**Abstract**

The credit cards frauds is a big problem in many parts of the world. However the cost to be understood in its whole extension:

1. There is the loss due the fraud itself
2. There is the cost associated to managing the losses (exceeds the cost of the frauds 300%)
3. There is the cost of mistakenly rejecting orders
4. There is the cost of developing and applying mechanisms to avoid frauds.

Therefore, the problem is not only what you lose due the frauds, but the cost to manage this process (Update security measures, block cards, reimburse customers etc), the cost of building and maintaining mechanisms to prevent the frauds and of course the cost of losing money when you unduly blocks a sales assuming wrongly it is a fraud.

Therefore, the challenge is to build a model which is ease to maintain, highly effective in spotting frauds and at the same time doesn´t have a too high false positive rate. AI/ML seems to be well placed to address all these issues. It automatize the process of adjusting for identifying new types of frauds (the big problem with the current processes) and it can archive an effective identification rate without too many false negative.

**Problem statement /Business problem:**

Our objective is to spot possible frauds in credit card operations. This identification will be based on the client´s profile, the seller´s profile and in the data of the transaction itself. The objective is to identify the transactions to be red flaged as high possibility of fraud.

Today frauds spin around 4% of all sales made with credit cards in Brazil. Today the credit card company already has mechanisms in place to try to spot potential problems, however these mechanisms have two sorts of problems:

1. The fact that they deploy static rules generates a scenario where people in the background have to keep looking for new types of frauds and adjusting the defences.
2. The process suffers a paradoxical problem: if it is too stringent it creates problems for the clients blocking legit sales, if it is too loose it allows a too high level of frauds. A middle term is difficult to archive – even more so when you have to keep adjusting the rules.

To address these two issues, the idea would be to create an AI/ML algorithm which would not only identify (or at least red flag) the suspect transactions but also would identify changes in the patterns and adapt automatically to new fraud patterns.

In order to do that we managed to get a database merging the three instances of data (client, seller and transaction) and the idea is to develop a AI/Machine learning model which not only assertive (Assertive meaning identify a high percentage of the actual frauds without blocking too many legit ones) but adaptable.

The current mechanism spots around 50% (2% of the total) of potential frauds and red-flags around 2% of legit ones. That means the current process get it right in 2% of the cases and wrong in 2%. In summary it is not able to stop 50% of the frauds.

It is interesting to notice that although frauds respond for just 4% of the transactions they answer for 8% of the value of the transactions. That means each 1% of fraud eliminated responds for approximately R$ 16.000.000,00 month (CAD 5.330.000,00)

**Datasets/Getting the data**

We used a real sanitized dataset representing a subset of the transactions occurred during one day of September of 2019 in Brazil, totalizing 290.398 transactions.

**Data exploration/Evaluating the data/ Cleaning the data**

Accuracy and completeness: A visual inspection showed that the data was basically correct. No missing data was identified.

**Stan Insert here**

**Selecting the training data and the test data**

The idea is to use 95% of the measurements as our training data and 5% as our test data. We had a database with 290.398 clients and we separated it into training data 275.878 and test data 14.520.

**The meaning of the columns (data dictionary)**

This database is a crossing of three sources:

* Clients data
* Sellers data
* And the transactions proper.

Information regards the clients:

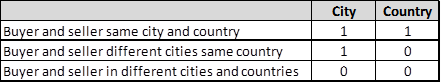
* Age
* Sex
* Income
* Average expenditure  in recurrent  payments  per transaction
* Average expenditure  buying goods (Using the card directly) per transaction
* Average expenditure buying services (using the card directly) per transaction
* Average expenditure buying goods on-line per transaction
* Average expenditure buying services on-line per transaction

Information about the seller:

* Score of the seller (Number 0 to 100) indicating the ranking of the seller regards frequency of frauds.

Information about the transaction:

* Type: which one of the five categories it belongs (0-recurrent, 1- goods, 2-services, 3-on-line good or 4-on-line services).
* Value of the transaction
* If the addresses of the seller and the buyer  are in the same city
* If the addresses of the seller and the buyer  are in the same country
* If the transaction was fraudulent or not (Y or N)



**Model/Analytical model**



**Normalization criteria**

* Income
* Seller score
* City
* Country
* type
* Dispersion

Values divided by the maximum value

**Approach /Analytical problem**

Initially we realized that the variable value only has a meaning as long it is compared with the average expenditure with this particular type of transaction. Given this fact we realized that it would be necessary to create a new compounded variable called “Dispersion”. Dispersion is created comparing the value of the transaction and its type with the average expenditure with this particular type. Example: If value is equal R$ 20,00 and type equal 0. That means this is a recurrent transaction. The average expenditure with recurrent transactions is R$ 25,00. In that case “Dispersion” will be: absolute (25-20)/25 -> 0.20. This variable gives us a view of how far from the average the transaction is.

In another initial evaluation we deployed the method decision-tree to try to figure-out if we could use it directly to identify the frauds. The results were a bit disappointing, although the accuracy seems good it happens just because the data is unbalanced and the frauds are  4% of the total.

The objective is to actually say if the transaction is a fraud or not (not just calculate the chance it to be). Note it identified correctly only 26% of the frauds (157 out of 588).

Confusion Matrix and Statistics

          Reference

Prediction     N     Y

         N 13898   431

         Y    34   157

               Accuracy : 0.968

                 95% CI : (0.965, 0.9708)

    No Information Rate : 0.9595

    P-Value [Acc > NIR] : 4.669e-08

                  Kappa : 0.391

 Mcnemar's Test P-Value : < 2.2e-16

            Sensitivity : 0.9976

            Specificity : 0.2670

         Pos Pred Value : 0.9699

         Neg Pred Value : 0.8220

             Prevalence : 0.9595

         Detection Rate : 0.9572

   Detection Prevalence : 0.9868

      Balanced Accuracy : 0.6323

However, the method indicated how many clusters would be ideal (74) and also gave us an idea about how to procced. The tree also showed an interesting thing: The personal data has almost nothing to do with the results. The relevant factors identified were:

* Score of the seller – Indicates the seller is often target for frauds (probably due type of service or lack of internal controls).
* The type of transaction – Internet services have a way more frauds than everybody else
* City – Transactions where the buyer and the seller are in different cities have much more frauds (they tend to overlap with internet services sales).
* Dispersion (How far from the average spent with this kind of item the value of the operation is)

Then, we adopted the strategy of thorough k-means group the items with more chance to be frauded then use the % of success parameter using the decision-tree to filter the more probable candidates.

In addition of that we used linear regression to stablish the correlation between the variables and the frequency of occurrence of frauds. We identified the following:



That understanding allows us to create an algorithm which checks if the variables of the transaction is below or above the mean giving the transaction a score between 1 and 7. That variable becomes another of our indicators. Therefore we have two composed variables “dispersion” and “points”.

Using the variables Income, same\_city, Same\_country,Seller\_core,dispersion,type, % chance success cluster, chance fails cluster and points -> applied using decision-tree (fraud or not fraud) we managed to get a reasonable predictor.

**Summary of findings /Evaluating the results**

The composition of these variables applied in a decision tree-method generated the following result:

In a test set composed by 5% of the total database (5% of 290.398 -> 14.520)

* The model identified as fraud  and they were in fact frauds 365 ( 2,50%)
* The model identified as fraud but they were not 78 ( 0,53%)
* The model identified as not being frauds but they were 223 ( 1,53%)
* The model identified as not being frauds and they in fact were not 13.854 (95,41%)

**It spotted 62% of the frauds with a very low false positive rate (78 ->0,5%)**

Confusion Matrix and Statistics

Reference

Prediction N Y

N 13854 223

Y 78 365

Accuracy : 0.9793

95% CI : (0.9768, 0.9815)

No Information Rate : 0.9595

P-Value [Acc > NIR] : < 2.2e-16

Kappa : 0.6975

Mcnemar's Test P-Value : < 2.2e-16

Sensitivity : 0.9944

Specificity : 0.6207

Pos Pred Value : 0.9842

Neg Pred Value : 0.8239

Prevalence : 0.9595

Detection Rate : 0.9541

Detection Prevalence : 0.9695

Balanced Accuracy : 0.8076

'Positive' Class : N

This represents an improvement of 12% in the current model. That means in practical terms every day you would be able to spot something 7.300 frauds, letting just 4.470 scape.

This model adds value of 1.400 additional frauds spotted every day with the additional advantage that it “learns” new patterns if they appear and therefore will demand less effort to maintain.

Of course the actual implementation of the model need to be analyzed with care, tests need to be made and eventual performance issues evaluated. (We need to remember that the whole verification has to occur in few seconds just after the user made the transaction – although in the on-line services we may have the option of letting an order “pending approval”)