Customer rule enabled fraud detection model.

Govind Prasad Buddha
Kiran Babu Sekharamahanthi

Abstract:
The objective of this paper is to recommend a customer focused rule engine while disbursing payments across multiple channels. Currently Banks spend extensively on Fraud detection models and rule engines that are applicable across the solution but hardly there is any focus on letting the customer decide on the payment acceptance rules. For eg if the customer is based out of Hyderabad and uses his card only for shopping in local store, he can set his location and store code. The payments finally run through this rule engine and will be a final confirmation of customer's behavioral pattern. These rules can be dynamically modified by the customer. The rules can be either positive (to accept payments) or negative (to decline payment). If none of the rules' fire, then it will default to customer's Bank's default fraud models/rule engines to service fraud. This is an additional flavor to improve customer experience and let the customer be part of the overall Bank's fraud solution.

Keywords: Credit card, online shopping, P2P payments, fraud detection, customer driven rule engine

I. INTRODUCTION

Fraud is an ever-growing pattern that continuous to bleed both the customers and Banks every year. As per Nilson report losses amounted to 28.65 billion$ in 2020 with an YoY increase of 32% over 2019. Financial institutions allocate budgets running in millions of dollars and an army of technical and operational employees to service fraud losses every year. There are ample instances where Banks have been penalized heavily for vulnerable systems that fraudsters could penetrate and steal customer's money. These instances are a huge financial and reputation losses to Banks with very negative customer experience. While all financial institutions are moving towards better machine learning fraud detection models that are better than conventional rule engine-based systems in detecting fraud however there is a limitation even to this solution when we try to apply a generic detection model for all customers. Every customer's behavior, spending pattern, travelling pattern is different and generalizing them across the solution will inhibit the fraud detection. For eg if detection models notice large amount of fraud coming from gambling dens the models immediately start marking every transaction origination from a casino or gambling den as suspicious. However, there could be customers who are regular visitors to casinos and declining their cards is not a good experience. Same applies other way too, there are customers who use their cards primarily on grocery shopping near their homes only and letting their transactions go through during an account takeover however small the amount may be is also a negative experience. This article briefs on letting customers apply their own rules while using their payment channels.

Banks should provide an interface to the customers to write their own rules. For eg, a customer can decide to decline any payment originating out of 6 kms radius from Gachibowli, Hyderabad, India. He will be exposed with a set of variables that he can write his rules on. We have put in an initial list of variables based on our experience that will be useful for the customer, but the result is to let the customer be part of the fight against Fraud. If none of the customer centric rules fire then Bank should default to its own fraud detection system and also Bank will have the flexibility to override the customer preference if Bank feels a strong reason to do so. For eg when Bank knows the card is already a part of mass compromise. The interface should also allow customers to dynamically change their rules. We feel such a flexibility should reduce fraud losses as customer himself is driving his payments and acknowledging them. The access to these rule engines will not be open to all customers and is driven by specific customer centric parameters like credit score, customer type, accountability, credit limit etc.

II. FLOW DIAGRAM

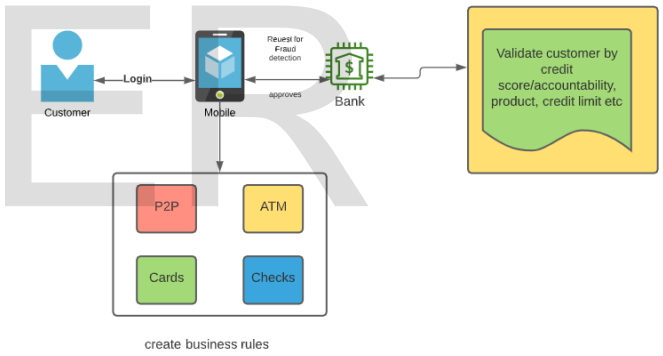
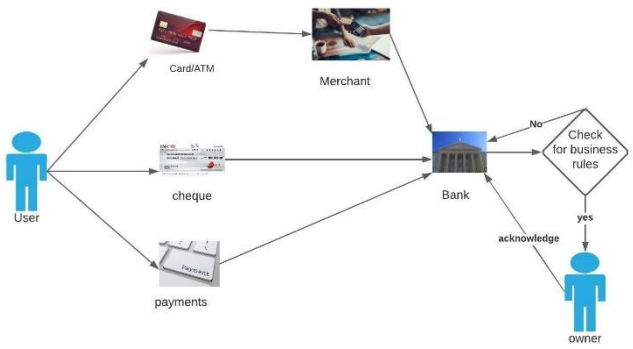


Figure 1: Flow diagram

III. SOLUTION FLOW

Step1: Customer enrolls for a customer centric fraud detection using mobile (refer to figure 1).
Step2: Bank reviews the information and approves based on customer credit checks.
Step3: Customer creates business rules for any of his credit/debit/cheques/ATM withdrawals/POS payments/P2P transfers or any specific accounts including deposit or savings accounts.
Step4: Customer will receive push or SMS notifications if the payments meet the rule the criterion.
Step5: These rules are applicable for all payment channels.

IV. SOLUTION DIAGRAM



V. CUSTOMER VARIABLES

Below are some of the variables recommended, the list can vary depending on customer's relationship with Bank, his risk exposure, credit score etc.

1) Customer Card/Account
2) Amount
3) Devices (Option to select multiple devices)
4) Customer Location
5) Payees
6) Merchants
7) Timings
8) Travel
9) Payee locations
10) Store locations
11) ATM locations
12) Merchant categories
13) Amount limits
14) Number of transactions per day

VI. Wireframe

VII. ADVANTAGES

- Providing flexibility to control customer's own transactions.
- Reducing blocking of credit/debit cards by Banks due to better acceptance and lower fraud risk.
- Reduced claims and fraud losses to Banks.
- Reduced Operational costs for fraud servicing.

VIII. CONCLUSION

While this customer centric rule engine does not remove any liability on the financial Institutions in fraud losses it does improve overall customer satisfaction by making them part of the fraud detection.

The customer is the best judge for his own payments and allowing him to create and run his rules during payments will improve the overall fraud bottom line for the organizations.

IX. REFERENCES

https://nilsonreport.com/mention/1313/1link/