Behavioral Fraud Mitigation through Trend Offsets

Raghuveer Kancherla*
Ratna Venkata
Anurag Verma

* Corresponding author.

Abstract

Fraud is often a dynamic and challenging problem in credit card lending business. Credit card fraud can be broadly classified into behavioral and application fraud, with behavioral fraud being the more prominent of the two. Supervised modeling/segmentation techniques are commonly used in fraud detection to distinguish risky transactions from non-risky transactions. However, these techniques frequently rely on identifying risky behavior at a global level. In this paper, along with the classical approach, a new technique has been studied to improve the behavioral fraud detection capability. The application of this proposed technique enables us to identify risky behavior at the account level. It assigns a signature to each account based on its most recent transaction behavior and captures deviations from the assigned signature. This results in an incremental reduction in fraud losses of 15 percent at false positives (good accounts impacted per fraud account) as low as 15.

1. Introduction

Fraud detection is a problem of rare event discovery. With the widespread availability of unmanned customer interaction channels (e.g., Internet and mobile banking), the challenge of controlling fraud has increased substantially. Credit card fraud in the United Kingdom accounted for £423 million of losses in the year 2006 [1]. U.S. credit card fraud was reported to be $3 billion in the same year [2].

Credit card fraud can be perpetrated in several ways. Literature on the types of credit card fraud is widely available [3]. Efficient and implementable techniques to combat fraud are a core capability required from financial institutions and merchants alike. There have seen several advancements in the techniques and technology used to control fraud losses in the last two decades. Technological advancements like Chip and Pin introduced in the European market are aimed at preventing unlawful transactions from happening. However, fraudsters evolve and find ways to get around the system. Hence fraud detection becomes an important and indispensable part of the fraud infrastructure.

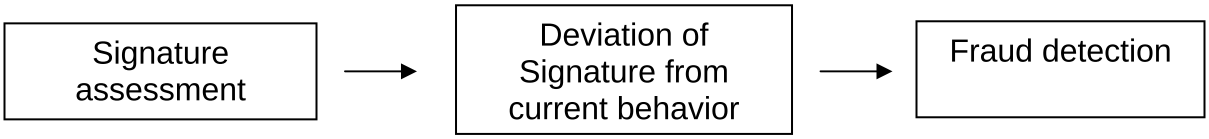
Outlier detection is a commonly used fraud detection technique and is a fundamental issue in data mining [4]. Outliers are data points that are inconsistent with the remainder of the dataset [5,6] or deviate so much from other observations so as to arouse suspicion that they were generated by a different mechanism [7]. Outlier detection can be achieved through techniques like neural net, self-organizing maps, peer group analysis and break point analysis. In particular, neural networks, a supervised learning technique, has received much attention. Researchers who have used neural networks for credit card fraud detection include Ghosh and Reilly (1994), Dorronsoro (1997) and Brause (1999). Unsupervised fraud detection techniques for credit card fraud detection were discussed in detail by Bolton and Hand with the introduction of peer group analysis (PGA) and break point analysis (2001). Several kinds of software are available for neural net implementation in credit card fraud detection, and these are used widely in the industry. Other techniques like generalized additive modeling (GAM), logistic regression, Classification and Regression Tree (CART) and CHi-squared Automatic Interaction Detector (CHAID) are also used for fraud detection.

In this paper, the focus is on outlier detection in a time series data and application of the same for credit card fraud detection using trend offset analysis (TOA). It focuses on identifying pattern changes at an individual account level. Bolton and Hand have proposed a similar technique, break point analysis, that focuses on identifying pattern changes for individual accounts, but it utilizes an unsupervised learning technique. TOA is a supervised learning technique and its performance was studied on large datasets.

In this work (TOA), we assigned a signature to each account based on most recent history of transaction behavior. Any significant deviation in current behavior from the assigned signature was used for outlier detection. In other words, we identified the spending behavior of a particular account, and tagged it as a local outlier if it was anomalous to the previously identified spending behavior of the same account (not necessarily anomalous to the entire population of transactions). The length of time period used to assign a signature for each account was decided based on the computational capability of the system of implementation. TOA was then compared with the widely used global outlier detection model. This technique, implemented on a credit card portfolio, has shown an incremental reduction in fraud losses of 15 percent.

2. Trend Offset Analysis: Methodology

FIGURE 1
Flow Chart for Trend Offset Analysis



Trend offset analysis primarily follows three basic steps as shown in Figure 1. Each step is elaborated in detail in subsequent sections.

2.1 Signature Assessment

In TOA, a fixed-length-moving window of transactions is considered for identifying spending behavior. The characteristic spending behavior of each account is termed as a signature. Current behavior is compared to this signature to tag local outliers. In moving window, the transactions are accounted as they enter into the window and the oldest transactions in the window are removed. In the current business scenario, for implementation and computational ease, the latest one day of transactions were added and the oldest one day of transactions were removed from the window.

If each transaction has characteristics denoted by $[T_1, T_2 \ldots T_J]_{A, T}$ for an account A at time T, then the signature $[S_1, S_2 \ldots S_K]_{A}$ of account A is calculated as mean, median, minimum, maximum and standard deviation over all transactions $[T_1, T_2 \ldots T_J]_{A, T}$. If D_0 denotes current day, D_1 denote previous day and D_{30} denotes 30 days prior to current day, then D_1 to D_{30} are a part of the window W while transactions on D_0 are compared to the signature calculated over the time period W.

2.2 Deviation from Signature

FIGURE 2
Pictorial Representation of Trend Offset Analysis

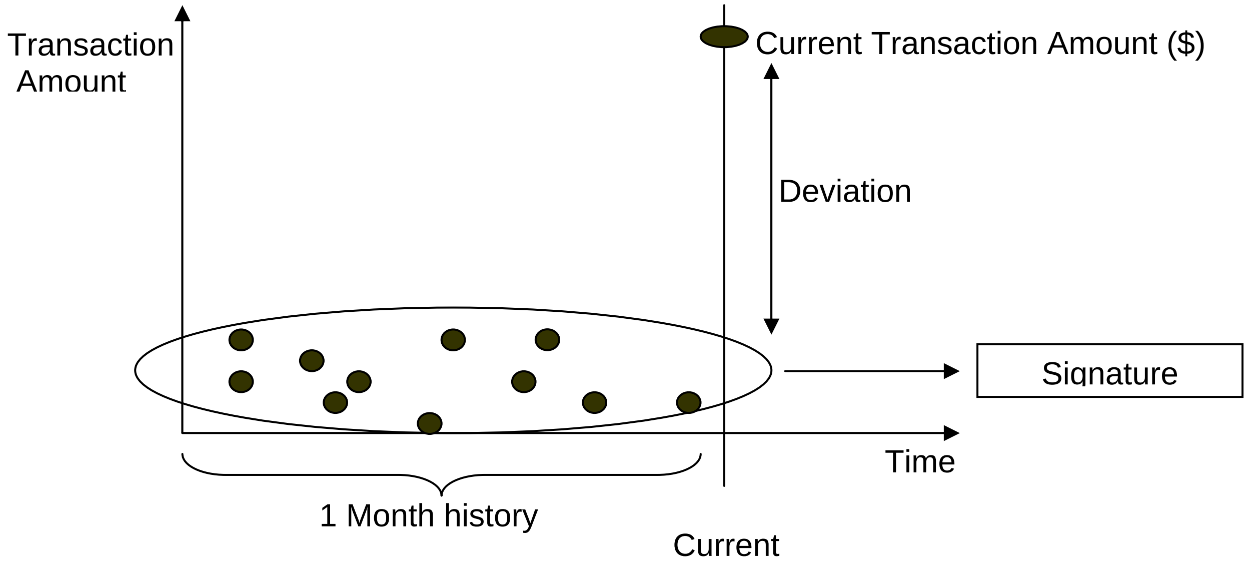


Figure 2 is an illustration of the deviation of current transaction from the signature of the account based on transaction amount. The most distinguishing feature of TOA lies in its focus on personalized patterns, i.e., at account level, rather than on global trends. In the traditional approach to capture fraud, fraudulent patterns as compared to the entire population are considered (global outlier detection models). The number of transactions in a specified time frame, dollar amount of transaction and channel by which the transaction is occurring are a few examples of traditionally used variables to detect fraud patterns. TOA relies on identifying deviations in the current values of these variables from their historically observed values. Exact variables and the type of deviation (deviation from minimum, maximum, mean) that better predicts fraud behavior are dependent on the portfolio being studied.

2.3 Fraud Detection: Supervised Learning

The Classification and Regression Tree (CART) technique was used to identify the pattern changes that are most predictive of fraud behavior. There are several advantages of using CART [10]. First, it is inherently non-parametric, i.e., it makes no assumptions on the distribution of the predictor values. It can effectively handle numerical data that is highly skewed as well as categorical predictors with either ordinal or non-ordinal structure. Second, it has sophisticated methods for dealing with missing values. During signature assignments several attributes may get missing values. For example, inactivity of an account in the last one month (signature assessment window used) can lead the entire signature to be absent. Also, CART-generated rules are relatively simple to understand, which is very important for implementation in a business scenario.

One can seldom be sure that fraud has been perpetrated using statistical analysis alone. Hence, there is a detection team involved for manual review of accounts detected as fraud by statistical analysis. Thus, it is imperative to keep low the total number of accounts queued by statistical analysis.

2.3.1 Results and Discussion

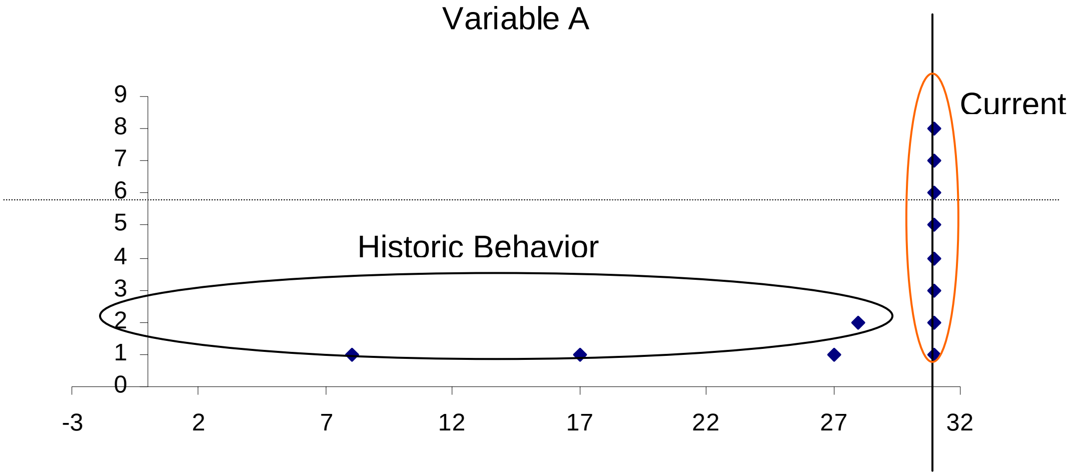
In a supervised learning technique based on classification, the first component is a categorical outcome or “dependent variable.” This variable is the characteristic to predict based on the predictor or independent variables. In this study, one month of transactions belonging to a bankcard product was considered. Also, to identify changes in transaction behavior at account level, an account identifier has been used. Since the chances of fraud are higher on a bankcard product than a private label card (credit limits on private label cards are lower), the choice of the data was ideal for the analysis.

TABLE 1
A Brief Structure of the Data Used for Trend Offset Analysis
(numbers and dates do not represent the data used)

Account Identifier	**Transaction**		**Variable**			**Fraud Indicator**	**Signature**		
	Date	**Time**	**1**	**2**	**M**		**1**	**2**	**N**
1	10/01/07	16:02:44	29	A	6	0	20	1	5
1	10/20/07	15:25:56	81	B	13	1	13	0	2
2	10/04/07	10:04:55	40	C	4	0	32	1	9
3	10/01/07	19:39:02	51	A	15	0	41	1	8
3	10/09/07	08:10:00	48	A	7	0	39	1	4
3	10/22/07	17:19:22	65	D	25	0	33	1	9
3	10/25/07	09:59:24	66	E	18	0	43	0	6
4	10/02/07	19:54:31	60	B	13	0	43	0	4
5	10/03/07	19:50:54	70	A	10	1	7	0	8
5	10/03/07	20:57:50	100	C	17	1	9	1	3

In Table 1, the variable account identifier helps to identify the transactions of the same account and the fraud indicator is the categorical dependent variable. Variable-1 to Variable-M are M variables that are available for each transaction in the data. Signature-1 to Signature-N are N variables calculated over the most recent one-month history of transactions for each account to capture trend offset behavior.

FIGURE 3
Illustrates the Use of Trend Offset Analysis in Detection of Fraudulent Behavior



In Figure 3, on the X-axis is the date of transaction, and the Y-axis represents the value of variable A. Even at a value of 6, the pattern is not risky when compared to the global pattern in transactions. But it is very clear that the pattern is risky when the value of variable A crosses 4 considering the deviation from the accounts' historic behavior. Note that there can be a significant number of good accounts (legitimate accounts) deviating from their previously displayed patterns. Especially during holiday months like November and December, good accounts are prone to showing such pattern changes. In some cases, this pattern is observed in non-holiday months as well.

For evaluating the performance of TOA, a large dataset with more than 3 million data points was considered. Since CART software cannot handle large datasets, biased sampling was used. Good transactions were sampled down to 5 percent, while the fraud transactions were not sampled. Further, to eliminate the manual bias in the measurement of TOA performance (in comparison with the global outlier model), inbuilt auto best split option was used. A similar procedure was followed for the rules identifying global outliers.

Table 2 shows TOA performance is slightly better than the rules based on the global outliers detection model. TOA gives lower queue rates on good accounts and good dollars while maintaining the fraud dollars saved. However, implementing TOA for fraud capture over global outliers detection model with this approach (auto split) calls for further research to prove its feasibility for higher benefits. An overlap analysis proves a significant advantage in using the two to compliment each other. Table 3 infers that a global outliers model provides 16 percent queue rate, and there is a 4 percent incremental queue rate by using TOA with it.

TABLE 2
Comparative Results of TOA and Global Outliers Model

	Queued					**Fraud Dollars Saved**
	Accounts	**Transactions**	**Dollars**	**Fraud Accounts**	**Fraud Transaction**	
TOA	0.63%	0.43%	0.66%	16%	10%	17%
Global Outliers Model	0.74%	0.42%	0.76%	16%	8%	17%

TABLE 3
Queue Rate Comparison of TOA and Global Outliers Model

		Global Outliers Model	
		Queued	**Not Queued**
Trend Offset Analysis	Queued	12%	5%
	Non Queued	5%	78%

For implementation in the business scenario, an analyst built the TOA classification rules (without using auto split) based on his/her business understanding. These rules included both global outlier patterns and trend offset patterns. When implemented on an existing rule set based on global outliers only, TOA proved useful in early capture of fraud. In comparison to the existing rule set, 13 percent of fraud accounts were detected earlier. This resulted in an incremental fraud dollars saved amount of 15 percent on the portfolio while maintaining the false positive (number of good accounts queued per fraud account) close to 15. Table 4 shows the realized benefits in days and dollars for a sample of five fraud accounts.

TABLE 4
Sample of Five Accounts Illustrating the Benefit of Implementing TOA on Existing Global Outliers Model

Account Identifier	Benefit (Days)	Dollar Benefit (% of Credit Limit)
1	7	18%
2	5	1%
3	12	9%
4	22	7%
5	4	35%

4. Conclusion

Trend offset analysis (TOA) is a local outlier-based supervised learning technique implemented for credit card fraud detection. TOA on relatively large datasets gives lower queue rates on good accounts and good dollars while maintaining the fraud dollars saved. An overlap analysis with global outliers detection model shows a significant advantage in using the two together to compliment each other. When implemented in a business setting, where global outliers based fraud detection models exist, TOA proved useful in early detection of fraud.

Acknowledgment

The authors are thankful to the management of Genpact India for giving the permission to publish this paper.

References

APACS—The U.K. Payment Association, Card Fraud Facts and Figures, http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html.

Barnett, V., and Lewis, T. 1994. *Outliers in Statistical Data*, 3rd ed.. New York: John Wiley.

Bolton, R.J., and Hand, D.J. 2002. "Statistical Fraud Detection: A Review." Statistical Science 17(3): 235–255.

__________. 2001. "Unsupervised Profiling Methods for Fraud Detection, Credit Scoring and Credit Control" VII, Edinburgh, U.K., 5–7 Sept..

Epaynews—Payments News and Resource Center, http://www.epaynews.com/statistics/fraud.html—Celent Communications, via Lafferty Publications.

Johnson, R. 1992. *Applied Multivariate Statistical Analysis*. New York: Prentice Hall.

Ghosh, S., and Reilly, D.L. 1994. "Credit Card Fraud Detection with a Neural-Network." System Sciences, Information Systems: Decision Support and Knowledge-Based Systems, Twenty-Seventh Hawaii International Conference, Volume 3, Issue 4–7, pp 621–630.

Glenn, D., and Katharina, E.F. 2000. "Classification and Regression Trees: A Powerful yet Simple Technique for Ecological Data Analysis." Ecology 81(11): 3178–3192.

Victoria, J. H., and Jim, H. 2004. "A Survey of Outlier Detection Methodologies." Artificial Intelligence Review 22(2): 85–126.

Zakia, F., and Akira, M. 2006. "Unsupervised Fraud Detection in Time Series Financial Data." Proceedings of the 17th Data Engineering Workshop (DEWS2006), Ginowan, Japan, March.