Available online at www.sciencedirect.com
ScienceDirect
Expert Systems with Applications 35 (2008) 1721–1732
Expert Systems with Applications
www.elsevier.com/locate/eswa

Real-time credit card fraud detection using computational intelligence

Jon T.S. Quah *, M. Sriganesh

School of Electrical and Electronic Engineering, Nanyang Technological University, Nanyang Avenue, Singapore 639798, Republic of Singapore

Abstract

Online banking and e-commerce have been experiencing rapid growth over the past few years and show tremendous promise of growth even in the future. This has made it easier for fraudsters to indulge in new and abstruse ways of committing credit card fraud over the Internet. This paper focuses on real-time fraud detection and presents a new and innovative approach in understanding spending patterns to decipher potential fraud cases. It makes use of self-organization map to decipher, filter and analyze customer behavior for detection of fraud.

Keywords: Self-organizing map; Unsupervised learning; Risk scoring; Transaction

1. Introduction

The fast and wide reach of the Internet has made it one of the major selling channels for the retail sector. In the last few years, there has been a rapid increase in the number of card issuers, card users and online merchants, giving very little time for technology to catch-up and prevent online fraud completely. Statistics shows that on-line banking has been the fastest growing Internet activity with nearly 44% of the population in the US actively participating in it (Fighting Fraud on the Internet, 1999). As overall e-commerce volumes continued to grow over the past few years, the figure of losses to Internet merchants was projected to be between $5 and $15 billion in the year 2005. Recent statistics by Garner group place online fraud rate between 0.8% and 0.9%, with auction fraud accounting to nearly half of the total incidents of fraud on the Internet (Online Banking, 2005). Considering the current trends of e-commerce volumes, the projected loss is $8.2 billion in the year 2006, with $3.0 billion in the US alone (Statistics for General & Online Fraud, 2007).

1.1. How and where does fraud begin

In order to understand the severity of credit card fraud, let us briefly look into the mechanisms adopted by fraudsters to commit fraud. Credit card fraud involves illegal use of card or card information without the knowledge of the owner and hence is an act of criminal deception. Fraudsters usually get hold of card information in a variety of ways: Intercepting of mails containing newly issued cards, copying and replicating of card information through skimmers or gathering sensitive information through *phishing* (cloned websites) or from unethical employees of credit card companies.

Phishing involves acquiring of sensitive information like card numbers and passwords by masquerading as a trustworthy person or business in an electronic communication such as e-mail (Schneck, 2007). Fraudsters may also resort to generation of credit card numbers using BIN (Bank Identification Numbers) of banks. A recent scheme of *Triangulation* takes fraud fighters many days to realize and investigate (Bhatla, Prabhu, & Dua, 2003). In this method, the fraudster operates through an authentic-looking website, where he advertises and sells goods at highly discounted prices. The unaware buyer submits his card information and buys goods. The fraudster then places an order with a genuine merchant using the stolen card information. He then uses

* Corresponding author. Tel.: +65 67905871; fax: +65 62701556.
E-mail address: itsquah@ntu.edu.sg (J.T.S. Quah).

0957-4174/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2007.08.093

the stolen card to purchase other goods or route funds into intractable accounts. Its only after several days that the merchant and card owners realize about the fraud. This type of fraud causes initial confusion that provides camouflage for the fraudster to carry out their operations.

1.2. Impact of fraud

It is interesting to note that credit card fraud affects card owners the least because their liability is limited to the transactions made. The existing legislations and cardholder protection policies as well as insurance schemes in most countries protect the interests of the cardholders. However, the most affected are the merchants, who, in most situations, do not have any evidence (eg. Digital signature) to dispute the cardholders' claim of misused card information. Merchants end up bearing all the loses due to chargeback, shipping cost of goods, card issuer fees and charges as well as their own administrative costs. Excessive fraudulent cases involving the same merchant can drive away customers, cause card issuer banks to withdraw service and also result in loss of reputation and goodwill (Yu & Singh, 2002). Card issuer banks have to bear the administrative cost of investigations into fraud cases as well as infrastructure costs of setting up the required software and hardware facilities to combat fraud. They also incur indirect costs through transaction delays. Studies show that the average time lag between the fraudulent transaction date and chargeback notification can be as high as 72 days, thereby giving fraudsters sufficient time to cause severe damage (Bhatla et al., 2003).

1.3. Fraud detection and prevention

The negative impacts of fraud make it very clear and necessary to put in place an effective and economical fraud detection system. Recent technological advancements to combat fraud have contributed number of solutions in this area (Bhatla et al., 2003; All points protection, 2007). Fraud detection techniques involving sophisticated screening of transactions to tracking customer behaviour and spending patterns are now being developed and employed by both merchants as well as card issuer banks (Tan & Thoen, 2000). Some of the recently employed techniques include transaction screening through Address Verification Systems (AVS), Card Verification Method (CVM), Personal Identification Number (PIN) and Biometrics. AVS involves verification of address with zip code of the customer while CVM and PIN involve checking of numeric code that is keyed in by the customer. Biometrics might involve signature or fingerprint verification. Rule-based methods and maintaining of positive and negative lists of customers and geographical regions are also used in practice. Data mining and credit scoring methods focus on statistical analyses and deciphering of customer behaviour and spending patterns to detect frauds (Huang, Chen, & Wang, 2007). Neural networks are capable of deriving patterns out of databases containing historical transactions of customers. These neural networks can be 'trained' and are 'adaptive' to the emerging new forms of frauds.

Deployment of sophisticated techniques and screening of every transaction alone will not reduce losses. It is necessary to employ an *effective and economical solution* to combat fraud (Turney, 1995). Such a solution should not only detect fraud cases efficiently but also turn out to be cost-effective. The idea is to strike a balance between the cost involved in transaction screening and review and the losses due to fraudulent cases. Analyses show that review of only 2.0% of transactions can result in reducing fraud losses accounting to 1.0% of total value of transactions. While a review of as high as 30% of transactions can reduce the fraud loses drastically to 0.06%, but that increases review costs exorbitantly (Bhatla et al., 2003). The estimated cost of not using anti-fraud software was about $60 billion in 2005 (Statistics for General & Online Fraud, 2007).

The key to minimize total costs is to categorize transactions and review only the potentially fraudulent cases. This should involve deployment of a step-by-step screening, filtering and review mechanism. A typical deployment can involve initial authentication of transactions through PIN, expiry date on card, AVS and CVM. A second level of screening can involve comparing with positive and negative lists as well as rules based on customers, geographical regions, IP addresses and policies. Risk and credit scoring with pattern and behaviour analyses can come next, followed by manual review. This classifies and filters out transactions as genuine or fraudulent in every step and as a result only a few transactions would require further manual review. Such a solution reduces the overall processing delay as well as total costs involved in manpower and administration.

The focus of this paper will now shift to risk scoring and behavioral pattern detection using neural networks.

2. Neural networks in fraud detection – literature review

Neural Networks have been extensively put to use in the areas of banking, finance and insurance. They have been successfully applied into credit scoring of customers, bankruptcy or business failure prediction, stock price forecasting, bond rating, currency prediction and many more areas (Stock Analysis, 2007; Quah & Srinivasan, 1999). In the area of fraud detection and prevention, neural networks like feed-forward networks with back-propagation have found immense applications (Fraud Brief – AVS & CVM, ClearCommerce Corporation, 2003; The Evolving Threat of Card Skimming, FairIsaac, 2007; ClearCommerce Fraud Prevention Guide, 2002). Usually such applications of neural networks systems involve knowing about the previous cases of fraud, to make systems learn the various trends. Fraud cases are statistically analyzed to derive out relationships among input data and values for certain key parameters in order to understand the various patterns of fraud. This knowledge of fraud trends is then iteratively taught to feed-forward neural networks, which can successfully identify similar fraud cases occurring in the future.