

PROJECT 2: FRAUDULENT CREDIT CARDS TRANSACTIONS

Context

A bank is interested in providing higher quality customer service to protect customers financial assets. The bank has been receiving several complaints about credit card frauds from their customers and the news media is regularly reporting about how the bank's customers are losing large amounts of money and the bank is doing nothing to stop it. This is impacting both the customers experience and their market share. The Senior Management is asking for a deep dive into this issue.

You just got hired as the Business Analyst for the bank, and they provided you with 6 months of available data (step 0 to 179 refer to the dates). They want you to share some insights using the features in the file to determine if you can see a pattern for the fraudulent transactions. They are expecting you to provide some suggestions on how to tackle the problem.

Questions

1. Show a summary of the variable you are studying (target variable). Plot the most appropriate graph to represent this data
2. Calculate summary statistics from the data
3. Calculation of daily trends of transactions for different categories of variables
4. What are your thoughts on the fraudulent transactions? Is there a threshold of the spent? Is there a specific 'gender' with a higher probability to be the victim of a fraudulent act? or 'category' of transactions with higher chance to be fraudulent?
5. What are your recommendations to the bank's management and describe how your solution will help regain trust from customers?
6. Any other data that you would ask the team to provide? Why?

1. CONTEXT

A bank is interested in providing higher quality customer service to protect customers financial assets. The bank has been receiving several complaints about credit card frauds from their customers and the news media is regularly reporting about how the bank's customers are losing large amounts of money and the bank is doing nothing to stop it. This is impacting both the customers experience and their market share. The Senior Management is asking for a deep dive into this issue.

Our task is to find solutions to the problems encountered by the bank.

2. Recognize the business problem

The problem encountered by our client is the various complaints that customers have made following the different losses they have suffered due to a lack of security on the transactions made by

credit cards. Then the media reports that the bank does nothing to remedy the situation of these customers who regularly lose large amounts of money.

This problem is important for the bank in the sense that it has negative repercussions on the viability of the company because to reach its first objective which is to offer the best service that possible to its customers since one does not manage to protect them from the risks of the fraudulent transactions made by credit card, moreover, its reputation and its customers are threatened, because the media denounce the inaction of the bank vis-a-vis such a situation.

3. Research the organization

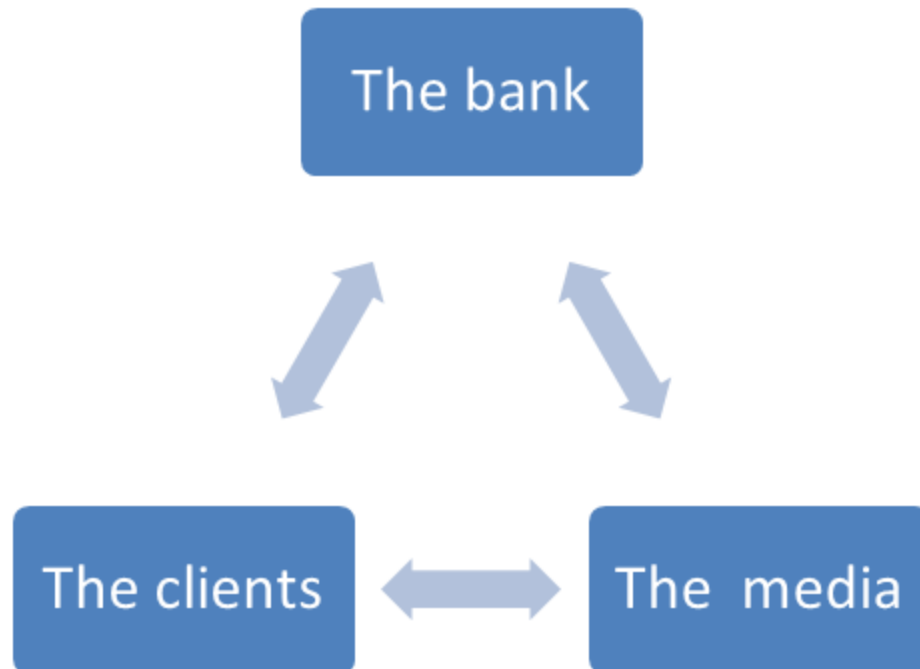
Customer satisfaction is always at the heart of the policy of all companies, it has a more than positive impact on the company. With satisfied customers, we are sure to improve the loyalty of your customers, to develop a positive word of mouth, to constitute ambassadors of your company.

The objective aimed by the bank by contacting us to carry out this work is first of all to help them has the satisfaction of their customers by proposing them a framework in which, the customers can in all safety carries out their transaction by credit card without risk of fraud and especially will allow them to wash their image with the eyes of the general public.

4. Client

Our client is the bank through its General Management. First of all, the Bank wants to regain the trust of its clients in order to restore its image. It expects us to propose a model for fraudulent transactions and suggestions to combat the problem.

5. Relevant stakeholders



Those who are impacted by the problem are:

- Customers: They are affected because of the loss of large sums of money and they have no security guarantees since they cannot be assured that they will not be victims of fraud.
- The Bank: It is at risk of losing its customers because it was not able to fulfill its wish to protect customers from active financial risks, many customers may decide to leave the bank and go to another more reliable one. The credibility of the bank is questioned, no investor would want to invest his money in a company that loses customers, it is a chain reaction, if there are no more investors and no more customers the bank will fail.
- The media: Vanguard gets involved, given the impact of the problem on the market share of customers, it could also have an impact on the economy.

6. SWOT Methodology

6.1. Strengths

- High service levels
- Highly automated systems
- Easy access to capital and funding
- Solid financial reserves
- Good understanding of the customer journey

6.2. Weakness

- high loan rates
- Poor cost efficiencies
-

6.3. Opportunities

- Leverage our big data
- Build online engagement with our brand.
- A growing economy.

6.4. Threats

- Excessive cost of big data
- Breach of data/privacy issues
- Online fraud
- Inability to grow the customer base long-term

7. Solutions and Recommendations

Solution 1: A machine learning model for fraud prediction .

Strength	Weakness
<ul style="list-style-type: none">-Speed- Scale- Efficiency	<ul style="list-style-type: none">- Lack of inspectability- Cold start-Blind to connections in data
Opportunities	Threats
<ul style="list-style-type: none">-Opportunity for the bank to be one step ahead of potential fraud cases.- Opportunity for the bank to have a defense system that evolves and adapts to new types of fraud cases.	<ul style="list-style-type: none">- There is always a risk that there will be fraud due to bias, the time it takes to adapt our program and the lack of human expertise.

Strengths:

- *Speed:* As the velocity of commerce is increasing, it's very important to have a quicker solution to detect fraud. **Machine learning** can evaluate huge numbers of transactions in real time. It is continuously analyzing and processing new data.

- *Scale*: Machine learning algorithms and models become more effective with increasing data sets. Once told which transactions are genuine and which are fraudulent, the systems can work through them and begin to pick out those which fit either bucket.
- *Efficiency*: Contrary to humans, machines can perform repetitive tasks. ML can often be more effective than humans at detecting subtle or non-intuitive patterns to help identify fraudulent transactions.

Weaknesses:

- *Lack of inspectability* : Even the most advanced technology cannot replace the expertise and judgment it takes to effectively filter and process data and evaluate the meaning of the risk score.
- *Cold start*: It takes a significant amount of data for machine learning models to become accurate.
- *Blind to connections in data*: Machine learning models work on actions, behavior, and activity. Initially, when the dataset is small, they are blind to connections in data.

Opportunities

- Opportunity for the bank to be one step ahead of potential fraud cases.
- Opportunity for the bank to have a defense system that evolves and adapts to new types of fraud cases.

Threat

- There is always a risk that there will be fraud due to bias, the time it takes to adapt our program and the lack of human expertise.

Solution 2 :Optimize a highly secure mobile application and introduce a two-step authentication mechanism to ensure that each transaction originates from the card owner.

Strengths:

- This allows cardholders to track the history of their transactions.
- Allows the customer to directly report any irregularities

Weaknesses :

- On the bank side, hire a programmer or a company to create the application.
- On the client side, it requires a phone connected to the internet.

Opportunities:

- The bank and the customer will always be in close communication.
- Opportunity for the bank to regain the trust of its customers

Threats

- If the customer's phone is not protected the risk persists.

- Due to the fact that it is not the bank that is in charge of the application, there may be a delay in upgrading the application and therefore cases of fraud in the meantime.

strengths	Weaknesses
<ul style="list-style-type: none"> -This allows cardholders to track the history of their transactions. - Allows the customer to directly report any irregularities 	<ul style="list-style-type: none"> -On the bank side, hire a programmer or a company to create the application. -On the client side, requires a phone connected to the internet.
Opportunities	Threats
<ul style="list-style-type: none"> -The bank and the customer will always be in close communication. - Opportunity for the bank to regain the trust of its customers 	<ul style="list-style-type: none"> -If the customer's phone is not protected the risk persists. -

Alternative Solution

- **Send a confirmation sms for each transaction:**

Strength:

- It is likely that the customers have a cell phone
- It's cheap and the bank can implement it quickly.

Weakness

- The telephone must always be within reach of the customer.
- It slows down the speed of transactions.

Opportunity:

- The bank and the customer will always be in communication.

Threat:

- The bank risks losing money due to the fact that transactions take longer

- **Limited use card or card with a short expiration date:**

This prevents the card from staying in circulation too long, which could increase the risk of fraud.

Strength:

- We reduce the period of time during which the client can be a victim of fraud
- The bank has better control over the circulation of its cards.

Weakness:

- Delivery time of the new card

- **Do not put the CVV of the cryptogram on the card:**

It is difficult to remember all the card numbers, but the last three are easier to remember and are necessary to make online purchases or payments. The three numbers must be communicated directly to the customer and not written on the card.

Strengths:

- a) Make it impossible for an unknown person to know the CVV and to steal from the client even if the card is lost.
- b) Allows the bank to be sure that it is the customer who makes the transaction.

Weakness:

The customer can forget the code.
You can always scan the card.

8. References & Appendices

- https://www.sas.com/en_us/insights/analytics/machine-learning.html
- <https://www.sciencedirect.com/topics/computer-science/fraud-detection>

9. Team Members

- **Raphael Alexandre Bony**
- **Valcin Pierry**
- **Versailles Chrismond**