Evaluating and Emerging Payment Card Fraud Challenges and Resolution

Pankaj Richhariya
Research Scholar
Dr KNMU University
Newai, Rajasthan

Prashant K Singh
Project Manager
ISC Software's
Bhopal

ABSTRACT
Payment card fraud losses for the card payment industry is generating billions of dollars. In addition to direct damage, the brand name due to fraud can be affected by a lack of customer faith. These cause the deficit is rising, financial institutions and card issuers are constantly new technologies and innovative payment card fraud detection and prevention are demanding. Fraudsters, customers and defense organizations around the world is applied various resolution financial institutions, payment card fraud. The solution is better spent on risk management techniques to predict label use, and customer experience management are designed with the aim of preventing losses. By retaining the right balance between these purposes operational risk management philosophy is driven by a firm. The aim is to protect the gainful customers by delivering them with a stable positive experience. This paper deliberates the solution of payment card fraud and discuss the various attributes of an effective payment card and its applied thoughts. Inspite of this, paper also reviews challenges, the concepts associated to the profiling of card-holder, advanced analytics, metrics to be followed, and mechanisms of the resolution of card fraud.

General Terms
Fraud resolution, alert, fraudulent, normal.

Keywords
Payment card fraud, fraud detection, behavior patterns.

1. INTRODUCTION
The banking industry is strategically timely information about fraudulent activities. Many of the banks and very large databases Valuable business information that can be extracted from these data stores [1]. Valid payment card fraud detection in two classes (real) process of identifying those transactions that are fraudulent and fraudulent transactions [2]. Payment card fraud is largely that can be classified into three categories , traditional card fraud(stolen , application , acquisition , imitation and fake accounts) related , business -related fraud (dealer collusion and triangulation) and Internet fraud (site cloning , credit cards and false merchant sites Generator)[3]. Primary goal for banks is developing and that try to ensure the strategies to apply the try first place is not in.

The available options are emerging that can effectively detect fraud. However, due to cost constraints and current economic conditions, banks are reluctant to invest in expensive option. For example, "chip and pin" card about 20 cents to U.S. $ 1.50 each cost than a magnetic stripe card. In addition, the implementation of new options often requires high investments in infrastructure. Moving forward the answer most effective and cost- friendly and more advanced phishing problem, analytics - based solution is developed.

2. CHALLENGES
Many types of card fraud has evolved over the years and are regularly promoted throughout the world. The most popular and commonly known type include skimming card details. However, the new banking channels have opened and increased in popularity, and has increased the use of credit and debit cards as fraud has grown in both sophistication and scope [8].

Industry transaction through the introduction of chip and PIN or CAP(Chip Authentication Program) devices , online and telephone banking transactions for the implementation of authenticated users and to prevent card fraud monitoring technologies to develop in case has come a long way . Though, banks are now cutting costs and increasing especially in the current economic climate facing pressure to ensure maximum return on investment are.

Potential attack fraudulent manner to protect you need to find the efficiency of financial institutions maintaining effective implementation of anti-fraud Dyanmen Nition and keeping costs low. The first thing you need to focus on the challenges of doing so in their combat card fraud [9].

The datasets are extreme imbalance and highly skewed [4, 5, 6, and 7]. The genuine transactions dominate than fraudulent transactions. The fraudulent events occur rarely. So it is difficult to find the fraudulent. If the fraudulent transaction is consider as legal then it will cause great loss.

The huge amount of datasets and the dimensionality is very high. It is not an easy process to handle the massive amount of data efficiently. The scalable machine learning system is needed to process the large amount of data. The real data is not shared for the number of reasons such as to maintain the privacy of the user. Generally the misclassification cost is high for these detections. Efficient measure should take to reduce the misclassification cost.

Financial institutions fighting today against the Payment card fraud. There are various challenges facing by the financial institutions some of them are given below:

2.1 Defining the Correct Payment Fraud
Definitions and levelling of payment fraud was reported widely throughout industry, region to region and even from institution to institution separately. Consequently, the measured levels of fraud and how the cost of fraud within a country or industry consensus is small Thus, the global payment fraud on a massive scale figures are impossible to find. The level of fraud is usually reported in purely financial terms, and then broken down into various subcategories that make up the fraud for example, cards, check, online and identity fraud.

This kind of data is often collected and untimely Report fraud. This leads to a number of problems. First, the old information means that fraud strategists are always one step behind the

fraudster. Lack of detailed reporting fraud, the modus operandi countermeasure techniques to assess and implement the appropriate experts within banks is difficult. For example, it is known that CNP fraud levels are rising, but the supply is useful to look at what the real fraud?

Other thing the non - grainy high level 'loss reporting a fraud to gain a snapshot view of the extent of the condition is good, but it does not give you clues that will help pinpoint weak spots in an anti-fraud strategy. More sophisticated methods such false - positive, to improve detection rates and to drive the point of identification can be used as measuring the true performance of a fraud prevention strategy.

Finally, the report may be fraudulent. This is somewhat due to mistake in descriptions of fraud. If the first party fraud under different categories such as bad debt is written off, for example, some banks may announce lower levels of fraud.

Right to determine the levels of fraud in order for the industry, a number of changes need to be made:

- A global fraud reporting system should be put in place
- guide the definition and labelling needs to be agreed
- Real-time information sharing becomes the norm

2.2 Fraud Departments Resides in Silos

Typically, banks have supported each new delivery channel and, sometimes, each new product or service, with its own system within the IT infrastructure. Card fraud teams are often isolated from teams dealing with other types of fraud conducted via different payment tools or access points — such as internet banking. This makes it difficult to gain a comprehensive overview of customers' payment patterns or to identify fraud that crosses payment types. In a case of account takeover as a result of phishing, a fraudster who goes online and changes the account address and then requests a new card to use for fraudulent purchases may not be picked up within a siloed system. The address change may be viewed by one team and the card transaction by another team.

In isolation, this may appear to be normal activity, but when combined, it looks abnormal.

2.3 Current Techniques do not Detect Fraud Quickly Enough

The current techniques and metrics deployed by banks to fight fraud often only highlight a problem once a card has been used for fraudulent transactions once, twice or even several times. Without real-time transaction decisioning, the fraud monitoring solution may not be keeping up with the pace of the fraudster. By the time the fraud has been detected, the money has been taken and the customer experience has been affected.

In order to protect their customers, it is crucial for financial institutions to consider real-time detection methods which can prevent losses from being sustained on customers' compromised cards. These tools allow institutions to monitor and immediately recognize suspicious transaction patterns, allowing them to act as soon as the fraudster makes an attempt and thereby prevent any losses.

2.4 Moreover, Fraud is Measured a Reasonable Issue

Usually, banks have considered their fraud prevention techniques as proprietary and therefore a reasonable issue — one where they worry about exposing potential gaps in transaction security.

However, fraud is a good example of an area where financial institutions need to cooperate and start to share information. Embracing the idea that fraud is a non-competitive issue is one of increasing importance for the entire banking community. Various technologies, rules, patterns and fraudster will all continue to develop and the extensive view of fraudulent activity by the industries will be the central for making the resolution to fight against the fraud. As cross-border payments become easier, the sharing of anti-fraud techniques needs to become accepted and easy to facilitate.

2.5 Enhance Working Practices

With fraudsters adapting their techniques from one payment channel to the next, banks need to look at the current structures of their fraud departments, their expertise and the adequacy of the staffing levels. With the appropriate workflow system in place, including a combination of the right levels of expertise and automated fraud detection tools, financial institutions can ensure they target fraud quickly and efficiently.

And this should be done by adopting a variety of performance metrics as well as transaction queuing and automation technologies.

3. EMERGING AN EFFECTIVE FRAUD RESOLUTION

Unfortunately for banks, card fraud is on the rise. Fraud solution space (for example, FICO, SAS, RSA and others) major sellers in the increasing fraud threat are challenged to develop better products. To stay ahead of the fraudsters requires to invest in product innovation. Related to customers, products, accounts transactions and fraud types it also calls for the solutions that are integral with enterprise wide modules. Probably the most importantly, outdated rule and score based models want to be updated by integrating many optimization modules.

Developing an effective fraud solution Prior need to a better understanding mobility of fraud. Fraud is a multi-dimensional dangers that continuously developed and shift in response patterns of fraud prevention efforts. Fraud Solutions also multi-dimensional, advanced and with at least human intervention need to be versatile. Detect fraud after it has occurred is not enough. The ability to flag suspected activity at the perfect time is the key.

Any solution design goal should be of following points to constantly accomplish this:

3.1 Analytic Oriented

To improve the performance the resolution cover the analytic by designing the various modules. The following are to be considered:

- To make the solution more significant to the business advance modules can be integrated with the product to provide transaction alerts based on scenarios.
- Transaction profiling can be achieved based on channel to be used (ATM, POS, Mobile), amount, IP, country, time, during the transaction. To keep update the behavior of customer a standardization module is included in profiling process.
- To get the help to identify the normal behavior compare to abnormal behavior various sub-module can be added into

the standardization module. This can help connect fraud decisions to customer decisions throughout the service lifecycle of the portfolio.

- To make the decision the behavioural attributes can be included in the profile. This is an enhancement over the activity attributes used earlier

3.2 Enterprise- Oriented

The Day to day increasing in payment type and the introduction of new channels for the transaction the payment risk have been increased. Numerous types of card fraud have developed over the years and are perpetrated regularly throughout the world. **T**he solution should be able to cover all the areas such as multiple products, channels, clients and locations. With multi-dimension capabilities, the product will be able to suit the enterprise's needs better than an isolated solution trying to target a specific area or scenario.

3.3 Technology Oriented

There are various technologies used for the resolution of the fraud and are focus on the service oriented architecture, module based design, oriented architecture, open systems to connect to multiple applications without anomalies, high efficiency and reliability.

The flow of transaction in card fraud solution is shown in figure 2, to success of a card fraud solution the scoring engine is perhaps the most perilous. There are sequence of sub modules in the scoring engine which are:

- All the profile variable allied to fraud are tracked by the card holder profiling
- As the outlier variable related to fraud are created or the deviation in the behaviour seen the scores are generated.
- Abnormal profiling used to generate scores based on outlier variable related to fraud.
- Auto-standardization profiles used to analyse online variables and re-scaling.

Based on historical profile of the fraud and non-fraud situations advance analytics used to generate scores

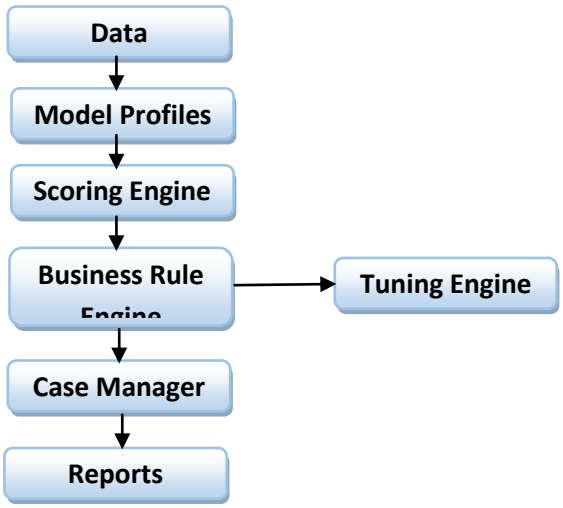

Fig 2 Card fraud solution transaction flow

The idea of various stages of protection in developing resolution that can address the various categories of fraud (such as identifying the fraud type, old fraud types trying to disguise the system, new fraud pattern, feeble patterns, network attack). Fraud protection layers of complexity can be designed as shown in Figure 3. To this end fraud protection is required to achieve significant improvements in the areas of card holder design and advanced analytics, as discussed in the following sections.

Fraud Complexity	**Protection Layer**
Low	Identified Fraud Types(from historical fraud data)
	Transformed Fraud Patterns (old fraud types trying to disguise the system)
	New fraud Patterns(new types of fraud activity)
High	Feeble Patterns(sleeper modules getting activated on triggers)
	Network attacks(Large scale attacks on financial institution

Fig 3 fraud complexity & protection layer

3.3.1 Profiling of the Card Holder

To use the credit card there are various places and sites, and it is extremely very hard to match the pattern. There are millions of possible places and e-commerce sites to use a credit card which makes it extremely difficult to match a pattern. Also, there can be earlier transactions made by fraudsters which also fit a pattern of normal (legitimate) behaviour [10]. The profile of normal and fraudulent behaviour changes constantly. The cost analysis of user behaviour in order to detect fraud is an important concept. If normal spending behaviour with respect to any inconsistencies are found, then it is regarded as suspicious behaviour. And it is taken for further consideration. Spending behaviour varies from person to person. The current cost of fraud detection based on behaviour analysis cardholder payment card fraud is a promise to find a way.

Fraud detection model based behavioral data used in the model means that the cardholder or the transactional behavior are directly derived from them. Each person may have a different cost behavior patterns. The utmost present detection methods of fraud use the pattern of behavior as measure to find the demolition in the transactions. Various usual activities of the customer are learned by the spending pattern of the customer's such as transaction time, transaction amount, billing address and shipping address etc. Some measures to evaluate the suspension behavior are the maximum amount of purchase, variation of billing address and shipping address, big transaction done far away from the living place etc. All that behavior are taken for the further consideration which is suspected and deviate from the normal ones.

On every card analyze the spending patterns and find out any irregularity with respect to the "normal" spending patterns. The only way to detect this kind of fraud. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card

frauds. If there is any Deviation in such patterns is found to a potential risk to the system. Card holder profiling forms the foundation on which various other components of the solution are deployed.

Normal Usage		**Risky Usage**
Card usage occasionally		High Velocity
Electronics & Entertainment	→	Cash Advances
Traveling Occasionally		Cross Border
Online Transactions few		Regular Online Purchases

Fig 4 Normal usage transition to risk usage

To ensure a rock-solid base from which to build the rest of the solution on, the profiling process needs to evolve from pure segmentation based static variables to behavioral variable reflecting the nature of risk. Customer segment- based profiling (based on variables, such as customer age or transaction amount) usually does not convey much about the transaction risk involved. To improve the efficacy of profiling efforts, profiles must be created at the customer level, recognizing that each customer's behavior is unique. Also, the profiles need to be updated on a real time basis based on customer activity. The goal is to provide the system with the ability to compare a customers' recent behavior with his or her past or risky behavior.

Another profiling problem is the issue of aggregation. Aggregation tends to compare different transactions on similar metrics. For example, 'purchase value' can be a segmentation variable; however, when investigated further, there can be cases when low value and high volume transactions are present in a high value transaction segment. The key is to start analyzing the data at a granular level and then aggregate at higher levels to find structures and patterns.

The worldwide nature of the fraud is also covered by the profiling process. It is however one transaction influences only one profile. It is important to considering the multi-dimensional description of fraud, from single transaction being triggered from a POS or ATM or merchant across the globe multiple profiles be update and read. An example could be an ATM-level, Country specific profiling process. However, this may have an impact on the customer experience. As such, its implementation should be carried out with utmost care and only when there is sufficient evidence to believe that the transaction behavior is abnormal.

The concept of real-time profiling further enhances the ability of the score to make a correct decision.

3.3.2 Advanced Analytics

For the new generation of fraud solutions, adapting to a rapidly changing environment remains a key challenge-models must be adapted and updated to ensure that historical performance and model weights are relevant and effective. The previous generation of models had their model weights frozen and there was no way to know if the model was still performing optimally.

A common metric, 'Points to Double the Odds (PDO)' can be used to measure score performance over time. A rescaled score distribution tends to be more stable and realistic compared to an originally developed one. The rescaling is done to focus on the changes in behavioral patterns, rather than the fraud pattern. For example, one would expect to see a changed pattern during the following scenarios:

- Promotion of Electronic gadgets- Customers line up to buy electronic gadgets.
- Festival Celebration- Customers spend on buying gift items during Diwali, Christmas and New Year.
- Changes in Interest Rates- Customers changing their spending patterns accordingly.
- Increase in inflation rates- customers changing their spending patterns accordingly.

The model (see fig 6) should have the ability to measure its performance in real-time and adjust the model weights accordingly (though a technological challenge, the benefits to the business of such a capability are quite significant). An analytics-driven, advanced scoring technique can supplement the shared network repository knowledge with real time updates from the case management system.

The base score can be augmented with internal and external sources to provide a complete and updated view of the risk.

The final score from the above process is fed into the business rules designed specifically to capture current fraud patterns (which are not captured by advance scoring engine).

To monitor the performance of the advanced scoring technique, it is suggested that detection rates can be plotted against FPR with and without the technique. Detection rate is the percentage of frauds correctly identified by the model against the total actual frauds. As expected with advanced scoring, the detection rate is almost 6% higher at an FPR of 10. This is remarkable considering the value at risk. The goal of the advanced scoring technique is to maintain and improve model performance on a continuous basis or between model refreshes.

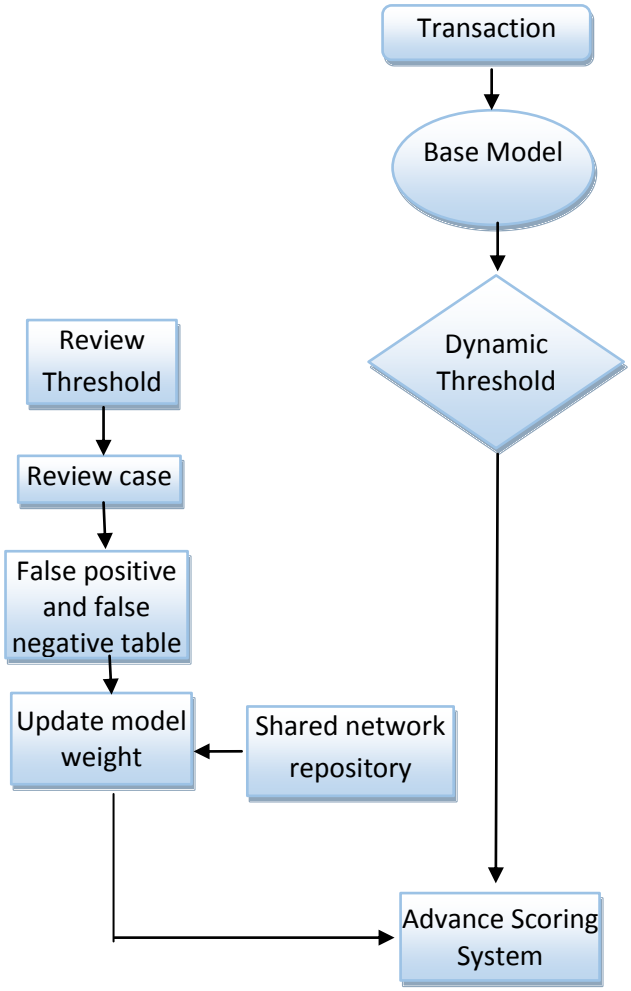

Fig 6: Advance Scoring Engine

4. FURTHER ATTENTION ON THE AREAS

The ability to multi-profile is another key feature of a robust solution. Multi-profiling for customer, account, location, point of sale and ATM provides a holistic view of the transaction. Features like dynamic profiling can further enhance system efficiency and reduce latency. This enables the financial institution to remain current on the risk scenario and focus on long-term goals, rather Than responding to risk on a daily basis by adopting course correction.

The solutions implementation option is another area which should be evaluated in detail. The choices span from real time, online solutions to batch processing solutions-each option varying in model effectiveness, fraud detection, and decision latency(figure 8)

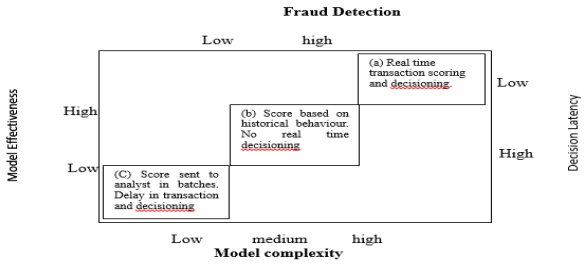

Fig 8 Implementation strategies of model

5. DISPOSITION FOR THE FUTURE

In the future, it is likely that new fraud patterns emerge - each more complex and effective solution would be to call. Future Fraud Detection Solution includes some areas that need to be addressed such as

- Advance Warning System based on the ability to line whip rules, user defined priority, transactions and other relevant standards.
- A set of rules wrapped such that with the solution and determined by the shared network repository. And frequently it can be updated monthly, weakly, hourly where the fraud is occurring other organization and in other geographies in the real time.
- A case investigation drill down capability based on customer, account, transaction and other user defined attributes.
- Dashboard alerts: alerts based on specific scenarios such as non-monetary account activity, card block and replacement, high login failures, and external alerts.
- Non-monetary account activity alerts, card replacement block, based on specific scenarios such as high penetration failures, and external alerts
- Model profiles extended to merchants, devices, accounts, customers, and transactions.

Customer-based scorecard (customer life time value, cross-sell/ upsell and profitability) inclusion in the solution.

- Offices of foreign assets control (OFAC) watch list integration in the rules engine.
- Customer level cases and investigation.
- Case linking capability.
- SAR evidence analysis
- Model metric dashboard.

In addition to preventing fraud, a fraud management solution is another important aspect of the customer experience. This is generally accomplished when the solution is able to give each customer exclusively and is able to balance fraud and client beliefs as per defined business strategies. Sometimes strategies which are purely fraud oriented backfire- creating more problems for the customers than expected benefits. By keeping a tab on spend management and better risk prediction techniques are devised with the purpose of preventing losses are such fraud solutions. The purpose is to keep profitable clients by delivering them with a reliable positive experience with low FPR.

6. CONCLUSION

Evolving digital economy, new methods of payment card fraud are on increasing. While compliance remains a highest priority for banks, there is a need to devise strategies around risk categories. The anonymous nature of the data in credit card transaction is the major problem for the payment system of the bank. There is need to balance and to handle the class of imbalance problem by finding the legitimate as well as illegal transaction patterns for every customer. Secondly for Payment card fraud, banks should focus on advanced concepts such as dynamically profiled from the transactions by using a set of association rules, advance analytics, fraud metrics, and implementing technology projects to increase the transaction accuracy and processing speed of fraud detection. There is a need to

balance the cost of fraud is the solution. Another advantage is driving the business. With the increase in costs, banks can adopt to standardize their business processes.

The solution vendors clearly position its products targeting the bank's need for significant pain points.

7. ACKNOWLEDGMENTS

The authors are grateful to Dr. Piyush Shukla and Mr. Arvind Kourav for their insightful comments and their support.

8. REFERENCES

[1] Ogwueleka, F. N. 2008. Credit card fraud detection using data mining techniques. Ph.D. Dissertation. Department of Computer Science. Nnamdi Azikiwe University, Awka Nigeria.

[2] Maes, S.; Tuyls, K.; Vanschoenwinkel, B.; and Manderick, B. 2002. Credit card detection using Bayesian and neural networks. Proceeding International NAISO Congress on neuron fuzzy Technologies.

[3] Bhatla T.P.; Prabhu, V.; and Dua, A. 2003. Understanding credit card frauds. Cards Business Review# 2003-1, Tata Consultancy Services.

[4] Adnan M. Al-Khatib. 2007. "Mining Fraudulent Behavior in e-payment Systems"; Ph.D. Dissertation.

[5] Clifton Phua; "Minority Report in Fraud Detection: Classification of Skewed Data"; Sigkdd Explorations, Vol. 6.

[6] Salvatore J. Stolfo. 1997. "Credit Card Fraud Detection Using Meta-Learning "; Columbia University.

[7] Salvatore J. Stolfo and Wei Fan 1999. "Cost-based Modelling for Fraud and Intrusion Detection: Results from the JAM Project"; Columbia University; 0-7695-0490-6/99, IEEE.

[8] V. Dheepa, R. Dhanapal and D. Religious. 2010. "A Novel Approach to Credit Card Fraud Detection Model", Journal of Computing, Vol. 2, No. 12, pp. 96.

[9] Chan, P. and Stolfo, S. (1998): Toward scalable learning with non-uniform class and cost distributions: A case study in credit card fraud detection. Proc. of the Fourth International Conference on Knowledge Discovery and Data Mining, pp.164–168.

[10] Mena, J: (2003) Investigate Data mining for security and criminal Detection, Butterworth- Heinemann, Amsterdam.