Expert Systems with Applications 39 (2012) 12650–12657

Contents lists available at SciVerse ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Employing transaction aggregation strategy to detect credit card fraud

Sanjeev Jha [a,*], Montserrat Guillen [b,1], J. Christopher Westland [c,2]

[a] Department of Decision Sciences, Whittemore School of Business and Economics, University of New Hampshire, McConnell Hall, Durham, New Hampshire 03824-3593, USA
[b] Department of Econometrics, Riskcenter-IREA, University of Barcelona, Diagonal, 690, 08034 Barcelona, Spain
[c] Department of Information & Decision Sciences (MC 294), Room 2400, University Hall, University of Illinois, Chicago, 601 S. Morgan Street, Chicago, IL 60607-7124, USA

ARTICLE INFO

Keywords:
Fraud detection
Predictive modeling
Logistic regression

ABSTRACT

Credit card fraud costs consumers and the financial industry billions of dollars annually. However, there is a dearth of published literature on credit card fraud detection. In this study we employed transaction aggregation strategy to detect credit card fraud. We aggregated transactions to capture consumer buying behavior prior to each transaction and used these aggregations for model estimation to identify fraudulent transactions. We use real-life data of credit card transactions from an international credit card operation for transaction aggregation and model estimation.

1. Introduction

Credit card fraud costs consumers and the financial industry billions of dollars annually (Chan, Fan, Prodromidis, & Stolfo, 1999; Chen, Chen, & Lin, 2006). The reported loss due to online fraud for the year 2008 was $4 billion, an increase of 11% on year 2007 loss of $3.6 billion (Leggatt, 2008). Credit card transactions, as a share of payment system, have been growing worldwide along with credit card fraud. Moreover, credit card fraud funds other criminal activities, including terrorism in ways that may be difficult to track and prevent (Everett, 2009). As fraud detection has steadily evolved, perpetrators have become more sophisticated in tandem with these improvements (Bolton & Hand, 2002). The audit of credit card fraud is an ongoing 'arms-race' that requires constant innovation on the part of card issuers.

However, there are various obstacles to this innovation. For example, academicians have difficulty in getting credit card transactions datasets leading to less academic research and also not much of proprietary detection techniques get discussed in public lest fraudsters should gain knowledge and evade detection (Leonard, 1993). There is a dearth of published literature on credit card fraud detection, which makes exchange of ideas and possible innovation in fraud detection difficult (Bolton & Hand, 2002). One difficulty with analysis of credit card fraud is that perpetrators do not usually carry on a single fraudulent transaction. Analyzing fraud from the perspective of a "one by one" transaction omits the idea of clustering that is inherent of credit card fraud actions. Perpetrators usually produce a group of fraudulent transactions. We argue that analyzing the aggregated behavior is essential to improve credit card fraud detection rates.

In this study we employ transaction aggregation strategy (Krivko, 2010; Whitrow, Hand, Juszczak, Weston, & Adams, 2009) to create variables for the estimation of a logistic regression model to attempt to detect (and thus control and prosecute) credit card fraud. We demonstrate the efficacy of aggregating transactions to capture consumer buying behavior prior to each transaction. The underlying rationale is that the buying behavior of fraudulent and legitimate transactions is different. This difference gets captured in aggregated transactions and can be used for identification of fraudulent transactions. We use real-life data of transactions from an international credit card operation for aggregating transactions and then use them for model estimation.

A general definition of 'fraud' may be somewhat elusive, as new methods of fraud appear with regularity. For the purpose of this study, fraudulent transactions are specifically defined by the institutional auditors as those that caused an unlawful transfer of funds from the bank sponsoring the credit cards. These transactions were observed to be fraudulent ex post.

The remainder of this paper is organized as follows. In the next section we discuss credit card fraud and detection methods. In section 3, we discuss the dataset source, primary attributes, and creation of derived attributes using these primary attributes. In section 4, we discuss the estimation method and present a standard logit model. Thereafter, we present our results, discussion, and conclusions of our study.

* Corresponding author. Tel.: +1 603 862 0314; fax: +1 603 862 3383.
E-mail addresses: sanjeev.jha@unh.edu (S. Jha), mguillen@ub.edu (M. Guillen), westland@uic.edu (J. Christopher Westland).
[1] Tel.: +34 93 4037039; fax: +34 93 4021821.
[2] Tel.: +1 312 996 2323; fax: +1 312 413 0385.

0957-4174/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.eswa.2012.05.018

2. Background

2.1. Credit card fraud

Credit card frauds can be committed in a number of ways (Blunt & Hand, 2000). However, credit card frauds have been classified into two broad categories: application and behavioral frauds (Bolton & Hand, 2001). Application fraud occurs when fraudsters obtain new cards from issuing companies and are of two types. In the first type, perpetrators obtain new cards from issuing companies using other people's information and keep using the cards with the stolen identity until fraud is detected. In the second type, perpetrators seek new credit cards using false personal information with the intention of never repaying their purchases (Bolton & Hand, 2002). Financial institutions have traditionally used credit scores to deny issue of credit cards to individuals likely to default payments either because they do not have sufficient income or because they fit the profile of those likely to commit fraud (Hand & Henley, 1997). Also, financial institutions use various models to monitor purchase behavior over time to detect cards obtained using false information. For example, a first time card holder who reaches his or her credit limit within a few days of issuance of a card or exhibits similar unusual purchase behavior may raise alarm. Researchers have employed case-based reasoning approaches to detect credit card application fraud (Wheeler & Aitken, 2000).

Behavioral frauds are of four types: mail theft, stolen/lost card, counterfeit card, and 'card holder not present' fraud. Mail theft fraud occurs when fraudsters intercept credit cards in mails before they reach cardholders. Stolen/lost card fraud happens when fraudsters get hold of credit cards through theft (for example of a purse or wallet). In case of counterfeit card fraud, like the previous two kinds of fraud, a physical card is used to commit fraud. However, the difference is that perpetrators pilfer card information in order to create a physical counterfeit card. For 'card holder not present' fraud, unlike the other three types of fraud, a physical card is not necessary. 'Card holder not present' fraud is done remotely and perpetrators are not present physically at a merchant's premises. Card details are enough to carry out a transaction (Bolton & Hand, 2002). Since transactions are carried out remotely, perpetrators do not have to sign for purchases or to physically swipe credit cards or even show proof of identification. Thus perpetrators carry out fraudulent transactions in complete anonymity. These four types of behavioral fraud represent a very high proportion of losses (Bolton & Hand, 2002). In this study, we investigate behavioral credit card frauds.

Williams (2007) chronicled the manner in which credit card fraud has evolved over the years. In the 1970s, stolen cards and forgery were the most prevalent type of credit card fraud, where physical cards were stolen and used. Later, mail-order-telephone-order fraud became common in the 1980s and 1990s. Now, credit card fraud has moved to the Internet, which provides the anonymity, reach, and speed to commit fraud across the world.

2.2. Fraud detection methods

Financial institutions and merchants fight against fraud at two levels: fraud prevention and fraud detection (Bolton & Hand, 2001). Fraud prevention pertains to all activities and practices engaged in stopping fraud from happening in the first place. An example of fraud prevention is the practice of credit card activation before its first use to prevent theft of credit cards from surface mails. Internet security systems for credit card transactions are another example of fraud prevention. Pin numbers for debit cards are another example of fraud prevention, as perpetrators need to know the pin number and have physical possession of the debit cards in order to withdraw money from ATMs.

Fraud detection, on the other hand, pertains to practices and systems to quickly detect fraudulent transactions as soon as these transactions take place (Bolton & Hand, 2001). The sooner fraudulent transactions are detected the more losses can be avoided by stopping transactions made with fraudulent credit cards. Fraud detection is a continuous activity as there is no way to know if fraud prevention has failed and which transactions are fraudulent. Statistical fraud detection methods have been classified into two broad categories: 'supervised' and 'unsupervised' (Bolton & Hand, 2001).

In supervised statistical methods, estimated statistical models are used to discriminate between fraudulent and non-fraudulent purchase behavior to classify new observations into an appropriate class: fraudulent or non-fraudulent transaction (Bolton & Hand, 2001). The performance of models is assessed by measuring their accuracy in correctly classifying new observations as fraudulent or non-fraudulent. Supervised statistical methods have three important characteristics. First, supervised statistical methods require samples of both classes, fraudulent and legitimate observations, as models are trained based on examples of observations in both classes. Second, supervised statistical models can only detect frauds that have occurred and have been detected previously (Bolton & Hand, 2001). This method cannot detect new kinds of fraud. Hence, the training datasets should have all kinds of fraudulent transactions for appropriate performance of statistical models, and the sample classes have to be periodically updated to include newer kinds of fraud.

Previous research on credit card frauds employing supervised methods can be divided into three categories (Bolton & Hand, 2002): traditional statistical classification methods, rule-based methods, and recent development of power tools. Examples of traditional statistical classification methods are linear discriminant analysis and logistic regression (Hand, 1981; McLachlan, 1992). Rule-based methods, such as tree-based algorithms (Breiman, Friedman, Olshen, & Stone, 1984; Quinlan, 1993) are supervised learning algorithms that use rules of *If* (fulfills certain conditions) ... *Then* (appropriate category). Examples of recent sophisticated "power tool" methods of classification are neural networks (Hand, 1997; Quah & Sriganesh, 2008; Ripley, 1996; Webb, 1999), SVMs (Whitrow et al., 2009), and Random Forest (Whitrow et al., 2009). Kou, Chang-Tien, Sirwongwattana, and Huang (2004) provide a summary of fraud detection techniques used in past research. Phua, Lee, Smith, and Gayler (2005) have done comprehensive survey of data mining based fraud detection research. Bose (2006) has reviewed existing intelligent technologies for managing fraud and identity theft.

Although prior studies have proposed different techniques and algorithms for credit card fraud detection, a number of studies were done in an experimental setup and very few studies used real credit card data. In this research, we use a dataset of real-life credit card transactions to estimate a supervised statistical model.

Unsupervised methods attempt to detect unusual observations, such as customers, transactions, or accounts whose behavior may be different from the norm. These unusual observations, different from the baseline normal behavior, are identified for closer examination and subsequent classification. Unlike supervised methods, unsupervised methods do not require samples of fraudulent and legitimate transactions. Hence, unsupervised methods may find use in situations where there is no prior knowledge of classes of observations. The other advantage of unsupervised methods over supervised method is that previously undiscovered frauds can be detected, while supervised methods can only be trained to detect the kinds of frauds in historical databases. However, unsupervised methods, compared to supervised methods, have been less popular in fraud detection and have not received much attention in fraud detection literature (Bolton & Hand, 2001).