INCOGNIA

Optimizing Fraud Detection in the Digital Banking Mobile App

A Descriptive Analysis of Transaction Events and a new suggestion of a fraud decision flow for transactions classification

Table of Contents

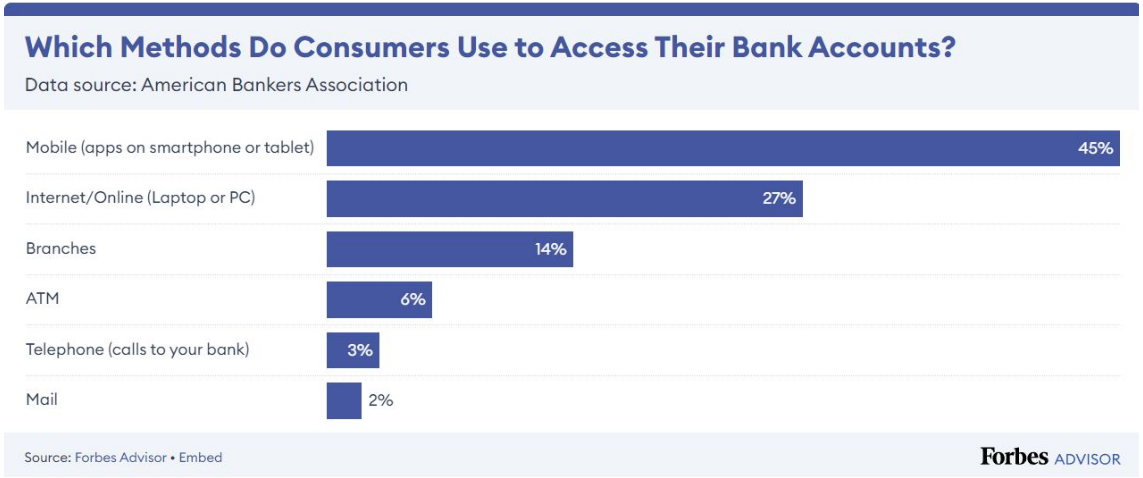
INCOGNIA

New fraud decision flow for the Digital Banking Mobile App - Introduction

Fraudulent activity is a big concern for all types of transactions in every business sector, especially in Digital banking, and having a robust, frictionless and assertive fraud detection system is a must. A national survey conducted by the American Bankers Association found that in 2022, **45% of bank customers used apps on smartphones or other mobile devices as their top option for managing their bank accounts**, while 27% used online banking from a traditional computer (laptop or desktop), and according to the survey, **47% of consumers cited security concerns as the main reason for not using mobile banking services**. (Source: Deloitte)

In this report, we will detail a brief analysis for the Transactions data from Digital Bank Mobile App, giving details about the variables and the data, how it's distributed, a deep dive and data quality issues. Present a new set of Fraud Risk Classification Rules, comparing good users vs fraudsters and detailing the new decision flow.

We will take some fraud behavior deep dives, blocking and 2FA thresholds and the criterias for each risk band, and later, evaluate the rules, comparing the current vs new decision flow by revenue, fraud costs, approval rate and False Positives / Negatives. At the end, we will give recommendations for better fraud recognition and improvement of User Experience, and then summarize all the results.


Which Methods Do Consumers Use to Access Their Bank Accounts?

Data source: American Bankers Association

Source: Forbes Advisor • Embed

Descriptive Analysis of Transaction Events

Details about the variables, data, how it’s distributed, a deep dive and data quality

Exploring the datasets: Transactions and Fraud transactions

We were provided with a Transactions dataset containing transaction events from a Digital Bank Mobile App, and the Fraud transactions dataset with the list of transactions that resulted in fraud

Each event is represented by the following variables:

- **transaction id**: Unique event identifier
- **transaction timestamp**: Timestamp of the event in milliseconds
- **transaction value**: Monetary value of the transaction in reais (R$)
- **account id**: Identifier of the associated account
- **device id**: Identifier of the device used for the event
- **distance to frequent location**: Distance in meters from a frequent location associated with the account at the time of the event
- **device age days**: Number of days since the device was first associated with the account
- **is emulator**: Indicates if the device was identified as an emulator
- **has fake location**: Indicates if the device was generating false location information
- **has root permissions**: Indicates if the device had root privileges
- **app is tampered**: Indicates if the app used was tampered
- **client decision**: Apps' final evaluation of the transaction (approved or denied) after the two-factor authentication (2FA) process, i.e., the response of the 2FA process

And to start the Descriptive Analysis and the creation of the new decision flow, we will examine the following points for these variables:

- **transaction value**: Data distribution, values, outliers, fraud patterns and correlation with other variables
- **distance to frequent location**: Data distribution, values, outliers, fraud patterns and correlation with other variables
- **device age days**: Data distribution, values, fraud patterns and odd behaviors
- **client decision**: Values and odd behaviors
- **hour of transaction**: Values and odd behaviors
- **flags (is emulator, etc)**: Values, fraud patterns and correlation with other variables
- **accounts and devices**: Fraud patterns

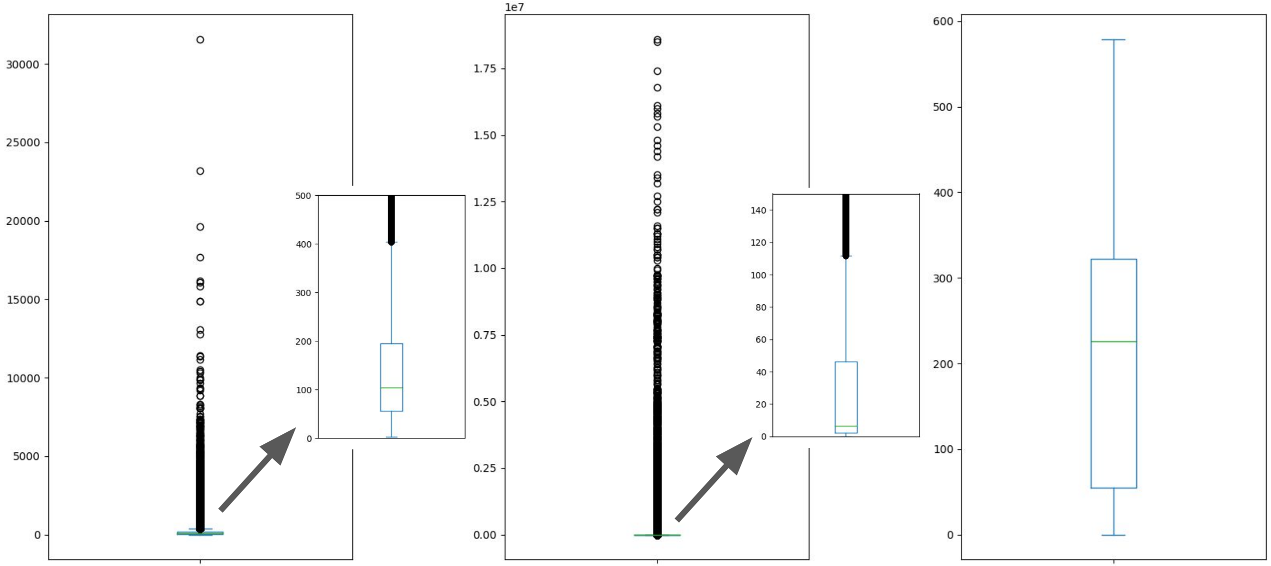
One important note: the transactions are classified as fraud later, but we don't know how long it takes. We are assuming that this evaluation is made after the last event, i.e., we can't use this information to make any decisions regarding when the transaction was classified as fraud or create rules using device or account watchlists.

There are a lot of outliers in transaction value and distance to frequent location variables

When we take a look into the box plots of the three numerical data from the Transactions dataset, we can see that there are a lot of outliers, both in the transaction value and in the distance to frequent location

Box plots of numeric variables from the Transactions dataset

MEAN, Q1, Q3, MIN, MAX and Outliers



TRANSACTION VALUE

DISTANCE TO FREQUENT LOCATION

DEVICE AGE DAYS

Even if the Q1, Q3 and Mean of the transaction value and distance to frequent location variables seems reasonable, **the maximum value is beyond what you would expect.**

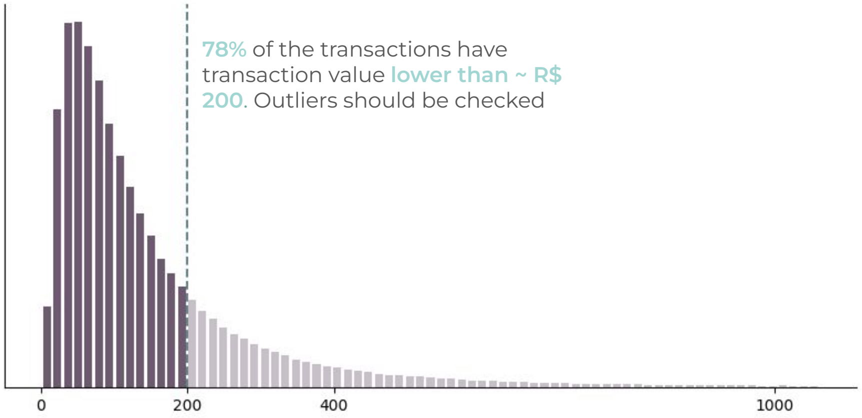
For example, in the distance to frequent location attribute, the **maximum value is 18.600 kms**. The longest non-stop flight in the world (New York to Singapore), is 15.350 kms long. Is someone from Asia creating transactions?

Most of the data consists of low transaction values, and they happen close to the frequent location

Distributions of total transaction value in BRL and the distance to frequent location in meters show that a big part of the Digital Bank Mobile App transactions happen inside the frequent location with low values.

Transaction Value in Brazilian Reais

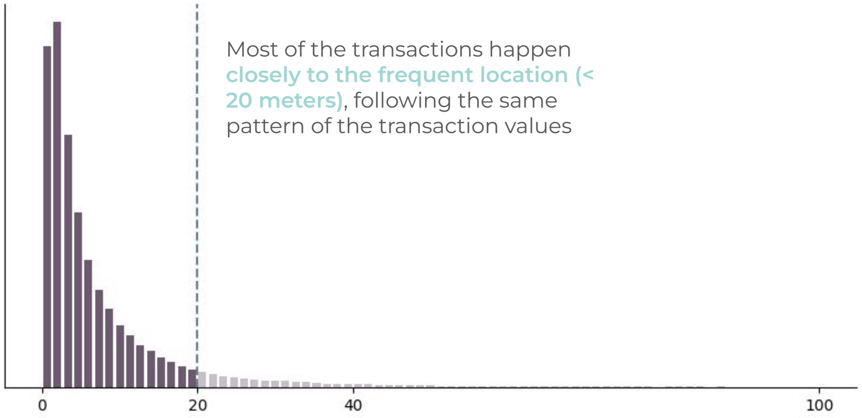
Histogram with transaction values, z-Score < 3



78% of the transactions have transaction value lower than ~ R$ 200. Outliers should be checked

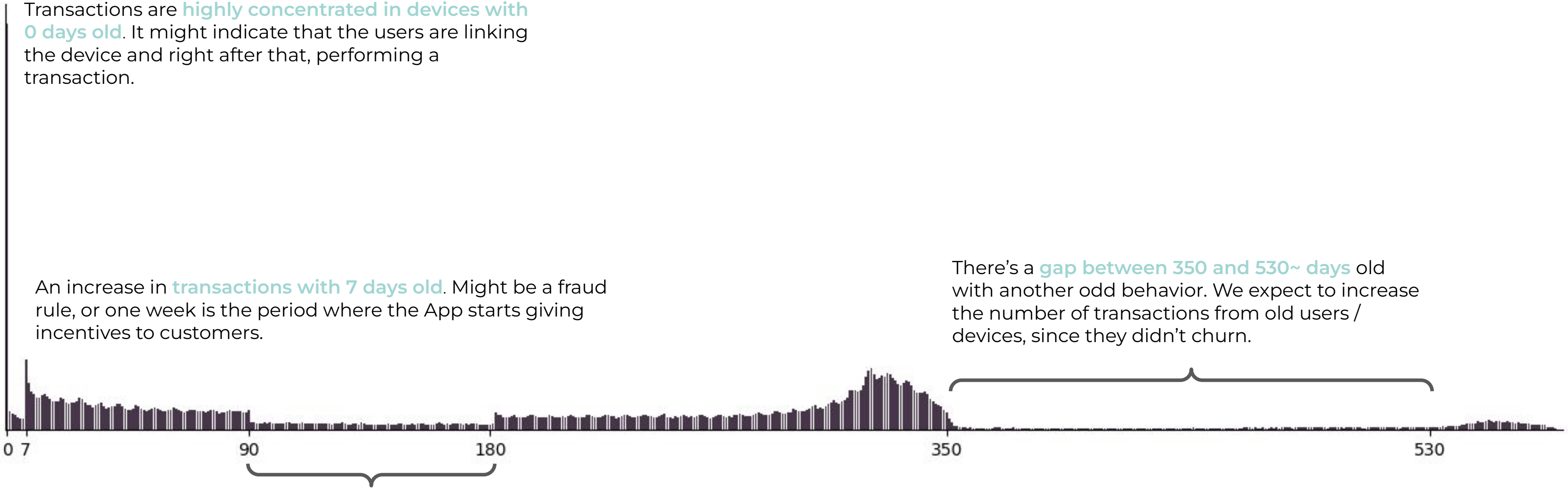
Distance to frequent location in meters

Histogram with distances (m), limited to 100 meters



Most of the transactions happen closely to the frequent location (< 20 meters), following the same pattern of the transaction values

The distribution of Device Age Days does not have clear outliers, as shown in the box plots, but when we check common patterns, there are a few odd behavior



Transactions are highly concentrated in devices with 0 days old. It might indicate that the users are linking the device and right after that, performing a transaction.

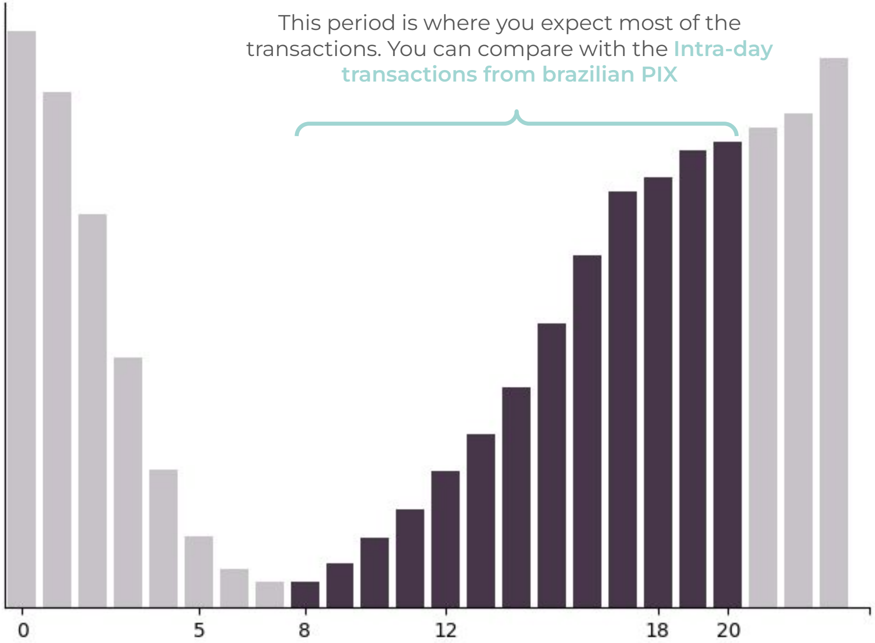
An increase in transactions with 7 days old. Might be a fraud rule, or one week is the period where the App starts giving incentives to customers.

There's a gap between 350 and 530~ days old with another odd behavior. We expect to increase the number of transactions from old users / devices, since they didn't churn.

There's a gap between 90 and 180 days old. It can be a lot of things, such as stopping promotional incentives at 90 and restarting on 180 days or even data quality problems. We need more information to get a correct answer on why this gap happens.

Most of the transactions are happening between late afternoon, at night and at dawn

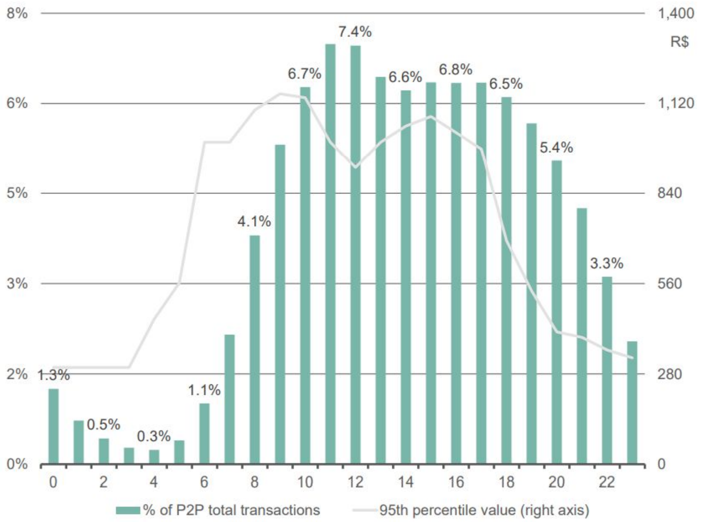
This behavior is different from what you would expect, since it's common to concentrate transactions **between 8AM and 8PM**



This period is where you expect most of the transactions. You can compare with the Intra-day transactions from brazilian PIX

Intra-day transactions from brazilian PIX

By time slot, from Nov/20 to Dec/22

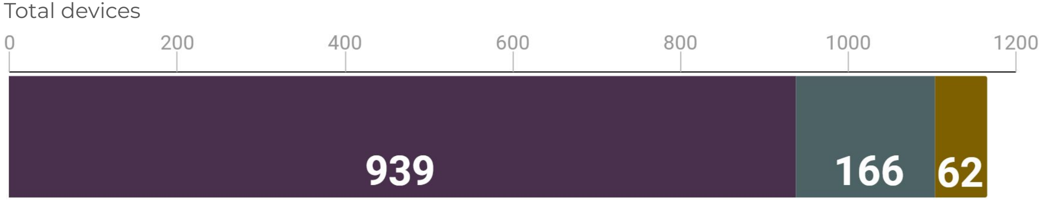


Source: BCB

There are devices with multiple accounts associated, and most of them create fraudulent transactions. The inverse, accounts with multiple devices, is not a concern.

A high number of accounts associated with the same device may indicate a fraudster creating new accounts and fraudulent transactions, or even users that create new accounts for campaign abuse

Number of devices with 3, 4 to 10 or more than 10 accounts associated



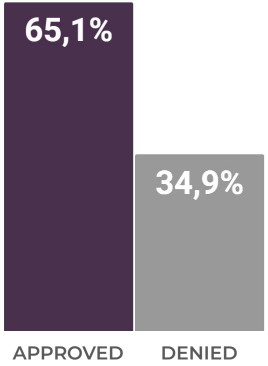
Despite not showing in the graph, there are 18117 devices with 2 accounts associated. It’s not a strong indicator, since you can easily imagine a couple sharing a device.

But when you check for **3 ACCOUNTS IN THE SAME DEVICE**, you have **939 OCCURRENCES**. **4 TO 10, 166 OCCURRENCES** and **MORE THAN 10, 62 OCCURRENCES**

When we look into **accounts with more than one device linked**, there are 35 with 2 devices, and nothing more.

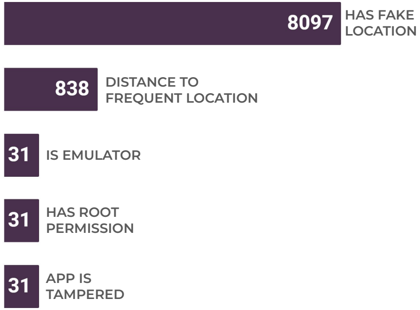
Beyond those points, there are a few User experience problems and data quality concerns that may need to be addressed

The amount of verifications that get denied might be very high, assuming that the user should perform a type of action to complete the 2FA



If we assume that this verification is causing too much friction, it **might affect user retention a lot**

There are Null values in the columns, making it hard to evaluate fraud suspicions. All of these transactions will go through the 2FA validation



All the other attributes don't have null values, **but they might have odd data**

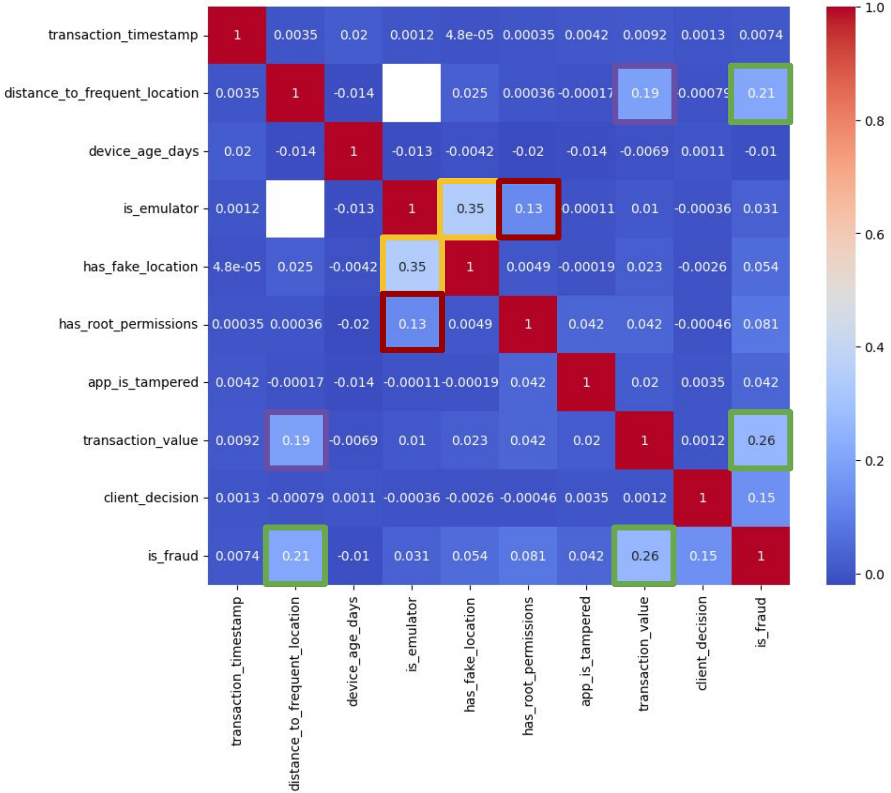
Transaction timestamp is not in the correct format. There are functions that can solve this problem, such as timestamp_millis()

1711158356605

↓

2024-03-23 01:45:56.605

Some of the distance to frequent location data is 0. Probably, the distance is very close to the frequent location, or the sensor has some problems.



	transaction_timestamp	distance_to_frequent_location	device_age_days	is_emulator	has_fake_location	has_root_permissions	app_is_tampered	transaction_value	client_decision	is_fraud
transaction_timestamp	1	0.0035	0.02	0.0012	4.8e-05	0.00035	0.0042	0.0092	0.0013	0.0074
distance_to_frequent_location	0.0035	1	-0.014		0.025	0.00036	-0.00017	0.19	0.00079	0.21
device_age_days	0.02	-0.014	1	-0.013	-0.0042	-0.02	-0.014	-0.0069	0.0011	-0.01
is_emulator	0.0012		-0.013	1	0.35	0.13	0.00011	0.01	-0.00036	0.031
has_fake_location	4.8e-05	0.025	-0.0042	0.35	1	0.0049	-0.00019	0.023	-0.0026	0.054
has_root_permissions	0.00035	0.00036	-0.02	0.13	0.0049	1	0.042	0.042	-0.00046	0.081
app_is_tampered	0.0042	-0.00017	-0.014	-0.00011	-0.00019	0.042	1	0.02	0.0035	0.042
transaction_value	0.0092	0.19	-0.0069	0.01	0.023	0.042	0.02	1	0.0012	0.26
client_decision	0.0013	-0.00079	0.0011	-0.00036	-0.0026	-0.00046	0.0035	0.0012	1	0.15
is_fraud	0.0074	0.21	-0.01	0.031	0.054	0.081	0.042	0.26	0.15	1

There are variables that are correlated to each other, and they might be good candidates to identify fraudulent transactions.

is emulator is positively correlated with **has fake location**

is fraud is positively correlated with **distance to frequent location** and **transaction value**

is emulator is positively correlated with **has root permissions**

transaction value is positively correlated with **distance to frequent location**

Fraud Risk Classification Rules

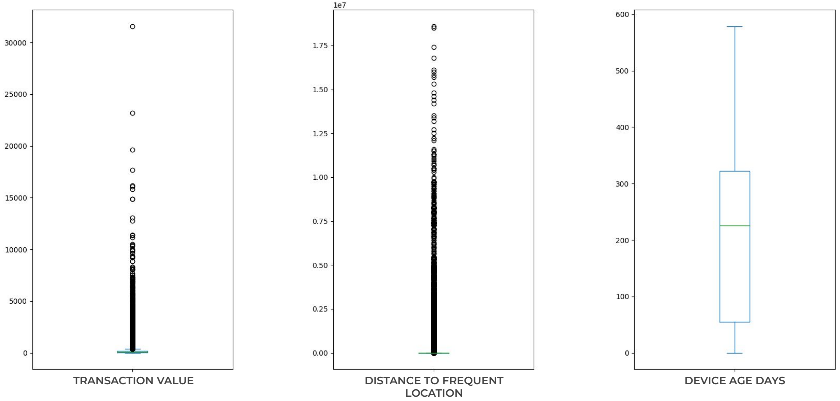
Good users vs fraudsters and the new decision flow

Fraudsters have higher transaction values and make them farther from the frequent location, on average

Box plots from Good transactions vs Fraud ones shows a bigger difference between 1st and 3rd quartile. There's no significant difference in Device age days.

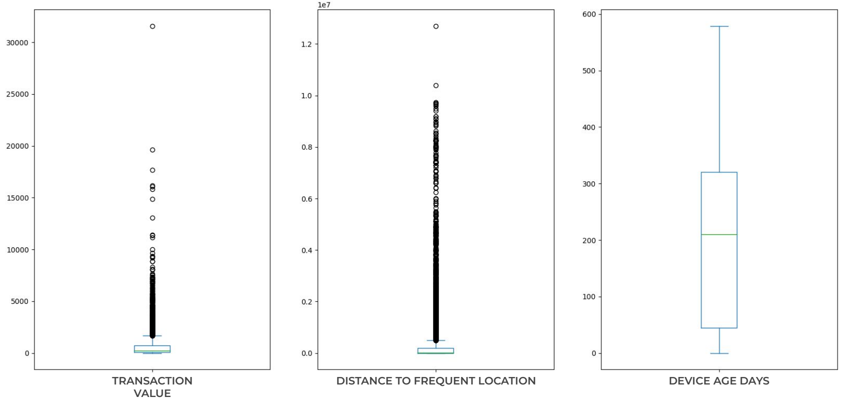
Good transactions happen close to the frequent location, with small transaction values

Letting these customers perform **transactions without 2FA** might be an option. Even if some of them end up being fraudsters, the cost per transaction will not be that big.



Fraudulent transactions, otherwise, have a bigger variance on those variables

We may have to **block** the outliers, and **challenge** the ones with a strange behavior with 2FAs or manual reviews.

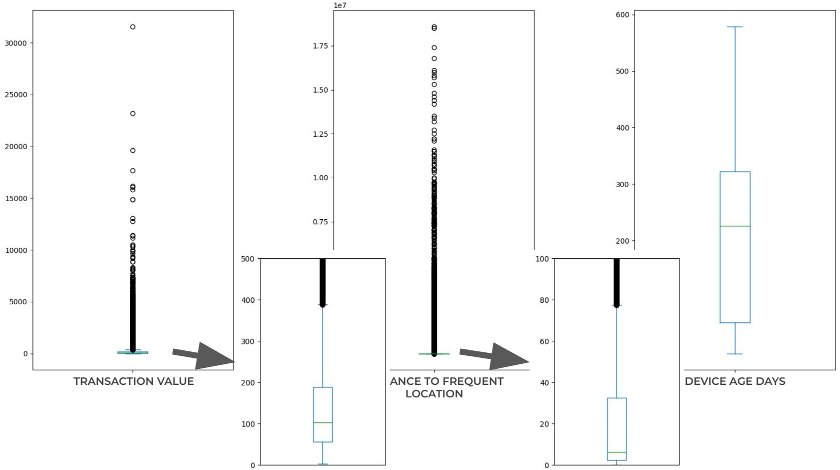


Fraudsters have higher transaction values and make them farther from the frequent location, on average

Box plots from Good transactions vs Fraud ones shows a bigger difference between 1st and 3rd quartile. There's no significant difference in Device age days.

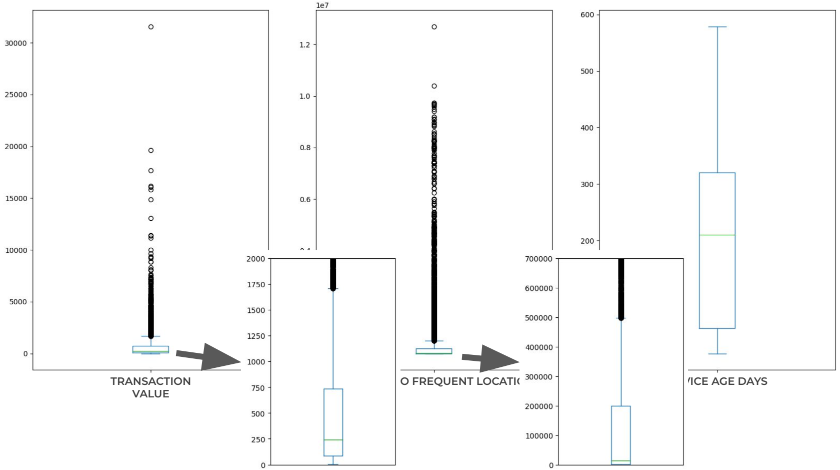
Good transactions happen close to the frequent location, with small transaction values

Letting these customers perform **transactions without 2FA** might be an option. Even if some of them end up being fraudsters, the cost per transaction will not be that big.



Fraudulent transactions, otherwise, have a bigger variance on those variables

We may have to **block** the outliers, and **challenge** the ones with a strange behavior with 2FAs or manual reviews.



The transactions will be evaluated in 3 risk categories: High, Medium and Low

INCOGNIA

High-risk transactions would be **immediately blocked**; medium-risk transactions would follow the current decision flow (**2FA**) and low-risk transaction would be **immediately approved**.

High risk

These transactions have a **high chance to be classified as frauds** and will be **immediately blocked**. It has to be a very high chance to be a fraudster.

Medium risk

They have at least one variable value that requires a 2FA process to guarantee the approval. It will be **transactions with any kind of data problems (null values),** values **significant enough to be tested** or an **extra check to guarantee that it's not a fraud.**

Low risk

They will be **immediately approved**, and consists on transactions with "usual" behavior. **Reducing friction is the main goal**.

Fraud Patterns and the new decision flow: criterias and thresholds

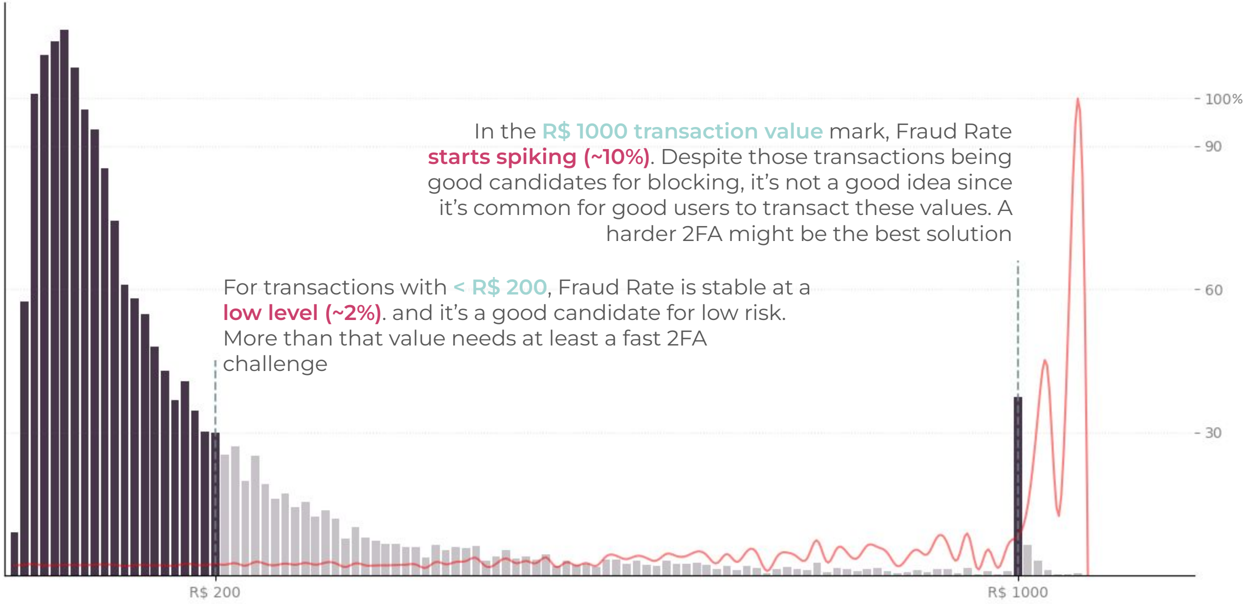
Fraud behavior deep dive, blocking and 2FA thresholds and the criterias for each risk band

Transactions with very high value (> R$ 1000) have a strong chance of being considered fraud.

For user experience purposes, **they will not be blocked** but instead, **having an Analyst revising it or a “harder” 2FA is the recommendation**

Total Value of transactions

# OF FRAUDS and **FRAUD RATE (%)**: # frauds / total transactions



In the R$ 1000 transaction value mark, Fraud Rate **starts spiking (~10%)**. Despite those transactions being good candidates for blocking, it’s not a good idea since it’s common for good users to transact these values. A harder 2FA might be the best solution

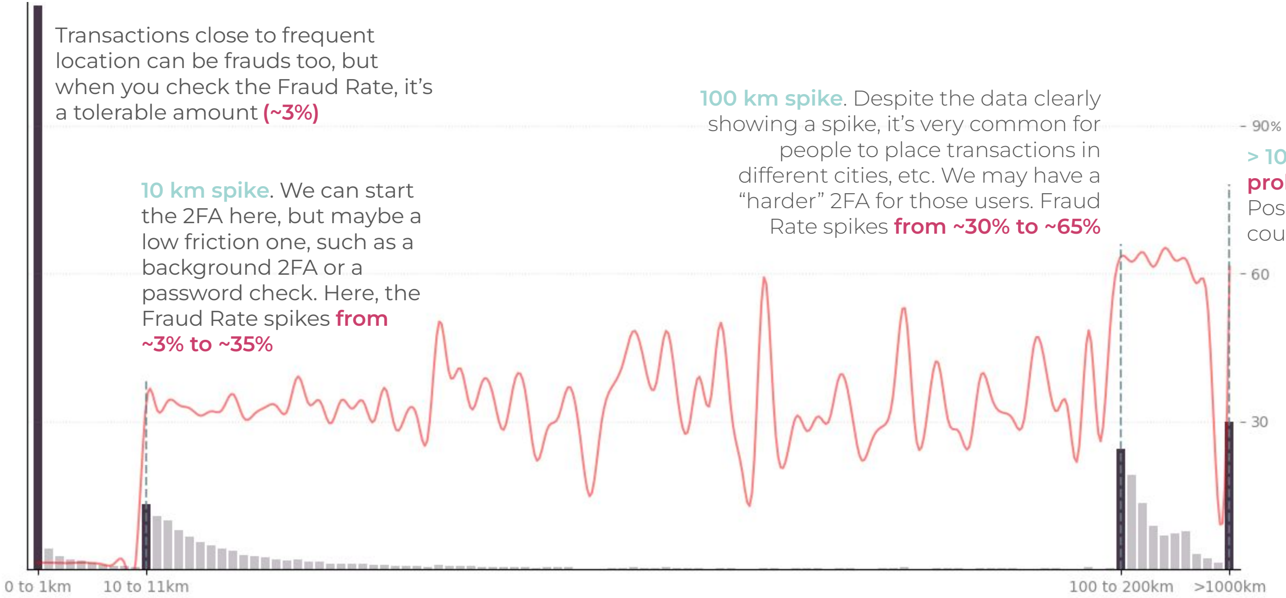
For transactions with < R$ 200, Fraud Rate is stable at a **low level (~2%)**. and it’s a good candidate for low risk. More than that value needs at least a fast 2FA challenge

Block transactions with distance greater than 1000 km, and challenge the ones with distance > 10 km

There's a big difference in total frauds on 1, 10, 100 and > 1000 kms marks

Distance to frequent location in transactions

# OF FRAUDS and **FRAUD RATE (%)**: # frauds / total transactions



Transactions close to frequent location can be frauds too, but when you check the Fraud Rate, it's a tolerable amount **(~3%)**

10 km spike. We can start the 2FA here, but maybe a low friction one, such as a background 2FA or a password check. Here, the Fraud Rate spikes **from ~3% to ~35%**

100 km spike. Despite the data clearly showing a spike, it's very common for people to place transactions in different cities, etc. We may have a "harder" 2FA for those users. Fraud Rate spikes **from ~30% to ~65%**

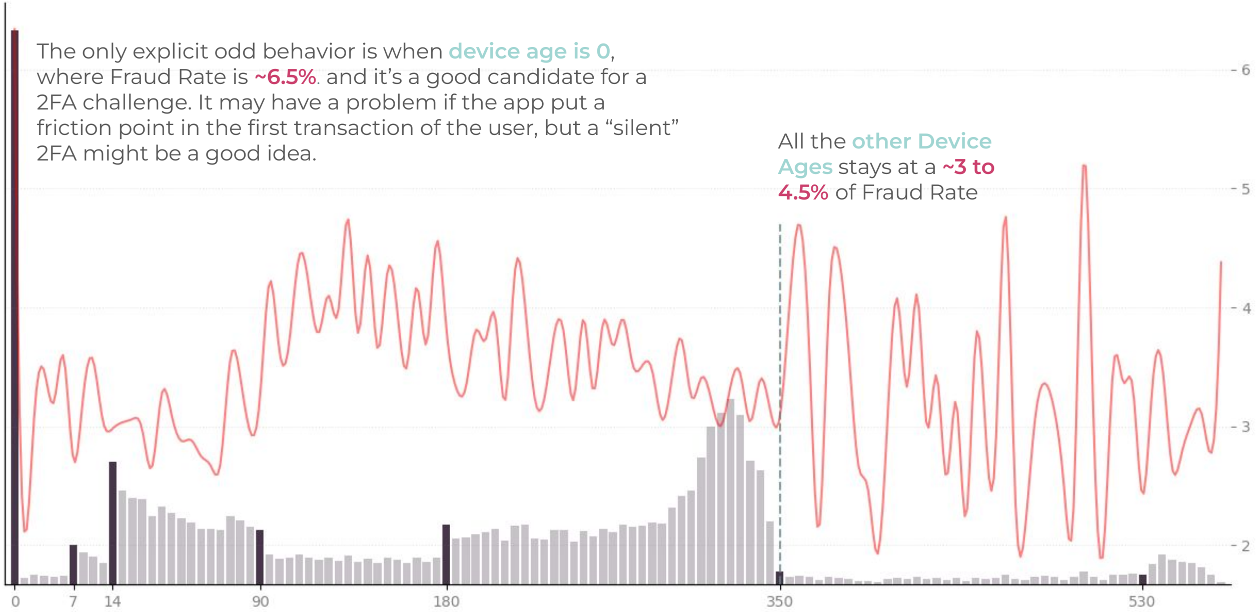
> 1000 km spike. It's very odd, and there's a **high probability of fraud** here. There might have False Positives, such as people currently travelling to other countries. Fraud Rate stays at **~65%**

Check transaction when device age is 0

The Fraud Rate doesn't indicate an explicit difference in the device ages. The only point where there might be a challenge point is when Device Age is 0

Device age distribution of fraudulent transactions

# OF FRAUDS and **FRAUD RATE (%)**: # frauds / total transactions



The only explicit odd behavior is when **device age is 0**, where Fraud Rate is **~6.5%**. and it's a good candidate for a 2FA challenge. It may have a problem if the app put a friction point in the first transaction of the user, but a "silent" 2FA might be a good idea.

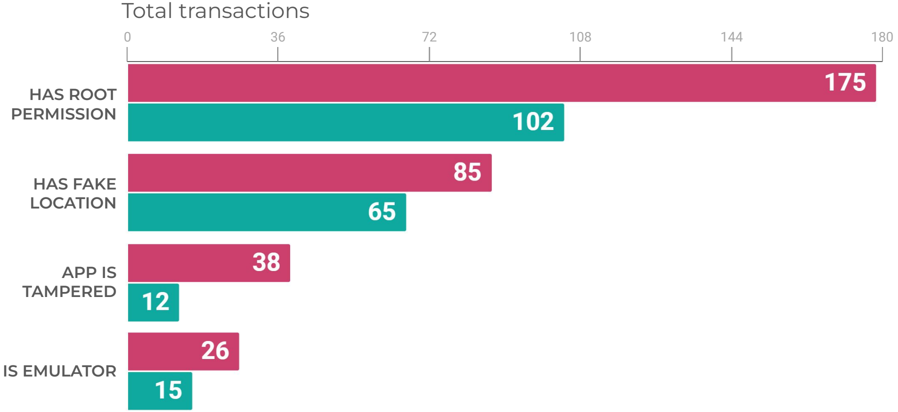
All the **other Device Ages** stays at a **~3 to 4.5%** of Fraud Rate

Block when Is emulator, has fake location, has root permission or app is tampered are True

They are good indicators of possible fraud, since most of the transactions with the flag set end up being tagged as fraud

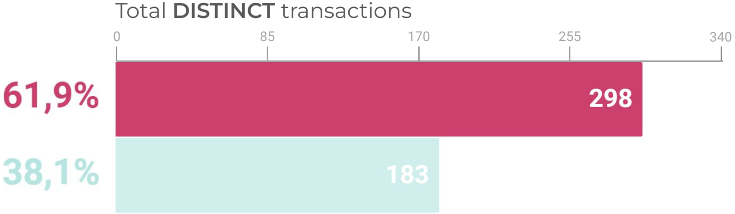
The number of transactions with those flags True is relatively low, but the amount of fraudulent transactions is **always higher than good ones**, for all the flags. Even if the transactions are not frauds, the fact that the user somehow is trying to modify their current state, it's **not a good behavior**

Number of transactions with the flag True



Some of the users have more than one flag set at the same time. On total, **61,9% of the transactions are tagged as frauds**. Blocking them will **prevent 481 possible fraudster to create transactions**

Distinct transactions with at least one flag True



Regarding costs prevented, we get **R$ 27.610 from the 298 fraudsters and R$ 16.431 from the 183 suspicious ones**, with **R$ 44.041 total blocked fraud cost**

Block devices with more than 3 accounts linked

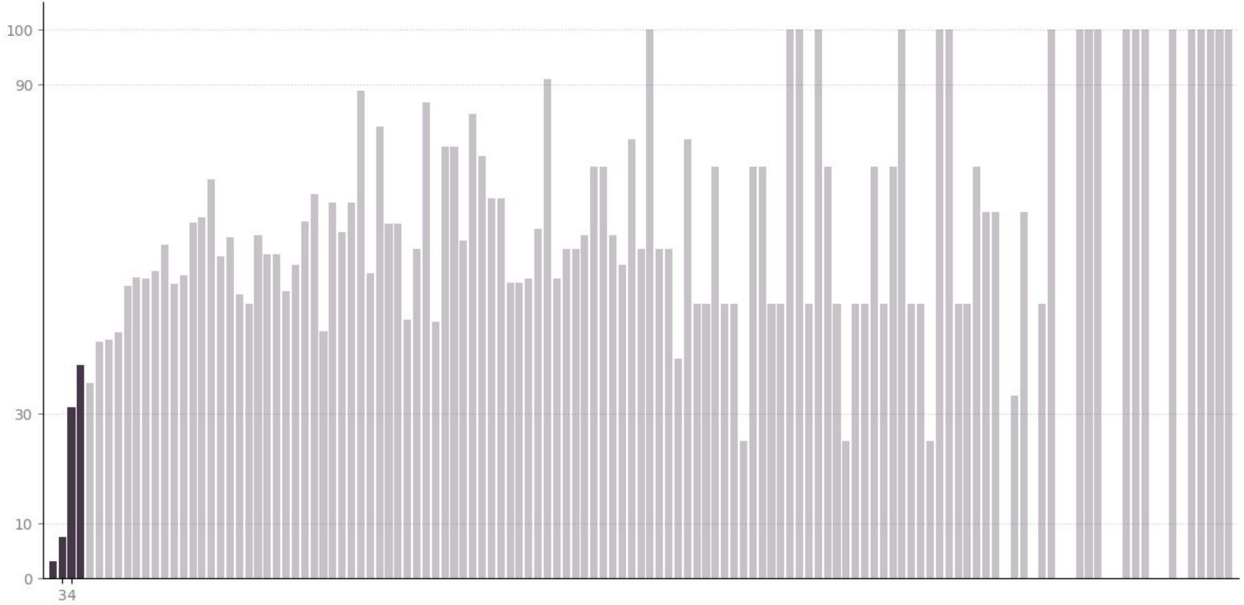
There's a **high chance of those devices to create fraudulent transactions**. The chance is greater than **35%**, and it goes up as the number of devices linked increases

There are **18117 devices with 2 accounts associated**, but the Fraud Rate is low. We need to start looking into devices with 3, 4 or more accounts.

As shown in the graph on the right, the Fraud Rate spikes when the **number of accounts in the device is 4 or more**. The recommendation is to block the transactions and show a message to contact the Customer Support team if necessary

Number of accounts linked to a single device

% OF FRAUD RATE



Putting all together: The new decision flow

After analysing the behavior of fraudsters and good customers, the new criterias and thresholds aims to make the new decision flow to drop the number of fraudulent transactions and reduce friction between non-fraudsters.

High risk

1,16%

4662
Transactions

- **distance to frequent location** is greater than **1000 km**;
- **is emulator, has fake location, has root permission or app is tampered** are True
- There are **more than 3 accounts** linked to the **device**

Medium risk

30,45%

121759
Transactions

- They are not **high-risk**
- One of the criteria below:
  - **transaction value** is greater than **R$ 200**
  - **distance to frequent location** is greater than **10.000 meters (10km)**
  - **device age days** is **0**
  - There's **no data in** at least **one of the variables** (null values)

Low risk

68,39%

273431
Transactions

- They are **not high-risk and medium-risk**
- All of the criteria below:
  - **transaction value** is less than **R$ 200**
  - **distance to frequent location** is less than **10.000 meters (10km)**
  - **device age days** is greater than **0**

INCOGNIA

Evaluation of Classification Rules

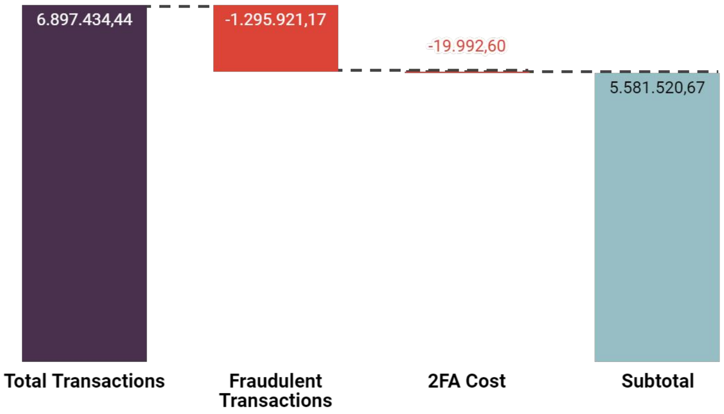
Comparison between current vs new decision flow: Revenue, Fraud costs, approval rate and False Positives / Negatives

After implementing the new rules, the revenue will increase by 20%, when comparing with the current one

The new decision flow assumes a "bad realistic scenario", where it's expected that the **users in the low-risk that were denied in the current flow to be fraudster at the same rate as in the general Fraud Rate (3,19%)**, which is usually higher than we expect, and have the **highest possible transaction value (R$ 200)** for the low risk band.

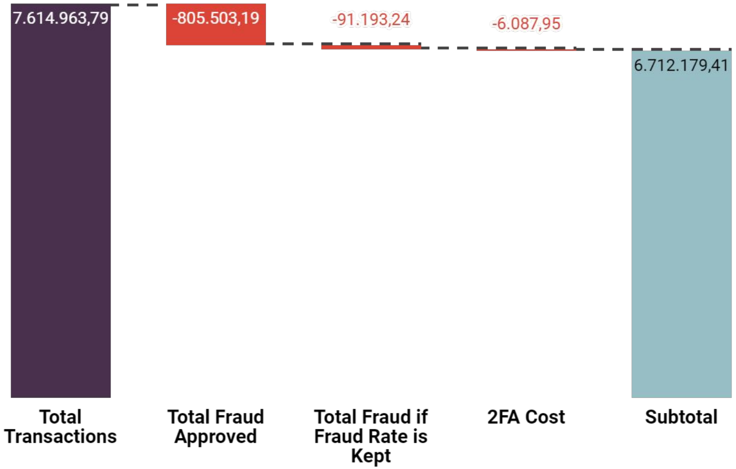
CURRENT REVENUE

All transactions go through a 2FA process, and even with this friction, the **revenue is lower** and the amount of **fraudulent transactions is higher** than when applying the new decision flow



NEW REVENUE

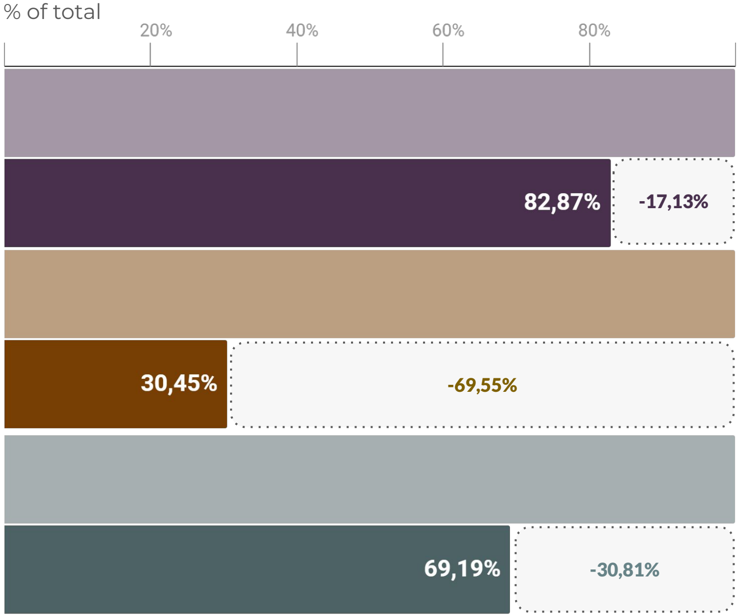
With the new flow, even assuming the "bad realistic scenario", the **revenue is greater, the fraud losses are lower and the friction is much lower.**



The losses from Fraud and 2FA will reduce substantially

Big part of the revenue improvement is the reduction in **fraudulent transactions** and **2FA costs.** Total Fraud Rate reduced from **3,84%** to **3,19%**

Comparison of fraud losses between current and new decision flow



With the new decision flow, the number of fraudulent transactions went from **15371** to **12738** (**-17,13%** reduction), because high-risk fraudster are blocked.

Beyond that, when we use the 2FA flow just for medium risk transactions, 2FA costs went from **R$ 19.992,60** to **R$ 6.087,40** (**-69,55%** reduction)

Putting all together, when the new decision flow blocks fraudster from performing transactions and applies 2FA challenges only to medium risk category, the total Fraud loss went from **R$ 1.296.689,72** to **R$ 897.158,85** (**-30,81%**), using the “bad realistic scenario”.

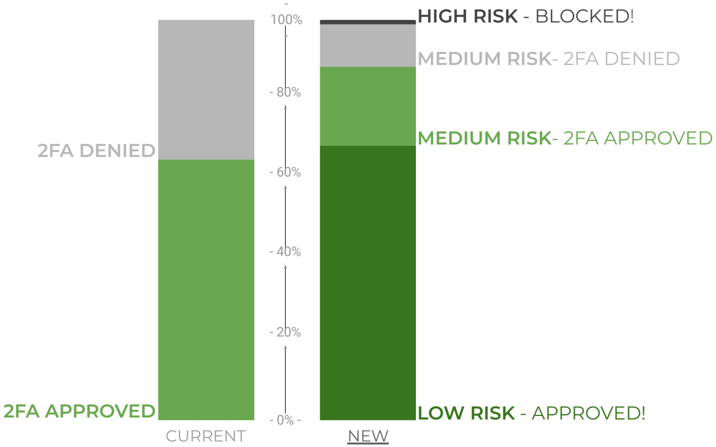
The approval rate will increase to 88,19% and there will be a big reduction in False Positives and Negatives

Since the new flow approves transactions automatically, the friction is expected to reduce.

68% of transactions are low-risk, being **approved immediately**. In the medium risk, 65% will be **approved after the 2FA**

Comparison of transactions approved

% of total Transactions

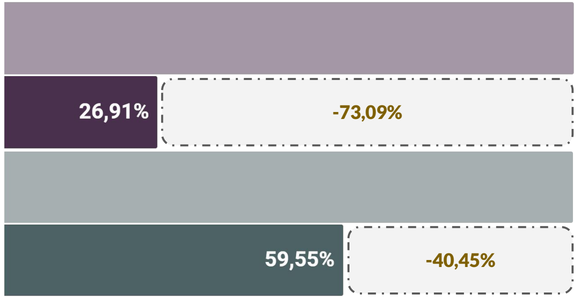


Regarding False Positives and Negatives, with the new flow, there are 2 types: **Hard and Soft**. Hard false positives / negatives regards blocking users, and Soft false positives / negatives, the users that went through the 2FA

Since there's no Block situation in the Current decision flow, **we will not compare Hard false positives / negatives**

Total Soft false positives / negatives

% of total Transactions



Soft false positives will **drop 73,1%**, from 260249 to 70043 transactions

Soft false negatives will **drop 40,5%**, from 15371 to 9153 transactions

(*) A **False positive** is the person that had to go through the 2FA process, and was not a fraudster; **A False negative** is the person that went through the 2FA process, passed and ended up being a fraudster; Since there's no Block situation in the Current decision flow, **we will not compare False Positives and False Negatives that resulted in Blocks yet**

Comparing the current vs new decision flow

	CURRENT	NEW	% DIFF
TOTAL FRAUD TRANSACTIONS	15.371	12.738	▼ -17,12%
TOTAL FRAUD COSTS (R$)	1.296.689	897.158	▼ -30,81%
FRAUD RATE (%)	3,84%	3,19%	▼ -0,65 pp
2FA COST (R$)	19.992	6.087	▼ -69,55%
TOTAL REVENUE (R$)	5.581.520	6.712.179	▲ 20,25%
TRANSACTION APPROVALS	260.249	352.638	▲ 35,50%
HARD FALSE POSITIVES	0	403	(*)
SOFT FALSE POSITIVES	260.249	70.043	▼ -73,09%
HARD FALSE NEGATIVES	0	3.585	(*)
SOFT FALSE NEGATIVES	15.371	9.153	▼ -40,45%

(*): The current flow does not block directly any transaction, so it's not possible to compare

Now, comparing the Positive and Negative impacts from the decision flow change

INCOGNIA

Negative

- **Non fraudulent transaction may be blocked:**
  - One of the rules blocks transactions with distance from the frequent location greater than 1000 kms, and it may cause good international transactions to not be allowed. There's a need to address this problem, such as creating a "Travel mode" for the user.
  - The new high-risk classification blocks devices with more than 3 accounts associated, and there might be good users with this characteristic. Having a message to contact the Fraud Support team should handle those cases.

- **There might be fraudsters in the low-risk classification.** Having more data and variables will make the decision more precise and with less False Negatives.

Positive

20,25% uplift on revenue by **reducing fraud losses by 30,81%** and **2FA costs by 69,55%**

68,39% of transactions would go through the decision flow **frictionless**, making the user experience much better

Protection from device emulation, tampered apps, location spoofing, jailbreaks, etc

Increased the approval rate to 88,19%

Reduced the number of **Soft False positives by -73,09%** and **Soft False negatives by -40,45%.**

Future Improvements

Recommendations for better fraud recognition and improvement of User Experience

Following the implementation of the new decision flow, it might be good to look for more improvements

Data from previous transactions per account: The Transactions dataset has almost only 1 transaction per account, and it would be very beneficial to get more data from previous interactions, for example: Average transaction values; Total completed transactions, Distance from other "frequent" locations, Risk Score from Bureaus, etc, and it would make the **detection of Account Takeovers (ATOs) by difference in the customer behavior;**

Develop a more robust fraud detection model, using ML and other technologies: This new decision flow is a rule-based one, and a ML model would get fraudster patterns much better and adapt to new ones. A combination of rules and models is a good approach.

Increase the number of variables since we have just 7, and having more data makes the fraud assessment easier and more precise. Examples of new variables:

- **Network**: User frequent IP, Wi-fi networks, number of fraudulent devices nearby, etc
- **Location**: High-risk regions, mismatches, etc
- **Previous accounts and devices with fraudulent transactions**: Create a blacklist (or a watchlist if the intent is to not block) with these devices, and increase the chance of blocking or performing a 2FA
- **Device information**: Year, model, etc
- And many more

Create new solutions for corner cases. For example, people traveling and creating transactions will not be allowed to do that.

Developing more types of 2FA: One that is harder, such as taking an ID photo, and another that is softer, such as inserting the password again or even checking other variables in the backend

Having analysts blocking or allowing transactions with high values and detecting new fraud patterns

INCOGNIA

Conclusion

With this descriptive analysis, we were able to **better understand the users behavior** and **identify some of the fraud patterns**, which led to the creation of new fraud risk classification rules and the new decision flow.

After applying these rules, that classifies the transactions into high, medium and low risk, the Digital Bank will be able to get a **20,25%** revenue uplift, reduce fraud losses by **30,81%**, 2FA costs by **69,55%**, improve the **user experience** by letting **68,39%** of transactions happen frictionless, **block transactions from device emulation, tampered apps, location spoofing, jailbreaks, etc**, increase the approval rate to **88,19%** and reduce the number of Soft False positives by **73,09%** and Soft False negatives by **40,45%**.

The performance can improve even more if, in the future, they get more variables, such as previous transactions and network data, develop other 2FA solutions and ways to deal with the corner cases, evaluate high-ticket transactions with Fraud Analysts and create a more robust fraud detection model, combining ML models, rules and analysts.

↓ **-30,8%** in fraud losses	↓ **-69,5%** in 2FA costs	↓ **-73,1%** False Positives
88,2% Approval Rate	**69,6%** Auto Approves	**3,19%** Fraud Rate
↑ **20,3%** in Revenue	↑ **35,5%** Approvals	↓ **-40,4%** False Negative

Github Repository

You can reproduce the code and create your own graphs in Databricks. The Github repository is HERE. In the README.md file, you have the instructions to set the environment.

Code Snippets

You can check a few code examples in the Appendix section from the Report HERE

INCOGNIA