be discussed later, the best practice implementations often utilize several of these fraud prevention techniques, if not all of the tools discussed here.

The various fraud prevention techniques are discussed below:

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. Moreover, manual review 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.

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.

CARD VERIFICATION METHODS

The Card Verification Method[3] (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-not-present* 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. Although CVM provides some protection for the merchant, it doesn't protect them from transactions placed on physically stolen cards. Furthermore, fraudsters who have temporary possession of a card could, in principle, read and copy the CVM code.

NEGATIVE AND POSITIVE LISTS

A negative list is a database used to identify high-risk transactions based on specific data fields. An example of a negative list would be a file containing all the card numbers that have produced chargebacks in the past, used to avoid further fraud from repeat offenders. Similarly a merchant can build negative lists based on billing names, street addresses, emails and internet protocols (IPs) that have resulted in fraud or attempted fraud, effectively blocking any further attempts. A merchant/acquirer could create and maintain a list of high-risk countries and decide to review or restrict orders originating from those countries.

Another popular example of negative list is the SAFE file distributed by MasterCard to merchants and member banks. This list contains card numbers, which could be potentially used by fraudsters, e.g., cards that have been reported as lost or stolen in the immediate recent past.

Positive files are typically used to recognize trusted customers, perhaps by their card number or email address, and therefore bypass certain checks. Positive files represent an important tool to prevent unnecessary delays in processing valid orders.

PAYER AUTHENTICATION

Payer authentication is an emerging technology that promises to bring in a new level of security to business-to-consumer internet commerce. The first implementation of this type of service is the Verified by Visa (VbV) or Visa Payer Authentication Service (VPAS) program, launched worldwide by Visa in 2002. The program is based on a Personal Identification Number (PIN) associated with the card, similar to those used with ATM cards, and a secure direct authentication channel between the consumer and the issuing bank. The PIN is issued by the bank when the cardholder enrolls the card with the program and will be used exclusively to authorize online transactions.

When registered cardholders check out at a participating merchant's site, they will be prompted by their issuing bank to provide their password. Once the password is verified, the merchant may complete the transaction and send the verification information on to their acquirer.

[3] Various card issuers use different names to indicate this security feature: CVV2 for VISA, CVC2 for Master Card and CID for American Express.

LOCKOUT MECHANISMS

Automatic card number generators represent one of the new technological tools frequently utilized by fraudsters. These programs, easily downloadable from the Web, are able to generate thousands of 'valid' credit card numbers. The traits of frauds initiated by a card number generator are the following:

- Multiple transactions with similar card numbers (e.g. same Bank Identification Number (BIN))
- A large number of declines

Acquiring banks/merchant sites can put in place prevention mechanisms specifically designed to detect number generator attacks.

FRAUDULENT MERCHANTS

Both MasterCard and Visa publish a list of merchants who have been known for being involved in fraudulent transactions in the past. These lists (NMAS - from Visa and MATCH - from MasterCard) could provide useful information to acquirers right at the time of merchant recruitment preventing potential fraudulent transactions.

Recent Developments in Fraud Management

The technology for detecting credit card frauds is advancing at a rapid pace – rules based systems, neural networks, chip cards and biometrics are some of the popular techniques employed by Issuing and Acquiring banks these days.

Apart from technological advances, another trend which has emerged during the recent years is that fraud prevention is moving from back-office transaction processing systems to front-office authorisation systems to prevent committing of potentially fraudulent transactions. However, this is a challenging trade-off between the response time for processing an authorisation request and extent of screening that should be carried out.

SIMPLE RULE SYSTEMS

Simple rule systems involve the creation of 'if...then' criteria to filter incoming authorisations/transactions. Rule-based systems rely on a set of expert rules designed to identify specific types of high-risk transactions. Rules are created using the knowledge of what characterizes fraudulent transactions. For instance, a rule could look like – If transaction amount is > $5000 and card acceptance location = Casino and Country = *'a high-risk country'*.

Fraud rules enable to automate the screening processes leveraging the knowledge gained over time regarding the characteristics of both fraudulent and legitimate transactions. Typically, the effectiveness of a rule-based system will increase over time, as more rules are added to the system. It should be clear, however, that ultimately the effectiveness of the system depends on the knowledge and expertise of the person designing the rules.

The disadvantage of this solution is that it can increase the probability of throwing many valid transactions as exceptions, however, there are ways by which this limitation can be overcome to some extent by prioritising the rules and fixing limits on number of filtered transactions.

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. Typically, 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. While 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. Thus, 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.

NEURAL NETWORK TECHNOLOGIES

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:

- Identifies cardholder's buying and fraudulent activity patterns.
- Processes data by trial and elimination (excluding data that is not relevant to the pattern).
- 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.

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.

SMART CARDS

To define in the simplest terms, a smart card is a credit card with some intelligence in the form of an embedded CPU. This card-computer can be programmed to perform tasks and store information, but the intelligence is limited – meaning that the smart card's power falls far short of a desktop computer.

Smart credit cards operate in the same way as their magnetic counterparts, the only difference being that an electronic chip is embedded in the card. These smart chips add extra security to the card. Smart credit cards contain 32-kilobyte microprocessors, which is capable of generating 72 quadrillion or more possible encryption keys and thus making it practically impossible to fraudulently decode information in the chip.

The smart chip has made credit cards a lot more secure; however, the technology is still being run alongside the magnetic strip technology due to a slow uptake of smart card reading terminals in the world market.

Smart cards have evolved significantly over the past decade and offer several advantages compared to a general-purpose magnetic stripe card. The advantages are listed below:

- Stores many times more information than a magnetic stripe card.
- Reliable and harder to tamper with than a magnetic stripe card.
- Performs multiple functions in a wide range of industries.
- Compatible with portable electronic devices such as phones and personal digital assistants (PDAs), and with PCs.
- Stores highly sensitive data such as signing or encryption keys in a highly secure manner
- Performs certain sensitive operations using signing or encryption keys in a secure fashion.

A consortium of Europay MasterCard and Visa (EMV) recently issued a set of specifications for embedding chips in credit cards and processing transactions from such cards. MasterCard and Visa have also issued deadlines for compliance with these specifications indicating that banks will have to bear a large portion of fraud losses if they do not comply with EMV specifications. However, the market response has been slow so far due to large investments needed in implementing the EMV compliant programs.

Managing the Total Cost of Fraud

An efficient fraud management solution is one that minimizes the *total cost* of fraud, which includes the financial loss due to fraud as well as the cost of fraud prevention systems. Too often success is mistakenly measured exclusively by one metric –the monthly chargeback rate (Chargeback rate is defined as the percentage of chargeback amount with regard to the net transaction amount). *The question is what is the optimal level of review that would keep fraud losses under control?*

To minimize the actual *total cost* of fraud, an optimal balance needs to be achieved between reducing fraud losses and overheads associated with review of transactions. Reviewing the appropriate number of transactions is the key to achieve this optimal balance. Figure 2 illustrates this trade-off between fraud reduction and the cost of achieving that reduction.

The graph depicts the total cost of fraud as the sum of the actual fraud losses plus the cost of review, which is typically proportional to the volume of transactions being reviewed. The column on the left shows a scenario where fraud losses dominate the total cost, because insufficient screening and review is applied. In this example, fraud loss account for 1% of total value of processed transactions while only 2% of the transactions are being reviewed.

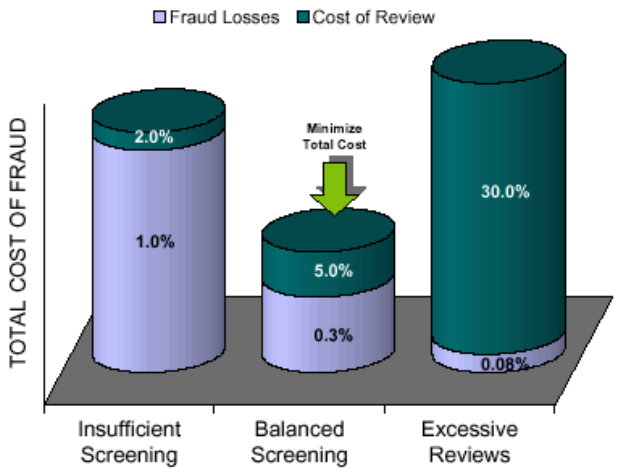

Figure 2: *Minimizing the total cost of fraud. The labels indicate the percentages of orders reviewed and fraudulent orders in each of the three scenarios .*

The column on the right shows the opposite extreme - 30% of the processed transactions are being reviewed and fraud losses are down to 0.06% of the total value of processed transactions. In this case, however, the cost of review drives up the total cost of fraud. While fraud losses are no longer an issue, the cost of achieving this result is not acceptable. Finally, the column in the middle shows the optimal scenario; minimized total cost with acceptable review cost and 'manageable' fraud losses.

As can be seen above, one of the major components of the 'total cost of fraud' is the review of incoming transactions. Review of incoming transactions has both direct and indirect costs associated with it. The direct aspect is the cost of human resources

dedicated to the review. This cost is directly proportional to the volume of transactions being subject to the review. The indirect costs, which are typically more difficult to quantify, include the cost of other resources such as computer hardware, delay in processing of transactions, etc.

The key to minimize the cost of review is to be able to segment transactions, products and cardholders in order to determine the profile of potentially fraudulent transactions. The risk of fraud is never the same for every single transaction. Indeed, there are many factors that help determine the risk associated with a particular transaction. By leveraging these factors, a bank can begin to isolate the problem and identify a relatively small segment of the incoming transactions where review activity needs to be concentrated.

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 analyse 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

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

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

2001. *Fraud Prevention Reference Guide*, Anonymous, Certegy, September 2001.

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

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

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

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

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

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

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.

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

Transnational Credit Card Frauds
http://www.ex.ac.uk/politics/pol_data/undergrad/owsylves/index.html

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

Celent Communications
http://www.celent.com

Authors belong to TCS' Cards Sub-practice. For further information on TCS' offerings in Cards and Banking, please visit our web site www.tcs.com or send email to banking.bidoffice@blore.tcs.co.in.