INTELLIGENT AUTOMATION & SOFT COMPUTING, 2017
https://doi.org/10.1080/10798587.2017.1342415

A Novel Cardholder Behavior Model for Detecting Credit Card Fraud

Yiğit Kültür and Mehmet Ufuk Çağlayan

Computer Engineering Department, Boğaziçi University, Istanbul, Turkey

ABSTRACT

Because credit card fraud costs the banking sector billions of dollars every year, decreasing the losses incurred from credit card fraud is an important driver for the sector and end-users. In this paper, we focus on analyzing cardholder spending behavior and propose a novel cardholder behavior model for detecting credit card fraud. The model is called the Cardholder Behavior Model (CBM). Two focus points are proposed and evaluated for CBMs. The first focus point is building the behavior model using single-card transactions versus multi-card transactions. As the second focus point, we introduce holiday seasons as spending periods that are different from the rest of the year. The CBM is fine-tuned by using a real credit card transaction data-set from a leading bank in Turkey, and the credit card fraud detection accuracy is evaluated with respect to the abovementioned two focus points.

KEYWORDS

Artificial intelligence; fraud detection; credit card; unsupervised learning; clustering

1. Introduction

The global plastic card business size was $21.60 trillion in 2012. Fraud losses were approximately $11.27 billion. The loss was 5.22¢ per $100 (HSN Consultants Inc., 2013). Banks aim to decrease their losses resulting from plastic card fraud.

Rule-based tools are commonly used in banks for credit card fraud detection. In rule-based tools, rules are derived from the experience of fraud experts and investigation results. A transaction is evaluated according to the rule-set, and an alarm is raised if it fits one or more rules. Such tools are successful in coping with previously observed fraud patterns. However, rule-based tools have an important drawback. A considerable number of fraudulent transactions matching a rule must have occurred before adding a new rule to the rule-set. In other words, the rule induction process takes some time, and fraud strategies may change during the rule induction period (Krivko, 2010).

Artificial intelligence (AI)-based tools are developed to work together with rule-based tools. AI models are considered mainly in two groups; supervised and unsupervised approaches. Both approaches have been used in credit card fraud detection. In supervised fraud detection, previously occurring fraudulent and legitimate transactions are used for training. Supervised approaches require accurate labeling of past fraudulent transactions as fraudulent or legitimate. Moreover, supervised approaches can only be used to detect fraud of a type that has previously occurred (Ganji & Mannem, 2012). In unsupervised fraud detection, the spending behavior of each cardholder is modeled by using past transactions. If an occurring transaction does not fit in the behavior model, it is considered as potentially fraudulent. An advantage of using unsupervised approaches over supervised approaches is that previously undiscovered types of fraud may be detected. Moreover, there is no need for accurate labeling of past fraudulent transactions. Major unsupervised approaches are k-nearest neighbors (Ganji & Mannem, 2012), distance-based (Jha, Guillen, & Westland, 2012; Ju & Wang, 2009; Krivko, 2010; Yu & Wang, 2009) and tree-based (Philip & Sherly, 2012).

In this paper, we focus on analyzing cardholder spending behavior and propose a novel cardholder behavior model for detecting credit card fraud. The model is called the Cardholder Behavior Model (CBM). Two focus points are proposed and evaluated for CBMs. The initial version of CBM, which lacks focus points, has been previously introduced by the authors (Kultur & Caglayan, 2015).

The first focus point is building the behavior model using single-card transactions versus multi-card transactions. In the single-card approach, the behavior of the cardholder for each card is evaluated separately to build card-specific models. In the multi-card approach, transactions from different cards of the cardholder are evaluated together to build a cardholder-specific model. As the second focus point, we introduce holiday seasons as spending periods that are different from the rest of the year. This idea originated as a result of data regarding spending statistics for holiday seasons such as Christmas, New Year's and other religious holidays. Cardholders spend more during such holidays (Shen, 2011; Visa Europe, 2011). As far as we know, these focus points have not been previously discussed in the credit card fraud detection domain.

The remainder of this paper is structured as follows: In Section 2, we provide background information regarding the credit card and credit card fraud detection literature. In Section 3, we discuss in detail the proposed model, focus points and implementation. In Section 4, we describe the data-set and evaluation criteria used and proceed with analyzing the experimental results. In Section 5, the concluding remarks are stated, and future work is discussed.

2. Background

Credit cards have been an important part of everyday life for more than half a century. The first universal credit card,

CONTACT Yiğit Kültür yigit.kultur@boun.edu.tr

which could be used at a variety of stores or businesses, was introduced by Diners Club in 1950. In 1959, the number of Diners Club cardholders reached one million (Diners Club, 2014). As another leading actor of the credit card industry, American Express entered the market in 1958. Two hundred and fifty thousand cards were issued prior to the official launch date (Grossman, 1987). The first cards were slips of paper with the account number and cardholder's name typed on them. In 1959, American Express began issuing plastic cards. In 1958, Bank of America became the first bank to issue a credit card with the BankAmericard brand. Initially, this card could be used only in the state of California. In 1974, the BankAmericard program went global. In 1976, BankAmericard became Visa (Visa, 2015). In 1966, Master Charge was introduced by several banks in California to compete with BankAmericard. In 1979, it was renamed MasterCard (Mastercard, 2014). Today, there are approximately 5 billion cards in the world. With these cards, people made transactions worth approximately $21.60 trillion in 2012 (HSN Consultants Inc., 2013).

Naturally, such a huge amount in the credit card domain draws the attention of fraudsters. The global plastic card fraud losses were approximately $11.27 billion in 2012 (HSN Consultants Inc., 2013). This amount means that 5.22¢ of each $100 went into fraudsters' pockets. In fact, decreasing plastic card fraud losses has always been one of the basic aims of banks. For this purpose, fraud detection experts have been hired, and fraud detection tools have been implemented.

Rule-based systems have been the common fraud detection tools for banks. In these systems, fraud experts define the rules according to past cases and investigation results. If a new transaction matches one or more of the previously defined rules, an alarm is raised to indicate that the new transaction is potentially fraudulent. The rule-based approach is successful for previously observed fraud patterns. On the other hand, it has the disadvantage of not being agile. Before adding a new rule to the existing rule-set, a considerable number of fraudulent transactions matching the rule must have occurred. This requires a long time. In this period, the fraud strategies may change, causing the induced rule to expire (Krivko, 2010).

The size of the credit card industry and amount of credit card fraud has caught the attention of not only fraudsters, but also researchers. Previously, many approaches have been proposed to detect credit card fraud. The proposed ideas are mainly based on artificial intelligence (AI). In the literature, AI models are grouped into two groups; supervised and unsupervised. Both supervised and unsupervised approaches have been used in credit card fraud detection. In supervised fraud detection, all fraudulent and legitimate transactions are used to train the AI model. The resulting AI model decides whether a new transaction is fraudulent or legitimate. The training process of the AI model is repeated to include recent transactions. In unsupervised fraud detection, the behavior of a cardholder is modeled using past legitimate transactions. Thereafter, an occurring transaction is analyzed regarding whether it is inside or outside the cardholder behavior. If the transaction is outside the cardholder behavior, an alarm is raised.

The previously proposed AI models for credit card fraud detection are summarized in Table 1 and Table 2. Note that several AI models have been used in this domain. Tree-based models, unsupervised models, neural network-based models, Bayesian models and genetic algorithms appear to be more popular than the others.

Table 1. Unsupervised Approaches for Credit Card Fraud Detection.

AI Model	References
K-nearest neighbors	Yu & Wang, 2009;
Distance-Based	Ju & Wang, 2009;
Tree-Based	Krivko, 2010;
	Ganji & Mannem, 2012;
	Philip & Sherly, 2012;
	Jha et al., 2012

Table 2. Supervised Approaches for Credit Card Fraud Detection.

AI Model	References
Decision Trees (DT) Random Forest (RF)	Gadi, Wang, & Lago, 2008a; Gadi et al., 2008b; Patil, Karad, Wadhai, Gokhale, & Halgaonkar, 2010; Sherly & Nedunchezhian, 2010; Bhattacharyya, Jha, Tharakunnel, & Westland, 2011; Sahin & Duman, 2011a; Alowais & Soon, 2012;
Neural Networks (NN)	Aleskerov, Freisleben, & Rao, 1997; Maes, Tuyls, Vanschoenwinkel, & Manderick, 2002; Gadi et al., 2008a; Gadi et al., 2008b; Sahin & Duman, 2011b;
Bayesian Networks (BN)	Maes et al., 2002; Filippov, Mukhanov, & Shchukin, 2008; Gadi et al., 2008a; Gadi et al., 2008b; Panigrahi, Kundu, Sural, & Majumdar, 2009;
Naïve Bayes (NB)	Filippov et al., 2008; Gadi et al., 2008a; Gadi et al., 2008b; Alowais & Soon, 2012;
Support Vector Machines (SVM)	Chen, Chen, Chien, & Yang, 2005;Bhattacharyya et al., 2011;Sahin & Duman, 2011a;Ganji & Mannem, 2012;
Genetic Algorithm (GA)	Ma & Li, 2009; Ozcelik, Isik, Duman, & Cevik, 2010; Duman & Ozcelik, 2011;
Artificial Immune System (AIS)	Gadi et al., 2008a; Gadi et al., 2008b;
Logistic Regression	Bhattacharyya et al., 2011; Sahin & Duman, 2011b;
Hidden Markov Model (HMM)	Bhusari & Patil, 2011; Rani, Kumar, Mohan, & Shankar, 2011;
Fuzzy Logic	Bentley, Kim, Jung, & Choi, 2000; Sanchez, Vila, Cerda, & Serrano, 2009;
Sequence Alignment	Kundu, Sural, & Majumdar, 2006; Kundu, Panigrahi, Sural, & Majumdar, 2009;
Scatter search	Duman & Ozcelik, 2011;
Self-Organizing Maps (SOM)	Quah & Sriganesh, 2008;
Influence Diagram	Cobb, 2010

3. Cardholder Behavior Model for Credit Card Fraud Detection

In this paper, we focus on analyzing cardholder spending behavior and propose a novel cardholder behavior model for detecting credit card fraud. The model is called the Cardholder Behavior Model (CBM). In this section, we will discuss details of the CBM, two focus points of the CBM and the CBM software implementation. In the first subsection, we will discuss the CBM for the credit card fraud detection process. In the second subsection, we will discuss clustering algorithms. In the third subsection, we will discuss the single-card versus multi-card focus. In the fourth subsection, we will discuss the holiday spending focus. In the last subsection, we will discuss the CBM software implementation.

3.1. CBM in Credit Card Fraud Detection Process

Our credit card fraud detection approach contains credit card holders, credit cards, credit card transactions, Credit

Card Transactions Database and several Cardholder Behavior Models. The overall view of this process is given in Figure 1. Credit card holders, called cardholders in short, may have one or more credit cards and generate credit card transactions for each of their credit cards. Credit card transactions are stored in the Credit Card Transactions Database. In this research, only principal card transactions are used. Additional card transactions are ignored, because additional cards are used by different people, such as the principal cardholder's family members, who have different spending behaviors. Thus, additional card transactions cannot be used for building Cardholder Behavior Models.

A credit card transaction has six attributes. The transaction attributes are; cardholder number, card number, merchant category code, amount, date and time. The cardholder number is a unique number identifying a bank cardholder. A person cannot have multiple cardholder numbers. The card number is a 16-digit unique number identifying a credit card. A Merchant Category Code (MCC) is a four-digit number used by the bankcard industry to classify suppliers into market segments. There are approximately 600 MCCs that denote various types of business (Visa USA, 2004).

One CBM is trained for each cardholder and MCC. For example, if a cardholder having three credit cards has credit card transactions in a supermarket (MCC: 5411) and in a jewelry store (MCC: 5094), one CBM is trained with supermarket transactions and one CBM is trained with jewelry store transactions for that cardholder. Each CBM may have transactions from the three different credit cards.

The CBM decision process starts with the occurrence of a new transaction. When a cardholder makes a new transaction, the corresponding CBM is retrieved by using the cardholder number and MCC of the new transaction. The corresponding CBM makes the decision whether the transaction is legitimate or fraudulent. The CBM decision process is detailed in Figure 2.

3.2. CBM Clustering Algorithms

The main approach in a CBM for deciding whether a new transaction is legitimate or fraudulent is clustering. If there

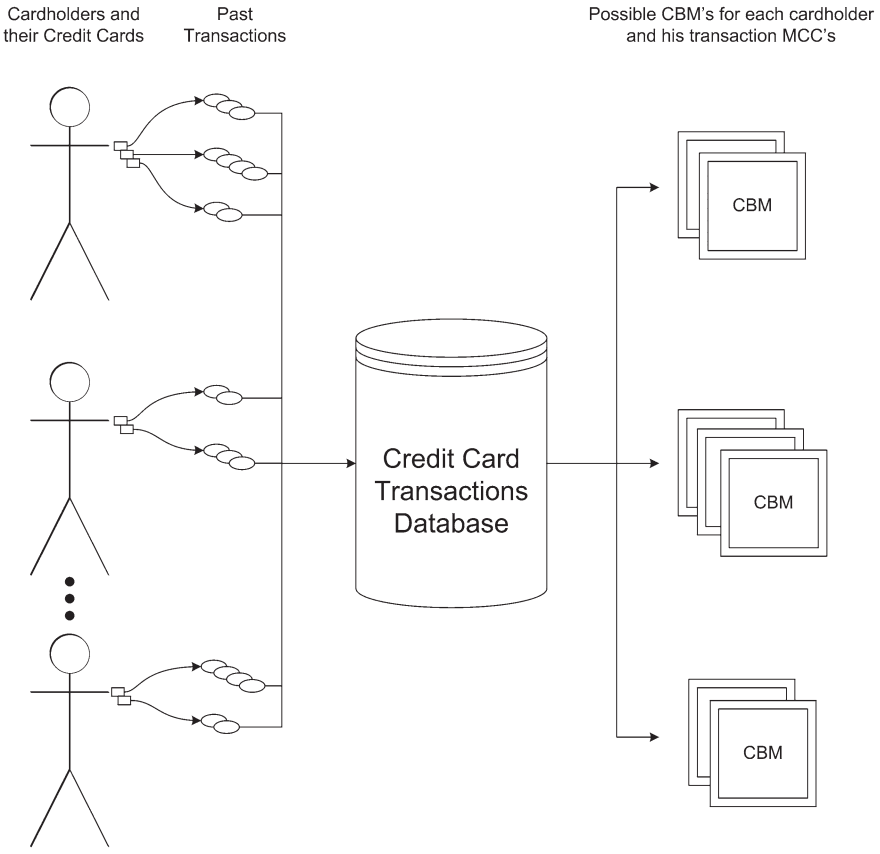

Figure 1. Overall View of a CBM in the Credit Card Fraud Detection Process.

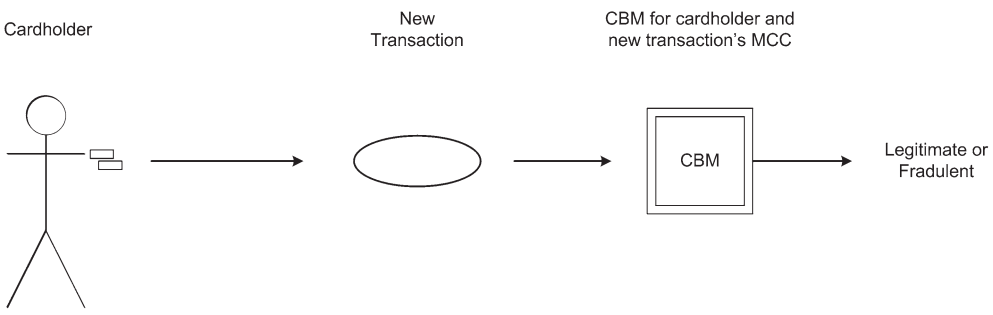

Figure 2. CBM Decision Process.

are no past transactions, clustering is not possible, and the CBM may decide that the new transaction is fraudulent. For example, the cardholder makes a new credit card transaction in a supermarket. The corresponding CBM is the one, which is trained by using the past supermarket transactions of the cardholder. The amounts of these purchases are fed into the clustering algorithm. In this case, assume that the cardholder has past supermarket transactions with amounts of 50.00, 65.00, 150.00 and 165.00. The clustering process is shown in Figure 3. The past transaction amounts are shown as blue diamonds. Formed clusters are shown as red ovals. The new transaction, which is shown as a red square, has an amount of 400.00 and does not fall into any of the clusters. Consequently, CBM decides that the new transaction is fraudulent. If the cardholder makes a new credit card transaction in a jewelry store for the first time, a corresponding CBM is not found (i.e., clustering is not possible), and an alarm is raised.

In this research, the number of clusters is previously unknown. Therefore, clustering algorithms that do not require the number of clusters a priori are selected as candidate algorithms. The candidate algorithms are COBWEB, DBSCAN and Expectation Maximization (EM) (Sharma, Bajpai, & Ritoriya, 2012). The Experimenter GUI of Weka is used to evaluate the candidate algorithms using sample cases (Hall et al. 2009). As the result of evaluation, the Expectation Maximization (EM) clustering algorithm is selected for clustering amount values (Dempster, Laird, & Rubin, 1977). EM clustering determines the number of clusters via cross-validation. For each cluster formed, we subtracted 10 percent from the minimum amount in the cluster and added 10 percent to the maximum amount in the cluster to provide the minimum and maximum borders of the cluster.

3.3. Single-card versus Multi-card Focus CBMs

To the best of our knowledge, former unsupervised fraud models have been built using card-specific transaction data. However, a cardholder may hold multiple cards issued by the same bank. Therefore, constructing a behavior model based on all cards of a cardholder rather than a single card is expected to improve the fraud detection performance.

The single-card versus multi-card focus point is detailed in Figure 4, in which the cardholder has three credit cards; 1234********1261, 1234********2737 and 1234********9863. The cardholder made four transactions with 1234********1261, two transactions with 1234********2737 and three transactions

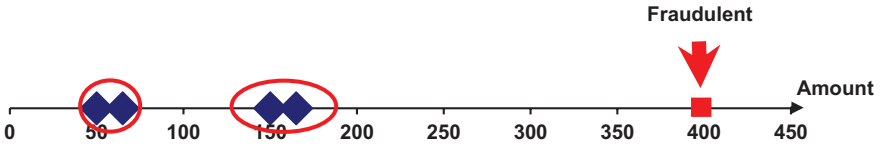

Figure 3. Clusters Formed from Past Supermarket Purchase Transactions and the New Supermarket Purchase Transaction.

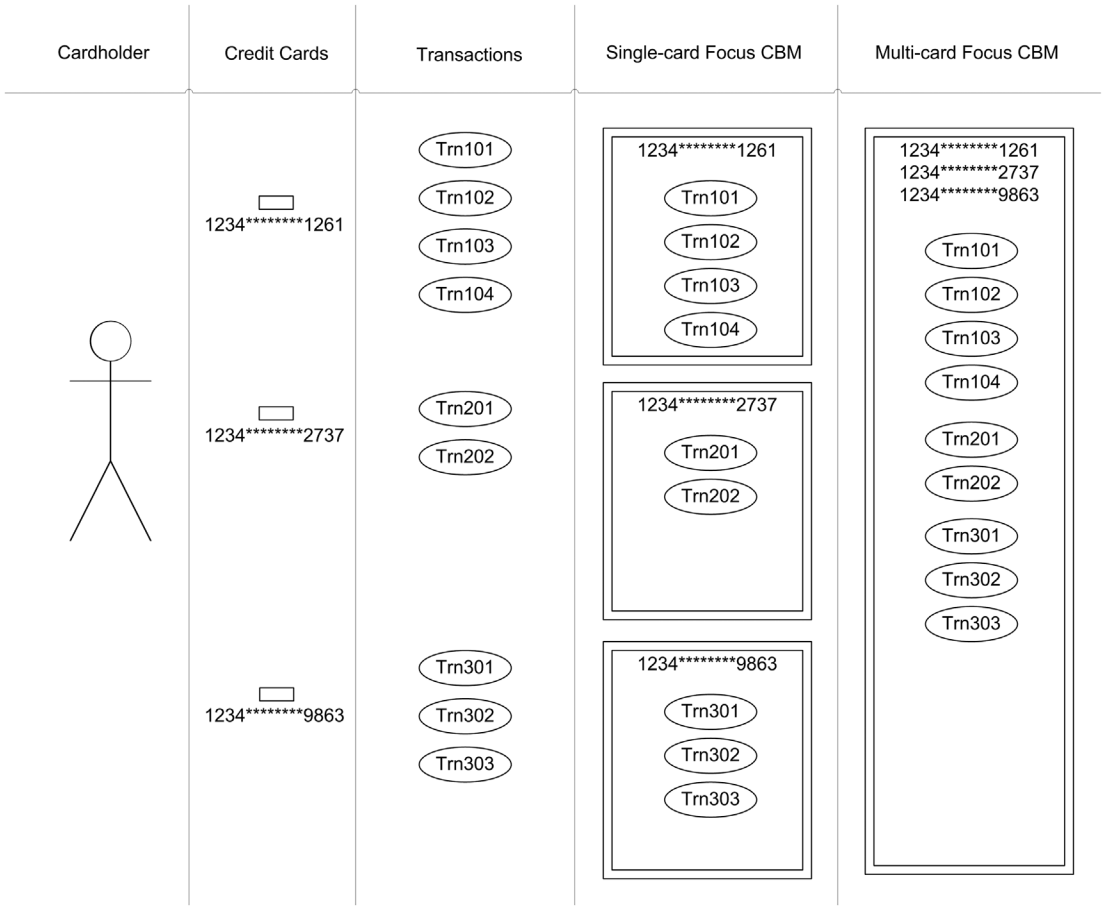

Figure 4. Single-card Focus versus Multi-card Focus CBMs.

Table 3. Transactions with a Single Credit Card.

Cardholder No	Card No	MCC	Amount	Date	Time
12345	6789********4321	5411	150.00	03/04/2012	19:25
12345	6789********4321	5411	132.00	10/04/2012	15:00
12345	6789********4321	5411	77.85	12/05/2012	20:05
12345	6789********4321	5094	7500.00	17/05/2012	20:22
12345	6789********4321	5094	12000.00	20/06/2012	19:37
12345	6789********4321	5411	170.09	15/07/2012	19:45

Table 4. New Supermarket Purchase Transaction for the Credit Card.

Cardholder No	Card No	MCC	Amount	Date	Time
12345	6789********4321	5411	350.00	19/08/2012	19:54

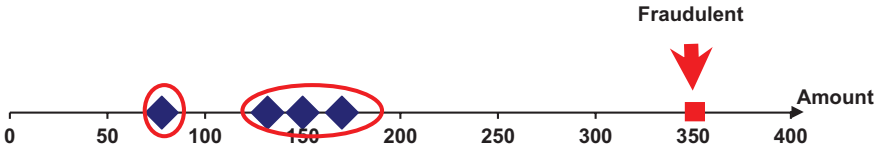

Figure 5. Clusters Formed from Past Supermarket Purchase Transactions and the New Supermarket Purchase Transaction.

Table 5. Transactions with the Cardholder's Other Credit Card.

Cardholder No	Card No	MCC	Amount	Date	Time
12345	3456********0912	4511	1800.00	07/03/2012	17:45
12345	3456********0912	4511	750.00	19/04/2012	19:02
12345	3456********0912	4511	150.00	27/05/2012	19:30
12345	3456********0912	5411	128.00	10/06/2012	15:00
12345	3456********0912	4511	1500.00	30/06/2012	18:00

Table 6. New Airline Purchase Transaction for the Credit Card.

Cardholder No	Card No	MCC	Amount	Date	Time
12345	6789********4321	4511	1600.00	19/09/2012	21:54

with 1234********9863. Three separate CBMs could be built for each of his credit cards. For each of these CBMs, only those transactions made with the corresponding credit card are used. This approach is called the single-card focus CBM. Alternatively, one CBM can be built using transactions made with all cards of that cardholder. This approach is called the multi-card focus CBM.

For further clarification, an example is given using sample transactions. To begin, the transaction records for a cardholder can be seen in Table 3. In Table 3, transactions have two different MCCs; MCC: 5411 indicates "Grocery Stores, Supermarkets", and MCC: 5094 indicates "Precious Stones and Metals, Watches and Jewelry".

Note that the cardholder has made four supermarket (MCC: 5411) purchases and two jewelry (MCC: 5094) purchases using the same card. He has spent amounts between 77.85 and 170.09 in a supermarket, while he has spent amounts between 7500.00 and 12000.00 in a jewelry store. Based on these records, it is obvious that the amount ranges for different MCCs may be different. Therefore, transactions with different MCCs are considered separately. Now, suppose that the cardholder makes a new supermarket purchase, the transaction record of which is shown in Table 4.

Until that time, the cardholder's supermarket purchase amounts had been between 77.85 and 170.09. These past transactions are shown as blue diamonds in Figure 5. The clusters formed by these transactions are shown as red ovals. The new transaction of amount 350.00 is shown as a red square. As seen in Figure 5, the new transaction falls outside the two clusters formed. In this situation, the CBM gives an alarm indicating that the cardholder has behaved in a different manner.

Let us assume that our example cardholder holds a second credit card with the transactions listed in Table 5. The cardholder has made four airline (MCC: 4511) purchases and one supermarket (MCC: 5411) purchase using this card.

Now, suppose that the cardholder makes an airline ticket purchase (MCC: 4511), the transaction record of which is shown in Table 6.

The airline ticket purchase in Table 6 has been made using the card with the four supermarket (MCC: 5411) purchases and two jewelry (MCC: 5094) purchases. If just the transactions of that card are considered and the other transactions of the cardholder are ignored, an alarm is raised, because there are no previous airline ticket purchases for that card. However, if all transactions of that cardholder are considered, it is noticed that the cardholder has made four airline purchases before. These past purchases are plotted as blue diamonds in Figure 6. The clusters are shown as red ovals. The new transaction in Table 6, which is plotted as a red square in Figure 6, falls into one of these clusters. Therefore, this new transaction matches the airline ticket purchase behavior of the cardholder. Thus, the CBM does not raise an alarm.

Focusing on such scenarios, the fraud detection performances of the single-card and multi-card focus CBMs are

evaluated. To the best of our knowledge, this focus point is the first in the credit card fraud detection domain.

3.4. Holiday Season Spending Focus CBM

In most countries, there are holidays such as New Year's and religious holidays. It is known that spending is usually higher during holiday seasons. For example, Christmas is the biggest holiday in the United States. Black Friday is the Friday following Thanks giving Day in the United States, often regarded as the beginning of the Christmas shopping season. In 2011, each of the 152 million Black Friday shoppers spent approximately $400 on average, resulting in $52 billion in sales (Shen, 2011). A similar spending behavior is seen also in Europe. Irish consumers spent approximately €257 million, with an average of €155, on online Christmas shopping (Visa Europe, 2011). Therefore, it is obvious that holiday seasons should be taken into consideration while building a behavior model for credit card fraud detection.

The holiday season spending focus point is detailed in Figure 7. A cardholder having one credit card made two transactions during the holidays and two transactions on other days. Two separate CBMs can be trained; one for holidays and one for the other days. For each of these CBMs, only transactions made within the corresponding days are used. This approach is called the holiday season focus CBM. Alternatively, one CBM can be built for all days. In this approach, all transactions throughout a year are used. This approach is called the all-time CBM and treats the whole year as a homogeneous spending period.

To explain the holiday season focus point using an example, the transactions of a cardholder shown in Table 7 are used. Because this research is evaluated using the transaction data-set from a Turkish bank, Turkish holidays are considered. These include two religious holidays, which are depicted as Holiday 1 and Holiday 2, and New Year's Day. It is expected that if transactions within a number of days before the start of a holiday are considered, the holiday season spending focus will be meaningful.

The cardholder makes clothing (MCC: 5651) purchases during the holiday seasons, with amounts between 800.00 and 1250.00.

However, the clothing purchase amounts are between 100.00 and 132.00 on non-holidays. In other words, the cardholder spends much more for clothing during holidays.

Now, suppose that the card is stolen and a fraudulent clothing purchase is made, as given in Table 8.

The transaction date is not a holiday. If holidays are considered as periods of different spending behavior, then, this transaction should be evaluated considering previous non-holiday

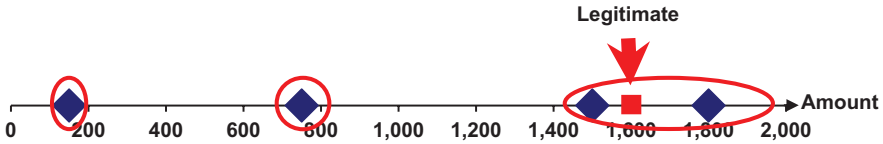

Figure 6. Clusters Formed from Past Airline Purchase Transactions (the Other Card) and the New Transaction.

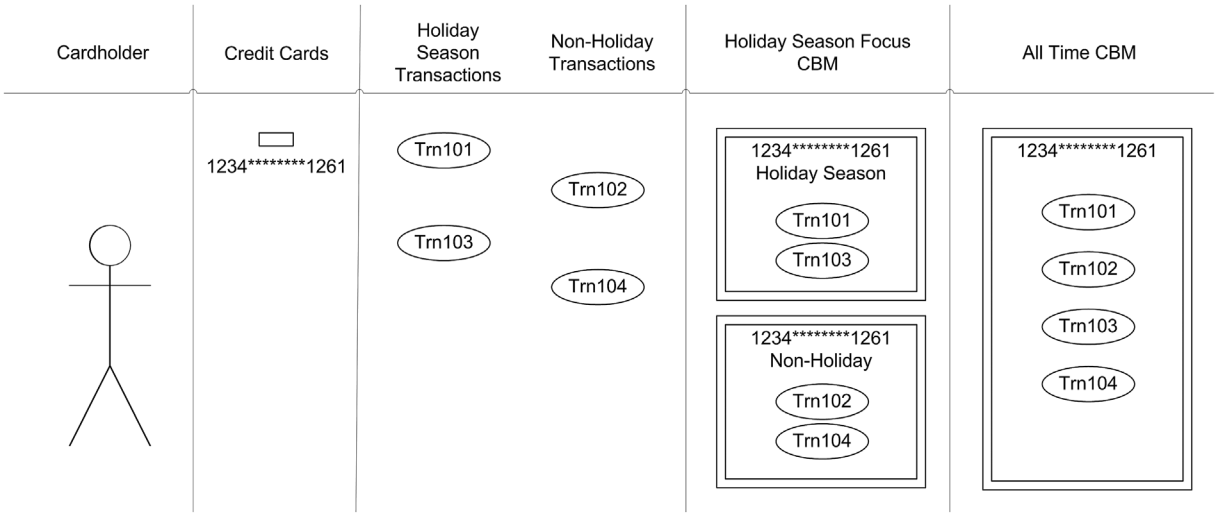

Figure 7. Holiday Season Focus CBM versus All-time CBM.

Table 7. Transactions During or Outside of Holiday Seasons.

Cardholder No	Card No	MCC	Amount	Date	Time	Holiday
35791	4680********5791	5651	125.00	09/07/2012	17:45	No
35791	4680********5791	5651	1150.00	16/08/2012	19:25	Holiday 1
35791	4680********5791	5651	132.00	13/09/2012	15:00	No
35791	4680********5791	5651	1250.00	22/10/2012	19:12	Holiday 2
35791	4680********5791	5651	100.00	11/11/2012	20:05	No
35791	4680********5791	5651	800.00	30/12/2012	20:22	New Year's

transactions. These previous transactions are shown as blue diamonds in Figure 8. One cluster is formed, which is shown as a red oval. The new transaction, shown as a red square, does not fall into that cluster. Therefore, the CBM raises an alarm regarding the new transaction, and the fraudulent transaction is rejected.

If the holidays are not considered as special spending periods, the CBM does not raise an alarm for this transaction, because there are past transactions close to this amount. Details can be seen in Figure 9, in which all past clothing transactions of the cardholder are shown as blue diamonds. The three clusters formed are shown as red ovals. The new transaction is shown as a red square. This new transaction falls into one of the clusters. Therefore, an alarm is not raised regarding the fraudulent transaction worth 1200.00.

Focusing on such scenarios, the fraud detection performances of the holiday season focus CBM and all-time CBM are evaluated. To the best of our knowledge, this focus point is also the first in the credit card fraud detection domain.

3.5. CBM Software Tool

The CBM Software Tool has been developed to implement CBMs with different focus points and evaluate their fraud detection performances. The CBM Software Tool is developed in Microsoft Visual Studio 2010, contains approximately 3000 lines of C# code, runs on Microsoft.NET Framework 4.0 and uses Microsoft SQL Server 2008 as its database engine. The Expectation Maximization (EM) clustering algorithm, provided by WEKA Data Mining Software, is used in the tool (Hall et al., 2009). The CBM Software Tool has an application programming interface so that it may be integrated into a bank's credit card system.

4. CBM Fraud Detection Evaluation

4.1. CBM Evaluation Data-set

A leading bank in Turkey has provided a real-life credit card transaction data-set for CBM evaluation. The transaction data-set is called the CBM Evaluation Data-set in this paper. The CBM Evaluation Data-set contains 152,706 credit card transactions of 105 cardholders. The transactions in the CBM Evaluation Data-set occurred between January 2006 and February 2013. More than half of the cardholders in the data-set hold more than one card as shown in Table 9.

In the CBM Evaluation Data-set, some transactions have been flagged as fraudulent, whereas the rest have been flagged as legitimate. In the bank's credit card system, a transaction is flagged as fraudulent in primarily two situations. In the first situation, the rule-based fraud detection of a bank system gives an alarm for an occurring transaction, and the fraud call-center of the bank calls the cardholder immediately to inform them regarding the suspicious transaction. If it is understood that the transaction has not been made by the cardholder, it is flagged as fraudulent. In the second situation, transactions that have not been made by the cardholder are listed in the credit card statement, and the cardholder calls the bank's fraud call-center to inform them regarding the situation. Thus, the corresponding transactions are flagged as fraudulent. The data-set does not contain cardholders' personal information, such as age and gender, because the bank did not provide personal information according to the bank privacy policy.

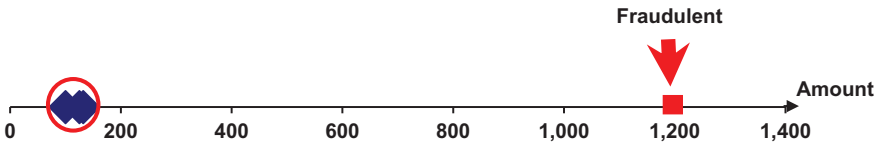

Figure 8. Clusters Formed from Past Non-holiday Clothing Purchase Transactions and the Fraudulent Clothing Purchase Transaction.

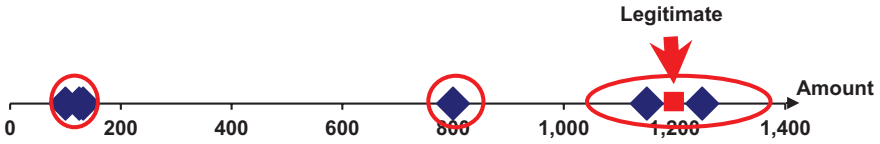

Figure 9. Clusters Formed from all Past Clothing Purchase Transactions and the Fraudulent Clothing Purchase Transaction.

Table 8. Fraudulent Clothing Purchase Transaction for the Credit Card.

Cardholder No	Card No	MCC	Amount	Date	Time	Holiday
35791	4680********5791	5651	1200.00	10/01/2013	21:30	No

Table 9. Cardholder Card and Transaction Counts in CBM Evaluation Data-set.

	Cardholder Count	Card Count	Legitimate Transaction Count	Fraudulent Transaction Count	Total Transaction Count
Cardholders with 1 card	52	52	75,193	618	75,811
Cardholders with 2 cards	42	84	60,658	352	61,010
Cardholders with 3 cards	7	21	10,107	17	10,124
Cardholders with 4 cards	4	16	5,729	32	5,761
All Cardholders	105	173	151,687	1,019	152,706

4.2. CBM Evaluation Criteria

Binary classification is the task of classifying elements into two groups based on a classification rule. Credit card fraud detection is a binary classification problem in which a credit card transaction is labeled either fraudulent or legitimate. As in all binary classification problems, evaluating the fraud detection performance of a model is based on comparing the number of alarms with the number of exact labels for fraudulent and legitimate transactions. Therefore, criteria that have become standards for binary classification model evaluation are used. The criteria used are sensitivity, specificity, false positive rate, precision, negative predictive value and accuracy.

The main results of CBM evaluation could be interpreted in terms of alarm types. True Positive (TP) is the number of fraudulent transactions for which correct alarms are raised, i.e., the number of detected fraudulent transactions. False Positive (FP) is the number of legitimate transactions for which false alarms are raised. True Negative (TN) is the number of legitimate transactions for which no alarm is raised. False Negative (FN) is the number of fraudulent transactions for which no alarm is raised, i.e., the number of missed fraudulent transactions.

The sensitivity measures the proportion of actual positives that are detected correctly. In our research, this is the percentage of fraudulent transactions for which the CBM raises an alarm. The equation for the sensitivity is given below

$$Sensitivity = \frac{TP}{TP + FN} \tag{1}$$

Where the sum of TP and FN gives the total number of fraudulent transactions.

The specificity measures the proportion of negatives that are correctly identified. In our research, this is the percentage of legitimate transactions for which the CBM does not raise an alarm. The equation for the specificity is given below

$$Specificity = \frac{TN}{FP + TN} \tag{2}$$

Where the sum of FP and TN gives the total number of legitimate transactions.

The false positive rate measures the proportion of negatives that are falsely identified. In this research, this is the percentage of legitimate transactions for which the CBM raises an alarm. The equation for the false positive rate is given below

$$FalsePositiveRate = 1 - Specificity \tag{3}$$

The precision measures the proportion of true positives among all positives. In our research, this is the percentage of true alarms among all alarms. The equation for the precision is given below

$$Precision = \frac{TP}{TP + FP} \tag{4}$$

Where the sum of TP and FP gives the total number of alarms.

The negative predictive value measures the proportion of true negatives among all negatives. In our research, this is the percentage of true "no alarm" decisions among all "no alarm" decisions. The equation for the negative predictive value is given below

$$NegativePredictiveValue = \frac{TN}{TN + FN} \tag{5}$$

Where the sum of TN and FN gives the total number of "no alarms".

Table 10. CBM Evaluation Setup.

	Fraudulent	Legitimate	Total
Training, January 2006—December 2012	0	150,957	150,957
Test, January 2013—February 2013	37	730	767

The accuracy is the proportion of correct decisions among all decisions. In our research, this is the percentage of alarms for fraudulent transactions and "no alarms" for legitimate transactions among all transactions. The equation for the accuracy is given below

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \tag{6}$$

Where the sum of TP and FN gives the total number of correct decisions, whereas the sum of TP, FN, FP and TN gives the total number of decisions.

4.3. CBM Evaluation Method

The CBM Evaluation Data-set contains over 152,706 transactions of 105 cardholders. These transactions occurred between January 2006 and February 2013. Each cardholder in this data-set has past transaction counts between 1440 and 1499. The transactions that occurred from January 2006 until the end of 2012 are used for training CBMs. The total number of training transactions is 150,957, and all are legitimate, i.e., all transactions that are marked as fraudulent are ignored, because exact cardholder behavior is being modeled. The transactions that occurred in 2013 are used for testing CBMs. The total number of test transactions is 767; 37 of them are fraudulent. The evaluation setup is summarized in Table 10. To determine the statistical significance of the results, t-tests with 95% confidence intervals are conducted.

4.4. CBM Experimental Results and Analysis

This section is organized in terms of the two focus points for CBMs.

4.4.1. Focus Point 1: Single-card versus Multi-card Focus CBMs

Single-card versus Multi-card Focus CBMs aim to analyze the single-card and multi-card CBMs. To the best of our knowledge, previous unsupervised fraud models have been built using card-specific transaction datasets. However, as noted in the CBM Evaluation Data-set, a cardholder may hold multiple cards issued by the same bank. Therefore, CBMs for all cards of a cardholder rather than a single card have been built.

As seen in the sensitivity column of Table 11, single-card CBMs have significantly higher sensitivities than multi-card CBMs. In other words, single-card CBMs detected more fraudulent transactions than multi-card CBMs.

Multi-card CBMs have significantly higher specificities than single-card CBMs, as seen in the specificity column of Table 11. In other words, multi-card CBMs have smaller false alarm rates than single-card CBMs. The same fact can also be seen in the false positive rate column of Table 11. In the worst case, single-card CBMs give false alarms for 27.12% of legitimate transactions, whereas multi-card CBMs give false alarms for 19.04% of legitimate transactions.

Table 11. Evaluation Results for Multi-card and Single-card CBMs.

	Sensitivity		Specificity		False Positive Rate		Precision		Negative Predictive Value		Accuracy	
Consider Holidays	Multi-card	Single-card	Multi-card	Single-card	Multi-card	Single-card	Multi-card	Single-card	Multi-card	Single-card	Multi-card	Single-card
No	43.24%	**54.05%**	**80.96%**	72.88%	**19.04%**	27.12%	**10.32%**	9.17%	96.57%	96.90%	**79.14%**	71.97%
Yes	45.95%	**56.76%**	**81.78%**	73.42%	**18.22%**	26.58%	**11.33%**	9.77%	96.76%	97.10%	**80.05%**	72.62%

Bold values indicate better fraud detection performance results.

Table 12. Evaluation Results for Holiday Season Focus CBMs and All-time CBMs.

	Sensitivity		Specificity		False Positive Rate		Precision		Negative Predictive Value		Accuracy	
Single-card / Multi-card	Cons. Holidays: No	Cons. Holidays: Yes	Cons. Holidays: No	Cons. Holidays: Yes	Cons. Holidays: No	Cons. Holidays: Yes	Cons. Holidays: No	Cons. Holidays: Yes	Cons. Holidays: No	Cons. Holidays: Yes	Cons. Holidays: No	Cons. Holidays: Yes
Multi-card	43.24%	**45.95%**	80.96%	81.78%	19.04%	18.22%	10.32%	**11.33%**	96.57%	96.76%	79.14%	80.05%
Single-card	54.05%	**56.76%**	72.88%	73.42%	27.12%	26.58%	9.17%	9.77%	96.90%	97.10%	71.97%	72.62%

Bold values indicate better fraud detection performance results.

The precision column of Table 11 shows that multi-card CBMs have significantly higher precisions than single-card CBMs. In other words, multi-card CBMs have higher true alarm rates than single-card CBMs. In the worst case, 10.32% of alarms are true for multi-card CBMs, whereas 9.17% of alarms are true for single-card CBMs.

Multi-card CBMs and single-card CBMs have no statistically significant difference in negative predictive values, as seen in the corresponding column of Table 11. In other words, both multi-card CBMs and single-card CBMs have a similar count of true "no alarm" decisions.

As seen in the accuracy column of Table 11, multi-card CBMs have significantly higher accuracy than single-card CBMs. In other words, multi-card CBMs beat single-card CBMs in correct alarm and "no alarm" decisions.

Single-card CBMs have significantly higher sensitivities than multi-card CBMs. On the other hand, multi-card CBMs beat single-card CBMs in terms of specificity, false positive rate, precision and accuracy. If the strategy of the bank is to detect as much fraud as possible at the expense of giving more false alarms, single-card CBMs should be preferred. On the other hand, if the strategy of the bank is to give fewer false alarms at the expense of detecting less fraud, multi-card CBMs should be preferred. Because false alarms have a negative impact on cardholder satisfaction, the strategy of the bank may aim to minimize the false alarm rate and favor multi-card CBMs.

4.4.2. Focus Point 2: Holiday Season Spending Focus CBM

The Holiday Season Spending Focus CBM aims to take into account holidays in CBMs. Transactions within 3, 5, 7, 9, 11, 13 and 15 days before the start of a holiday are considered; the best results are obtained for up to 15 days before the start of a holiday.

As seen in the sensitivity column of Table 12, holiday season focus CBMs has significantly higher sensitivities than all-time CBMs in all cases. In other words, holiday season focus CBMs detected more fraudulent transactions than all-time CBMs.

Holiday season focus CBMs and all-time CBMs have no statistically significant difference in specificity and false positive rate, as seen in the corresponding columns of Table 12. In other words, holiday season focus CBMs and all-time CBMs have similar false alarm rates.

The precision column of Table 12 shows that holiday season focus CBMs have significantly higher precisions than all-time CBMs in one case, whereas there is no statistically significant difference in the other case.

Holiday season focus CBMs and all-time CBMs have no statistically significant difference in negative predictive values, as seen in the corresponding column of Table 12. In other words, holiday season focus CBMs and all-time CBMs have similar counts of true "no alarm" decisions.

As seen in the accuracy column of Table 12, holiday season focus CBMs and all-time CBMs have no statistically significant difference in accuracy. In other words, holiday season focus CBMs and all-time CBMs have similar counts of correct alarm and "no alarm" decisions.

Holiday season focus CBMs have significantly higher sensitivities than all-time CBMs in all cases. In terms of precision, holiday season focus CBMs beat all-time CBMs in one case, whereas there is no statistically significant difference in the other case. Additionally, holiday season focus CBMs and all-time CBMs have no statistically significant difference in specificity, false positive rate, negative predictive value and accuracy. The results show that holiday season focus CBMs should be preferred.

5. Conclusions and Future Work

In this paper, we focus on analyzing cardholder spending behavior and propose a novel cardholder behavior model for detecting credit card fraud. The model is called the Cardholder Behavior Model (CBM). Two focus points are proposed and evaluated for CBMs by using a credit card transaction data-set from a leading bank in Turkey.

The first focus point is to analyze single-card and multi-card CBMs. The evaluation results show that single-card CBMs detect more fraud than multi-card CBMs while yielding more false alarms. In other words, it is discovered that single-card CBMs are preferable for detecting more fraud, whereas multi-card models are preferable for yielding fewer false alarms.

The second focus point is to take into account holidays in CBMs. The evaluation results show that holiday season focus CBMs detect more fraud than all-time CBMs while yielding a similar number of false alarms. Consequently, it is discovered that holiday seasons should be considered in building CBMs.

We have focused on the practical problem of credit card fraud detection by proposing a novel model and focus points. We have empirically shown the effect of the proposed focus

points on fraud detection performance. The practical impact of CBMs is to provide a supportive fraud detection tool that will work together with the existing rule-based tools.

In future research, we will focus on internet transactions. In the first case, we will build two separate models; one with just internet transactions and the other with just card-present transactions. In the second case, we will build a single model with all internet and card-present transactions included. Thereafter, we will evaluate the fraud detection performance in each case. Moreover, we aim to repeat the experiments with datasets from other leading banks in Turkey to minimize the threat to external validity.

Acknowledgements

This work is supported by the Turkish State Planning Organization (DPT) under the TAM Project, number 2007K120610. The authors also extend their gratitude to Dr. Serif Bahtiyar, who reviewed the manuscript.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Yiğit Kültür is a Ph.D. candidate at the Computer Engineering Department of Boğaziçi University. He received a BS degree in Computer Engineering from Middle East Technical University in 2006 and an MS degree in Computer Engineering from Boğaziçi University in 2008. His research interests include software engineering, artificial intelligence and expert systems.

Mehmet Ufuk Çağlayan is a professor at the Computer Engineering Department of Boğaziçi University. He received a BS degree in Electrical and Electronics Engineering from Middle East Technical University in 1973, an MS degree in Computer Science from Middle East Technical University in 1975 and a Ph.D. degree in Electrical and Electronics Engineering and Computer Science from Northwestern University in 1981. His research interests include computer and network security, wireless and mobile networks, internet, distributed systems, operating systems, software engineering, artificial intelligence and expert systems.

References

Aleskerov, E., Freisleben, B., & Rao, B. (1997). CARDWATCH: A neural network based database mining system for credit card fraud detection. In *Proceedings of the IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr)* (pp. 220–226). New York City, New York, USA.

Alowais, M.I. & Soon, L.K. (2012). Credit card fraud detection: Personalized or aggregated model. In *Proceedings of the 3rd FTRA international conference on mobile ubiquitous and intelligent computing (MUSIC)* (pp. 114–119). Vancouver, Canada.

Bentley, P.J., Kim, J., Jung, G.H., & Choi, J.U. (2000). Fuzzy Darwinian detection of credit card fraud. In *Proceedings of the 14th annual fall symposium of the Korean information processing society* (pp. 1–4). Seoul, Republic of Korea.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J.C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*, 602–613.

Bhusari, V., & Patil, S. (2011). Application of hidden markov model in credit card fraud detection. *International Journal of Distributed and Parallel systems, 2*, 203–211.

Chen, R., Chen, T., Chien, Y., & Yang, Y. (2005). Novel questionnaire-responded transaction approach with SVM for credit card fraud detection. *Lecture Notes in Computer Science: Advances in Neural Networks, 3497*, 916–921.

Cobb, B.R. (2010). An influence diagram model for detecting credit card fraud. In *Proceedings of the 5th European conference on probabilistic graphical models* (pp. 89–96). Helsinki, Finland.

Dempster, A.P., Laird, N.M., & Rubin, D.B. (1977). Maximum likelihood from incomplete data via the EM algorithm. *Journal of the Royal Statistical Society, 39*, 1–38.

Diners Club. (2014). *About diners club international*. Retrieved December 6, 2015, from http://www.dinersclub.com/about-us.html

Duman, E., & Ozcelik, M.H. (2011). Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications, 38*, 13057–13063.

Filippov, V., Mukhanov, L., & Shchukin, B. (2008). Credit card fraud detection system. In *Proceedings of the 7th IEEE international conference on cybernetic intelligent systems (CIS 2008)* (pp. 1–6). London UK.

Gadi, M.F.A., Wang, X., & Lago, A.P. (2008a). Credit card fraud detection with artificial immune system. *Lecture Notes in Computer Science: Artificial Immune Systems, 5132*, 119–131.

Gadi, M.F.A., Wang, X., & Lago, A.P. (2008b). Comparison with parametric optimization in credit card fraud detection. In *Proceedings of the 7th international conference on machine learning and applications (ICMLA '08)* (pp. 279–285). San Diego, California, USA.

Ganji, V.R., & Mannem, S.N.P. (2012). Credit card fraud detection using anti-k nearest neighbor algorithm. *International Journal on Computer Science and Engineering (IJCSE), 4*, 1035–1039.

Grossman, P.Z. (1987). *American Express: The unofficial history of the people who built the great financial empire*. New York, NY: Crown Publishers.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I.H. (2009). The WEKA data mining software: An update. *SIGKDD Explorations, 11*(1).

Hejazi, M., & Singh, Y.P. (2012). Credit data fraud detection using kernel methods with support vector machine. *Journal of Advanced Computer Science and Technology Research, 2*, 35–49.

HSN Consultants Inc. (2013). *The Nilson report*. Oxnard, CA: Author.

Jha, S., Guillen, M., & Westland, J.C. (2012). Employing transaction aggregation strategy to detect credit card fraud. *Expert Systems with Applications, 39*, 12650–12657.

Ju, C.H., & Wang, N. (2009). Research on credit card fraud detection model based on similar coefficient sum. In *Proceedings of the 1st international workshop on database technology and applications* (pp. 295–298). Wuhan, China.

Krivko, M. (2010). A hybrid model for plastic card fraud detection systems. *Expert Systems with Applications, 37*, 6070–6076.

Kultur, Y., & Caglayan M.U. (2015). A Novel Cardholder Behavior Model for Detecting Credit Card Fraud. In *Proceedings of the 9th International Conference on Application of Information and Communication Technologies (AICT)*. Rostov-on-Don, Russia.

Kundu, A., Sural, S., & Majumdar, A.K. (2006). Two-stage credit card fraud detection using sequence alignment. *Information Systems Security, 4332*, 260–275.

Kundu, A., Panigrahi, S., Sural, S., & Majumdar, A.K. (2009). BLAST-SSAHA hybridization for credit card fraud detection. *IEEE Transactions on Dependable and Secure Computing, 6*, 309–315.

Ma, H., & Li, X. (2009). Application of data mining in preventing credit card fraud. In *Proceedings of international conference on management and service science (MASS)* (pp. 1–6). Wuhan, China.

Maes, S., Tuyls, K., Vanschoenwinkel, B., & Manderick, B. (2002). Credit card fraud detection using Bayesian and neural networks. In *Proceedings of the 1st International NAISO Congress on Neuro Fuzzy Technologies* (pp. 261–270). Havana, Cuba.

Mastercard. (2014). *About Mastercard*. Retrieved December 6, 2015, from http://www.mastercard.com/corporate/ourcompany/about-us.html

Ozcelik, M.H., Isik, M., Duman, E., & Cevik, T. (2010). Improving a credit card fraud detection system using genetic algorithm. In *Proceedings of international conference on networking and information technology (ICNIT)* (pp. 436–440). Philippines, Manila.

Panigrahi, S., Kundu, A., Sural, S., & Majumdar, A.K. (2009). Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning. *Information Fusion, 10*, 354–363.

Patil, D.D., Karad, S.M., Wadhai, V.M., Gokhale, J.A., & Halgaonkar, P.S. (2010). Efficient scalable multi-level classification scheme for credit card fraud detection. *International Journal of Computer Science and Network Security (IJCSNS), 10*, 123–130.

Philip, N., & Sherly, K.K. (2012). Credit card fraud detection based on behavior mining. *TIST International Journal for Science, Technology & Research, 1*, 7–12.

Quah, J.T.S., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. *Expert Systems with Applications, 35*, 1721–1732.

Rani, J.K., Kumar, S.P., Mohan, U.R., & Shankar, C.U. (2011). Credit card fraud detection analysis. *International Journal of Computer Trends and Technology, 2*, 24–27.

Sahin, Y., & Duman, E. (2011a). Detecting credit card fraud by decision trees and support vector machines. In *Proceedings of the international multiconference of engineers and computer scientists (IMECS)* (pp. 442–447). Hong Kong.

Sahin, Y., & Duman, E. (2011b). Detecting credit card fraud by ANN and logistic regression. In *Proceedings of international symposium on innovations in intelligent systems and applications (INISTA)* (pp. 315–319). Istanbul, Turkey.

Sanchez, D., Vila, M.A., Cerda, L., & Serrano, J.M. (2009). Association rules applied to credit card fraud detection. *Expert Systems with Applications, 36*, 3630–3640.

Sharma, N., Bajpai, A., & Ritoriya, L. (2012). Comparison the various clustering algorithms of weka tools. *International Journal of Emerging Technology and Advanced Engineering, 2*, 73–80.

Shen, A. (2011). *INFOGRAPHIC: Americans are spending a whopping $704.18 on gifts this year*. Retrieved December 6, 2015, from http://www.businessinsider.com/what-americans-spend-on-christmas-2011-12

Sherly, K.K., & Nedunchezhian, R. (2010). BOAT adaptive credit card fraud detection system. In *Proceedings of IEEE international conference on computational intelligence and computing research (ICCIC)* (pp. 1–7). Coimbatore, India.

Visa. (2015). *History of Visa*. Retrieved December 6, 2015, from https://usa.visa.com/about-visa/our_business/history-of-visa.html

Visa Europe. (2011). *Irish consumers to spend €257 million on Christmas internet shopping*. Retrieved December 6, 2015, from http://www.visa.ie/about-us/press-releases/irish-consumers-to-spend-257-million-on-christmas-internet-shopping

Visa USA. (2004). *Merchant category codes for IRS form 1099-MISC reporting*. Foster City, CA: Visa USA.

Yu, W.F., & Wang, N. (2009). Research on credit card fraud detection model based on distance sum. In *Proceedings of the international joint conference on artificial intelligence (JCAI '09)* (pp. 353–356). Hainan Island, China.