Credit Card Fraud: Bang in E-Commerce

Khyati Chaudhary[1] Bhawna Mallick[2]
[1, 2]Galgotias College of Engg. & Technology,
Greater Noida

Abstract
Recent decades have seen a gigantic expansion in the use of credit cards as a true transactional medium. Data mining is rising as one of the chief features of many homeland security\ initiatives. Often, it is used as a means for detecting fraud, assessing risk, as well as product retailing. Data mining is becoming increasingly common in both the private as well as public sectors. Data mining involves the use of data analysis tools to find out formerly unknown, believable patterns and relationships in large data sets. Credit card offers a number of secondary benefits unavailable from cash or checks. Credit cards are safer from theft than is cash. Fraud detection involves monitoring the behavior of populations of users in order to estimate, detect or avoid unwanted behavior. In this paper, we studied various factors required to distinguish transaction and characterizes factors affecting fraud detection with fraud prevention techniques.

Keywords: E-commerce, Credit Card, Fraud detection, Fraud Prevention

1. Introduction
Data mining involves the use of complicated data analysis tools to discover previously unknown, valid patterns and relationships among large data sets. These tools can include mathematical algorithms, statistical models, and machine learning methods (such as Neural Networks or Decision Trees). Consequently, data mining comprises of more than collection and management of data, it also includes analysis and prediction. Data mining can be performed on data represented in textual, quantitative or multimedia forms. Data mining applications can use a range of parameters to observe the data. This includes association, classification, sequence or path analysis, clustering and forecasting. When using normal measure, detection of credit card fraud is a tricky task. Therefore, the development of the credit card fraud detection model has become of much important, whether in the academic, organization or business community recently. Proposed models or existing models are mostly statistics-driven or Artificial Intelligent-based (AI), which have the theoretical advantages in not imposing artificial assumptions on the input variables [1].

Credit Cardholders have many beneficiary schemes as to hold interest-free balances for almost two months with "grace-period". Suitable information on fraudulent activities is tactical to the banking industry. Banks have huge databases. Extraction of important business information can be done from these data store. Data stores have some patterns into clusters that are natural to the input data. Concept of fraud detection has been laid on data mining techniques which include association rules, clustering and classification. The chief point of research on fraud detection has been focused on pattern matching in which abnormal patterns are identified from the normal ones. Popularity of online shopping is growing day by day on high pace. Nowadays, Credit card is the most popular mode of payment (59 percent), Germany and Great Britain have the largest number of online shoppers. Usually, Retailers like Wal-Mart handle much larger number of credit card transactions online as well as regular purchases [2]. There are numerous options for handing credit card payments on the Internet, as the processing of credit card transactions is generally independent of the type of e-commerce exchange. While a huge portion of e-commerce would consist of credit card purchases, like regular or often. It is more important for businesses and organizations that rely upon on income from e-commerce to know the options available as well as costs linked with credit card transaction processing on the Internet. No one has any hint about transaction being processed are whether a fraudulent transaction or legitimate which has passed the prevention mechanisms. Therefore, the goal of the fraud detection systems is to pre-determine every transaction for the possibility of being fraudulent regardless of the prevention mechanisms and to categorize transaction as fraudulent ones as early as possible after the fraudster has begun to commit a fraudulent transaction. Credit card fraud detection is a tremendous task but also trendy problem to solve. Many fraud detection systems estimate the transactions and generate a suspicion score (commonly a probability between 0 and 1) which shows the chances of that transaction to be fraudulent. Computational procedures of these scores are applicable to the techniques used to build the model(s) in the fraud detection systems. These corresponding scores are used with a predefined threshold value to differentiate between fraudulent transactions from the legitimate ones easily [3].

Introduction of new technologies such as telephone, automated teller machines (ATMs) and credit card systems have enlarged the amount of fraud loss for many banks. Analyzing whether each transaction being processed is legitimate or not is very expensive is another task to determine transaction genuinely. Further, if we check them in all transactions & confirm whether a transaction was done by a client or a fraudster by phoning all card holders is cost

prohibitive. Fraud prevention by automatic fraud detections mechanism can be applied where the well-known classification methods can be identified, where pattern recognition systems has key function. One can learn from fraud happened in the past and categorize new transactions easily. Recently, perhaps the most frequently used technique is Neural Networks in credit card business.
Credit Card Fraud Detection domain presents a number of challenging issues for data mining as well:

- There are millions of credit card transactions processed each day. Mining of such massive amount of data requires highly efficient techniques that scale data efficiently.
- Highly skewed-data,
- Each transaction record has a different dollar amount and there is a chance of variable potential loss.

II. The Fraud Detection Problem

Problem of detecting fraudulent transactions occurs after they have been focused to fraud prevention methods and relevant processes. There is immense literature on wide range of security methods to look after transactions from unauthorized use or exposure of their private/secure information and consequent valuable resources. Still, fraudsters find a mode through which many witty means of circumventing a countless prevention techniques.
On the other side, many transaction media such as ATM, bank cards or debit cards, require the use of pins, passwords, and in some cases "biometrics" to authenticate the legitimate owner. Credit cards create fascinating problems since generally no pin is required for their use; only the name, expiration date and account number is required. Popular means of criminally transacting with credit cards is by stealing someone's identity & in some cases, creating a new fake identity. Therefore, fraudulent electronic transactions (E-transaction) by credit card are the key problem. Credit cards need not be necessarily physically obtainable to transact and over the internet they can be used to fraudulently transact web better and heavier losses for banks and their customers if caught by fraudsters. The chief idea in fraud detection is that fraud may be detected by noticing significant deviation from the "normal behavior" of a customer's account. That is why; behavior of an account can thus be used to protect that account. Currently banks have come to realize that a fused, global approach is mandatory to detect fraud, involving the periodic sharing with each other of information about attacks.

Iii. Different Type of Fraud Techniques

There are many ways in which fraudsters bring out a credit card fraud. As the technology changes, so does the technology of fraudsters varies and thus the mode in which fraudsters go about carrying out fraudulent activities. Frauds can be broadly categorized into three stages i.e., traditional card related frauds, merchant related frauds and Internet frauds. Different types of methods for committing credit card frauds are:

A. Merchant Connected Frauds (MCF)

Merchant connected frauds are being committed either by owners of the merchant firm or their employees. Different types of frauds initiated by merchants are:

i. Merchant Collusion: When merchant owners or their employees plan to commit fraud using the cardholder accounts or by using the personal information [4].

ii. Triangulation*:* Triangulation is among the type of fraud which is done and operates from a website. Triangulation includes products or goods that are offered at heavily discounted rates and are being shipped before payment. The phenomenon initiate by the customer while browse the site and if he/she likes the product he/she place the online information such as name, address and valid credit card details to that particular site. However, when the fraudsters get these details, they order goods from a legitimate site using stolen credit card details. Further, after this, fraudster use credit card information for purchasing the products/goods.

B. Internet Associated Frauds (IAF)

Internet is the foundation for the fraudsters to make the frauds in the simple and the easiest technique(s). Currently, fraudsters have begun to operate on a actually transactional level. Internet has become a new worlds market, capturing consumers from countries around the world along with the development of trans-border, economic and political spaces. Some of the most frequently used techniques in Internet fraud are:

i. Site cloning: Site cloning is the process where fraudsters close whole site or simply the pages from which the customer made a purchase. There is no option left with the customers to believe that they are not dealing with the company that they wished to purchase goods or services from because the pages that they are viewing are somehow

matching to those of the real site. Further, cloned site will receive these details and propel the customer a receipt of the transaction through the email just as the real company would do.

ii. False merchant site(s): Actually, some sites offer a contemptible service for the customers. Site(s) requests the customer to fill his/her complete details such as name and address to access the webpage where the customer gets his requisite products. Numerous sites claim to be free but require a valid credit card number to verify an individual's age. In this mode sites collect as many as credit card details. Sites are generally part of a larger criminal network that either uses the details it collects to raise revenues or sells valid credit card details to small fraudster(s).

iii. Credit card generators (CCG): CCG are computer programs that create valid credit card numbers and expiry dates. CCG generates lists of credit card account numbers from a single account number. CCG software works by using the mathematical Luhn algorithm that card issuers use to produce other valid card number combination(s).

iv. Lost/ Stolen Cards: When individual loses his card or a card is stolen by someone or when a legitimate account holder receives a card and loses it or someone else steals the card for criminal purposes. This is the simplest way for the fraudsters where they get the information of the cardholders without investing on the modern technology. It is possibly the hardest form of traditional credit card fraud to embark upon.

v. Account Takeover: Fraud occurs when the valid customer's personal information is taken by the fraudsters. In this fraudster(s) takes control of a legitimate account by providing the customer's account number or the card number. Fraudster then acquaintances the card issuer as the genuine cardholder to ask the mail to redirect to a new address. In some cases, the fraudster reports card lost and asks for a replacement to be sent.

vi. Cardholder-Not-Present (CNP): CNP transactions are performed only on the Internet in such kind of frauds neither the card nor the cardholder is present physically at the point-of-sale. This would have many forms to commit the fraud as there are many types of transactions such as orders made over the phone or Internet, by mail order or fax.

In such transaction(s), retailers are not capable to physically check the card or the identity of the cardholder, which makes the user unknown and able to disguish between their true identities. In this, details of the credit card are usually copied without the cardholder's awareness. Fraudulently obtained card details are usually used with fictitious personal details to make fraudulent CNP purchases. Security Code imprinted on the back of cards can help in prevention of fraud where card details have been obtained but when the card is stolen it won't be helpful. This is the promising method for fraud prevention.

vii. Fake and Counterfeit Cards: Another type of fraud where the formation of counterfeit cards, together with lost or stolen cards poses maximum threat in credit card frauds. Fraudsters are always in search of new and more original ways to create counterfeit cards.

viii. Erasing the magnetic strip: In this type of the fraud, the fraudsters erase the magnetic stripe by using the powerful electro-magnet. Fraudster then tampers with the facts on the card so that they match the details of a valid card which they may have attained. The cashier will then carry on to manually input the card information into the terminal. This type of fraud has high risk because of the cashier would look at the card closely to read the numbers.

ix. Creating a fake card: In present scenario, we have refined machines where we can create a fake card from using the scratch. It is the expected fraud, though fake cards require a lot of effort and skill to produce it. Present cards are having many security features, all designed to make it tricky for fraudsters to make good quality fraudulent. Furthermore, after introducing the Holograms in the credit cards it makes very complicated to forge them effectively.

x. Skimming: Another kind of fraud being committed is skimming which is fast emerging as the most popular form of credit card fraud. Mostly, fraud cases of Counterfeit fraud involve skimming. It is a method where the actual data on a card's magnetic stripe is electronically copied onto another. Fraudster(s) does this even as the customer is waiting for the transaction to be validated through the card terminal. Card holder doesn't t know about this activity and it is very difficult for customer(s) to identify. In some of the cases, details obtained by skimming are used to carry out fraudulent card not-present (CNP) transactions by fraudsters.

xi. Phishing: Phishing is a type of fraud planned to steal a person's identity. It is generally committed via spam e-mail or pop-up windows. It is the phenomenon which works by a wicked person sending lots of false e-mails. E -mails received looks like they come from a website or company you trust. Message tells users to provide the company with your personal details including your payment card details. These companies can also claim that the reason for this is a

database crash or the like. For the fraudster might put a link to a website that look exactly like the real one but is in fact a scam site by making the e- mails look even more authentic. These copies are often known as "spoofed websites".

Iv. Literature Review

4.1 Overview on Credit Card

Credit card frequently used as a necessary mode of payments in today's society. People used credit card for a range of reason such as obtaining credit facility, cash advance, easy payment, charge card. There are some controversial issues that have been addressed not only in terms of the numbers of credit flooding the nation's economy, but the amount transactions that end up with payment default and the numbers of credit card fraud as been recorded which endangered the economy should be seriously paying attention [5]. But because of the advances and changing behavior in purchasing activities has considerably contributed to the diffusion of credit card as becoming more significant and applicable in maintaining the purchasing activities. Based on the judgment, it is stated that there is positive connection between usage rate and income. The fact that was frequently stated, most of the card issuers normally allowance a higher credit limit among the higher income group. Lastly, it was stated that higher income clients are the main targets for the credit card issuers. Bulky purchase allows people not to carry cash and is useful in Internet purchases and rental collateral. But the crisis is that it is improper on religious grounds because there will be an interest payments made when the outstanding balance is not repay in full.

In the card issuer's point of view, numerous problems occurred. Industry is growing and this research would be helpful for the banks offering the credit cards to focus on quite a few factors that pressurize the credit card holders in choosing their preferred credit cards.

Buttafogo began the workshop with a operational definition of credit card fraud as: "Unauthorized account activity by a person for which that account was not planned. Operationally, this is an event for which action can be taken to stop the neglect in progress and incorporate risk management practices to protect against similar actions in the future." He then described the range of fraudulent activities observed in the industry.

The Internet and the ambiguity associated with card not present (CNP) transactions current unique fraud management challenges. Authentication of the cardholder is a primary requirement in managing fraud on the Internet. There are no commonly accepted solutions. As a result, credit card fraud on the Internet is significantly greater than in the physical, or even, phone environments [6].

Data mining contributed towards fraud detection. Data mining has various categories through which various operations has been performed. Data Mining can be mainly classified into the following categories:

1) **Association rule mining** which uncovers interesting association patterns among a large set of data items by showing attribute- value circumstances that occur together regularly. Market basket analysis is a classic example in which analyzing purchasing habits of customers by finding associations between different items in customers' "shopping baskets."

2) **Classification and prediction** is the process of identifying a set of ordinary features and models that to explain and distinguish between classes or concepts. Models are used to guess the class of objects whose class label is unknown. For example, Bank which may classify a loan application as either a fraud or a potential business using models based on uniqueness of the applicant. A huge number of classification models have been developed for predicting future trends of stock market indices and foreign exchange rates (FRI).

3) Clustering analysis segments a bulky set of data into subsets or clusters. In this, each cluster is a collection of data objects that are similar to one another within the same cluster but dissimilar to objects in other clusters. Additionally, objects are clustered based on the principle of maximizing the intra-class resemblance while minimizing the inter-class similarity. For example, clustering techniques can be used to recognize stable dependencies for risk management as well as investment management.

4) Sequential pattern and time-series mining looks for patterns where one value leads to another later value. Example, after the inflation rate increases, the stock market is likely to go down.

V. Impact of Credit Card Frauds

Fraudulent activity on a card affects every person that is the cardholder, the merchant, the acquirer as well as the issuer. In this section, we analyses the impact that credit card frauds have on all the company involved in transacting business through credit cards.

5.1. Impact of Fraud on Cardholders

Cardholders are the least impacted party due to fraud in credit card transactions as consumer responsibility is limited for credit card transactions by the legislation existing in most countries. This is true for both card-present (CP*)* as well as card not- present (CNP*)* scenarios. Banks even have their own principles that limit the consumer's problem to a greater degree. Banks also have a cardholder protection policy that covers losses of the cardholder. The cardholder has to just report doubtful charges to the issuing bank, which in turn investigates the issue with the acquirer and merchant and further processes chargeback for the disputed amount [7].

5.2. Impact of Fraud on Merchants

Merchants are the most exaggerated party in a credit card fraud mainly in the ***card-not-present (CNP)*** transactions, as they have to accept full accountability for losses due to fraud. Every time a legitimate cardholder disputes a credit card charge, the card-issuing bank will send a chargeback to the merchant, reversing the credit for the transaction. The merchant does not have any physical confirmation available to challenge the cardholder's dispute then it is almost impossible to reverse the chargeback. As a result, the merchant will have to completely absorb the cost of the fraudulent transaction. The cost of a fraudulent transaction consists of:

1. **Cost of goods sold**: Since it is doubtful that the merchandise will be recovered as 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 kind of losses will be maximum for low-margin merchants.

2. Shipping cost: More relevant in a *card-not-present (CNP)* scenario. While the shipping cost is usually bundled in the value of the order, the merchant will also need to take up the cost of shipping for goods sold in a fraudulent transaction. Besides, fraudsters normally request high-priority shipping for their orders to allow fast completion of the fraud, resulting in high shipping costs.

3. Card association fees: Visa and MasterCard have put in place quite strict programs that fine merchants generating extreme charge backs. Usually, if a merchant exceeds well-known chargeback rates for any three-month period the merchant could be penalized with a fee for every chargeback.

4. Merchant bank fees: In addition to the penalties charged by card associations, the merchant has to pay an extra processing fee to the acquiring bank for every chargeback being transacted.

5. Administrative cost: Every transaction that generates a chargeback requires major administrative costs for the merchant. Usually each chargeback requires one to two hours to process. Because for 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.

5.3. Impact of Fraud on Banks (Issuer/Acquirer)

On the basis of the scheme rules defined by both MasterCard and Visa, it is sometimes possible that the Issuer/Acquirer bears the costs of fraud. Still in cases, where the Issuer/Acquirer is not bearing the direct cost of the fraud, there are some indirect costs that will finally be borne by them. As like in the case of charge backs issued to the merchant, there are also administrative and manpower costs that the bank has to sustain. The issuers and acquirers also have to make vast investments in preventing frauds by deploying complicated IT systems for detection of fraudulent transactions.

Vi. Fraud Prevention

Along with all the negative impacts of fraudulent credit card activities such as financial and product losses, fines, loss of reputation and technological advancements in perpetrating fraud, it is simple for merchants to feel offended and helpless. Though scientific advancements, preventing fraud have started to assure for fraud prevention.

Merchants and Acquirers as well as Issuers are creating original solutions to bring down on fraudulent transactions and lower merchant chargeback rates. Key challenge with fraud prevention is the long time pause between the time fraudulent transaction occurs and the time when it gets detected that is the cardholder initiates a chargeback. Analysis results shows that the average lag between the transaction date and the chargeback notification could be as high as 72 days [8]. It means that if no fraud prevention is in place, one or more fraudsters could easily produce significant damage to a business before the affected stakeholders even realize the problem.

6.1. Fraud Prevention Technologies

While fraudsters are using sophisticated methods to achieve access to credit card information and perpetrate fraud, new technologies are being available to assist merchants to detect and prevent fraudulent transactions as well. Fraud detection technologies enable merchants and banks to perform highly automated screenings of incoming transactions and flagging suspicious transactions. Although none of the tools and technologies offered here can by itself eliminate fraud, each technique provides incremental value in terms of detection ability. Various fraud prevention techniques are as follows:

6.1.1. MANUAL REVIEW (MR)

Manual review consists of reviewing every transaction manually for signs of fraudulent activity and involves a exceptionally high level of human involvement. It can prove to be very expensive, as well as time consuming. Furthermore, manual review is incapable to detect some of the more common patterns of fraud such as use of a single credit card multiple times on multiple locations (physical or web sites) in a short distance.

6.1.2. ADDRESS VERIFICATION SYSTEM (AVS)

AVS is applicable in *card-not-present (CNP)* scenarios. AVS matches the first few digits of the street address and the ZIP code information given for delivering the purchase to the corresponding information on record with the card issuers. Code on behalf of the level of match between these addresses is returned to the merchant.

6.1.3. CARD VERIFICATION METHODS (CVM)

The Card Verification Method (CVM) consists of a 3- or 4-digit numeric code printed on the card but is not imprinted on the card and is not accessible in the magnetic stripe. The merchant can request the cardholder to provide this numeric code in case of *card-not present* (CNP) [9] transaction and submit it with authorization. Main idea of CVM is to make sure that the person submitting the transaction is in control of the actual card, since the code cannot be copied from receipts or skimmed from magnetic stripe. CVM provides some protection for the merchant(s) it doesn't defend them from transactions placed on physically stolen cards. Moreover, fraudsters who have provisional possession of a card could read and copy the CVM code.

6.1.4. NEGATIVE AND POSITIVE LISTS (N/P L's)

Negative List (NL) is a database used to recognize high-risk transactions based on specific data fields. For example, negative list would be a file containing all the card numbers that have formed charge backs in the past, used to evade further fraud from repeat offenders. Likewise a merchant can put up negative lists based on billing names, street addresses, emails and internet protocols (IPs) that have resulted in fraud or attempted fraud, effectively blocking any more attempts. An acquirer could form and maintain a list of high-risk countries and decide to review or confine orders originating from those countries. Positive files/List (PL) represents a vital tool to prevent unnecessary delays in processing valid orders.

6.1.5. PAYER AUTHENTICATION (PA)

Payer Authentication is a rising technology that promises to fetch in a new level of security to business-to-consumer (b-c) internet commerce. First implementation of this kind of service is the Verified by Visa (VbV) or Visa Payer Authentication Service (VPAS) program. This program is based on a Personal Identification Number (PIN) linked with the card, comparable to those used with ATM cards and a secure direct authentication channel between the consumer and the issuing bank [10]. PIN is issued by the bank when the cardholder enrolls the card with the program and will be used completely to authorize online transactions. When registered cardholders check out at a participating merchant's site, they will be driven by their issuing bank to provide their password. Likewise, once the password is verified, the merchant may complete the transaction and send the verification information on to their acquirer.

6.1.6. LOCKOUT MECHANISMS (LM)

Automatic card number generators signify one of the new technological tools normally utilized by fraudsters. These programs are easily downloadable from the Web and are able to produce thousands of 'valid' credit card numbers. The qualities of frauds initiated by a card number generator are as follows:

(i) Multiple transactions with similar card numbers (for example, same Bank Identification Number (BIN))

(ii) A huge number of declines.

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

6.1.7. FRAUDULENT MERCHANTS (FM)

Both MasterCard and Visa publish a list of merchants who have been known for being occupied in fraudulent transactions in the past. These lists could provide functional information to acquirer right at the time of merchant recruitment preventing potential fraudulent transactions [11].

Vii. Conclusion

Credit card fraud has become more and more widespread in recent years. Building an accurate, efficient and easy-handling credit card risk monitoring system is one of the chief tasks for the merchant banks for improving merchants risk management level in an automatic, scientific and effective way,. In this era of digital world, credit card is of extreme importance to financial organizations, institutions and companies. As credit card becomes the most accepted mode of payment for both online as well as regular purchase, cases of fraud associated with it are also increasing. For the purpose of reducing the bank's risk, various techniques have been employed. In this study, we characterize various fraud commitment and prevention methods as well. However model has been proposed for credit card fraud detection in catching the fraudulent transactions.

References

1. A. Shen, R. Tong, and Y. Deng, "Application of classification models on credit card fraud detection," June 2007

2. Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar, "Credit Card Fraud Detection using Hidden Markov Model," *IEEE Transactions On Dependable And Secure Computing*, vol. 5, Issue no. 1, pp.37-48, January-March 2008.

3. Aihua Shen, Rencheng Tong, Yaochen Deng, Application of Classification Models on Credit Card Fraud Detection, 2007 IEEE.

4. Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, "Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning," *Special Issue on Information Fusion in Computer Security*, Vol. 10, Issue no 4, pp.354- 363, October 2009.

5. CLIFTON PHUA1*, VINCENT LEE1, KATE SMITH1 & ROSS GAYLER2**A** Comprehensive Survey of Data Mining-based Fraud Detection Research

6. Pengyue J. Lin, Behrokh Samadi, Alan Cipolone, Daniel R. Jeske**,** Development of a Synthetic Data Set Generator for Building and Testing Information Discovery Systems, Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06)2006 IEEE.

7. Jon T. S. Quah and M. Sriganesh, Real Time Credit Card Fraud Detection using Computational Intelligence, Proceedings of International Joint Conference on Neural Networks, Orlando, Florida, USA, August 2007.Kou, Y., Lu, C.-T., Sirwongwattana, S., Huang, Y.-P.: Survey of fraud detection techniques. In: Proceedings of the 2004 IEEE International Conference on Networking, Sensing and Control, Taipei, Taiwan (2004).

8. Tej Paul Bhatla, Vikram Prabhu & Amit Dua "Understanding Credit Card Frauds," 2003.

9. Y. Sahin, E. Duman "Detecting Credit Card Fraud by ANN and Logistic Regression" 2011.

10. Raghavendra Patidar, Lokesh Sharma, "Credit Card Fraud Detection Using Neural Network", International Journal of Soft Computing and Engineering (IJSCE) June 2011.

11. Y. Sahin, E. Duman**,** Detecting Credit Card Fraud by ANN and Logistic Regression, ©2011 IEEE