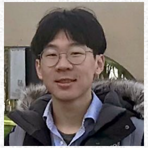
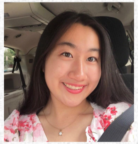
Scotiabank Data Science Discovery Days

Team 0To∞

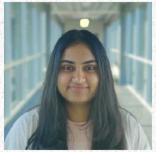


Alex



Sarah

Joe



Rithika

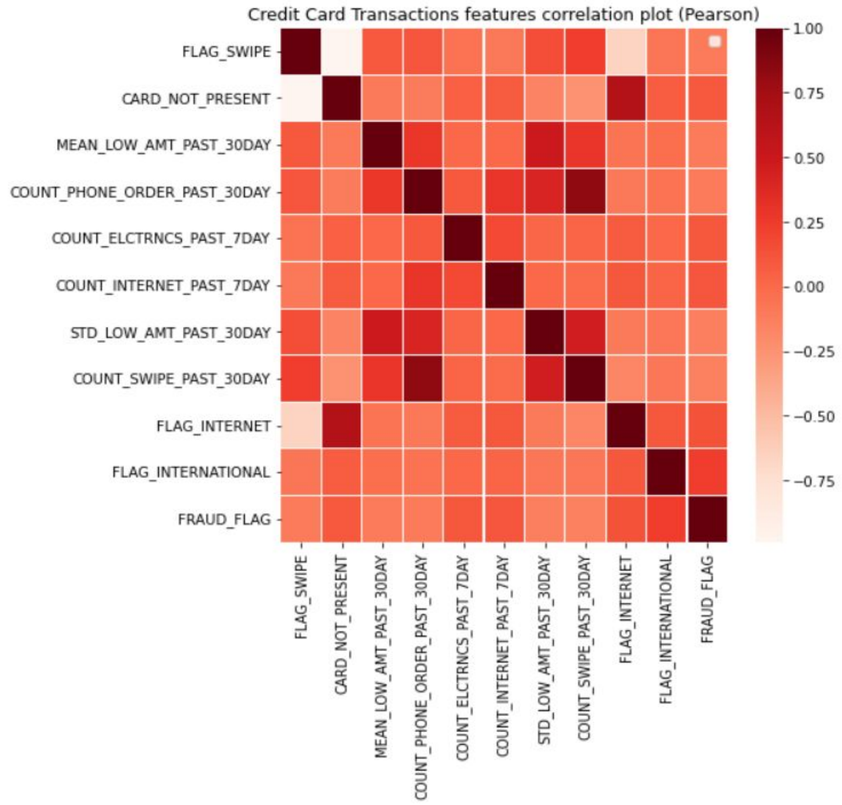
Austing

The Data

Let’s start by exploring the data to better understand the underlying patterns and interactions between variables.

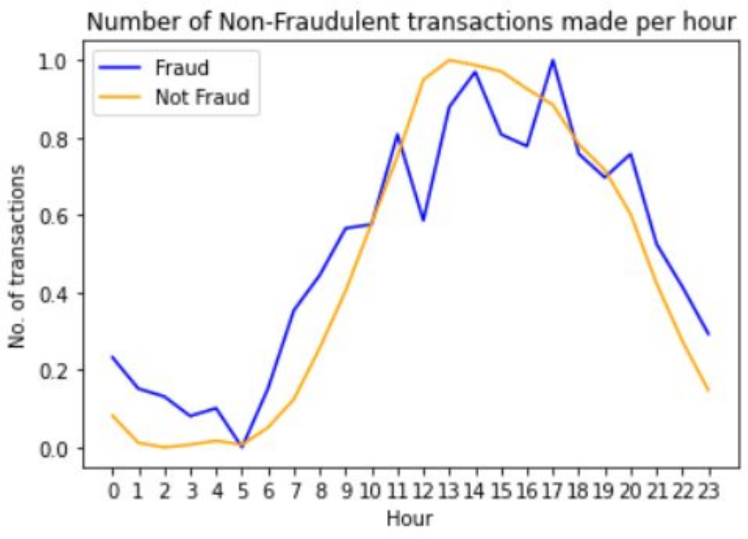
This plot shows the correlation between the **ten features** that have the highest magnitude of correlation with FRAUD_FLAG.

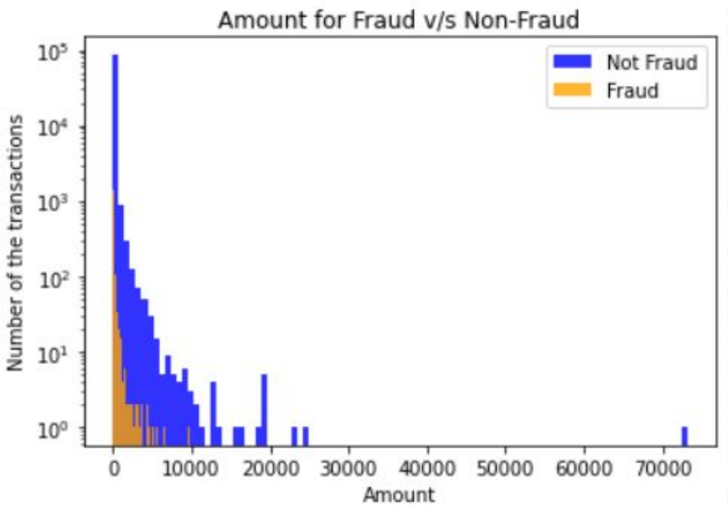
FLAG_INTERNATIONAL and FLAG_INTERNET are most correlated with FRAUD_FLAG.



The Data

Right: Distribution over time of day for fraudulent and legitimate transactions. Fraud transactions are distributed similar to legitimate transactions.





Left: Transaction amount histogram for fraudulent and legitimate transactions. Legitimate data is more heavy-tailed.

Our Model

XGBoost

We used **XGBoost** – a tried-and-tested implementation of gradient-boosted-decision trees, that has been shown to be effective on tabular data.

The data is **highly unbalanced**–only **2.4%** of transactions are fraudulent. Baseline XGBoost F1 suffers due to **low recall**.

We try two approaches to improve recall:
- **SMOTE** applies data augmentation to the minority class, to balance the number of examples in each class
- **Thresholding** – we search for the optimal prediction threshold to maximize F1 score on a validation set.

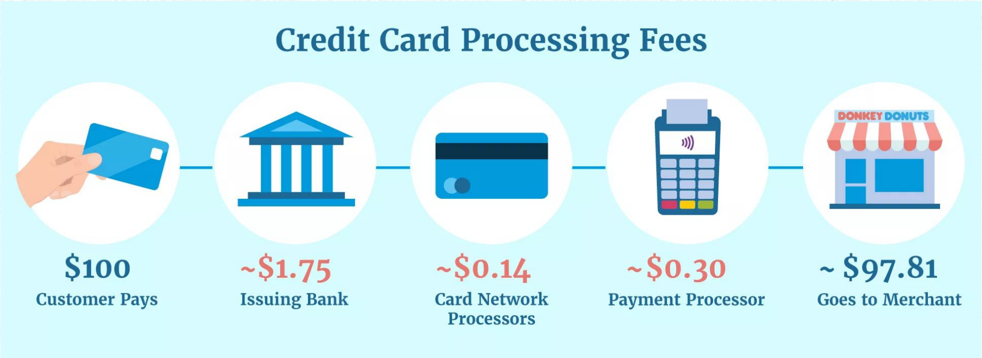
Thresholding works better. Combining Thresholding and SMOTE did not lead to improvements. Finally, we did some further hyperparameter search, which also helped improve F1.

Model	**F1**	**P**	**R**
XGBoost Baseline	0.43	**0.75**	0.30
SMOTE (1:1 ratio)	0.49	0.58	0.43
Optimal Threshold	0.58	0.55	0.60
+ Tuning	**0.62**	0.56	**0.69**

Which transactions should we decline?

We have a model that optimizes for F1. Is that the end of the story?

- **Of course not!** A fraud prediction model is only one component in our decision-making process for choosing which transactions to decline.
- Our downstream business objective is to **maximize revenue** for stakeholders.

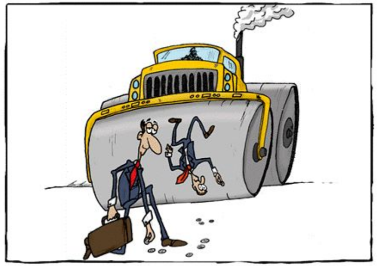


(**Image source: CreditDonkey** https://www.creditdonkey.com/credit-card-processing-fees.html)

(*Claim source: CPA Canada https://www.cpacanada.ca/en/news/canada/2019-12-06-credit-card-fraud)

- The issuing bank is typically liable for successful fraud*. Hence, marking **fraud as safe** is roughly **50x more costly** than marking **safe as fraud** (on a $100 transaction, a bank stands to gain $2 at the risk of losing $100).

Which transactions should we decline?



(**Image source:** https://seekingalpha.com/article/4083775-picking-up-nickels-in-front-of-steam-roller)

We consider a **simplified model of revenue**:

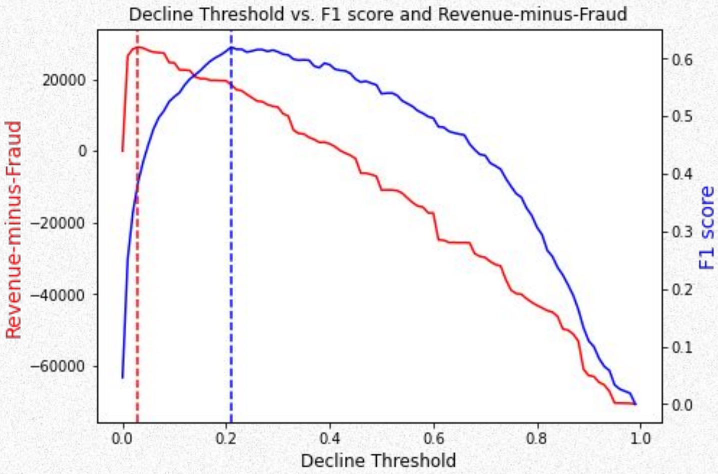
- Approve a legitimate translation: +2% of transaction cash value.
- Approve a fraud transaction = -100% of transaction cash value.

Evaluating models by revenue:

Model	Revenue ($)	F1
F1-OPT Threshold	18,507	**0.62**
Rev-OPT Threshold	29,047	0.39
+ Upweight Pos. Training	**30,992**	0.34

- The threshold that maximizes F1 does not maximize revenue.

- Also, upweighting loss of error on fraud examples during training improves revenue.



How to minimize the negative impact to customer experience while preventing fraud?

Model	Revenue ($)	# of Legit Transactions Declined	Decline Rate of Legit Transactions
F1-OPT	18,507	**282**	**1.29%**
Revenue-OPT	**29,047**	1432	6.57%
Balanced	27,178	458	2.10%

- When we fully optimize for F1, we are paying $9.08 for each false positive reduced.

- Being conservative only for transactions ⩾ $150 (Balanced) buys us 974 FP reductions @ $1.92 each.

A simple strategy for lowering decline rate while preserving revenue: use the conservative model when the amount is ⩾ some threshold ($150). Improves customer experience for small revenue hit.

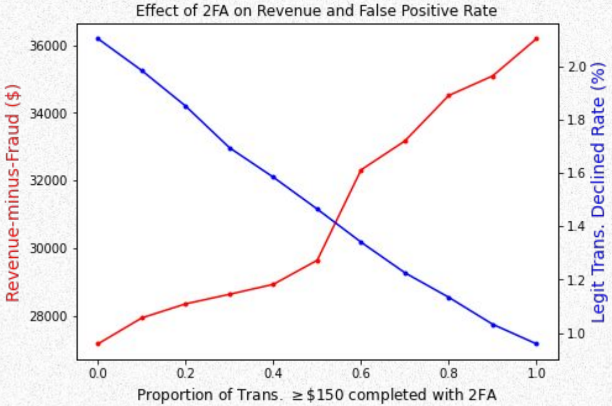
Limitation: our simplified revenue model doesn't account for second order effects of declining legitimate transactions on revenue. We need to study its effects on customer churn rate.

How to minimize the negative impact to customer experience while preventing fraud?

Two-factor authentication: We should let customers submit their own preferences for **personal fraud tolerance** (ie. opting in for 2FA for increased fraud protection, or subscribing to **notifications** on certain purchases and patterns). **Increased adoption of 2FA increases revenue and reduces false positives**.

Privacy concerns for fraud alerts: Precise location, dates, and times are sensitive information–we should minimize access to this information, internally and externally. Instead: offer general warnings ("Review your transaction history for suspicious activity.").

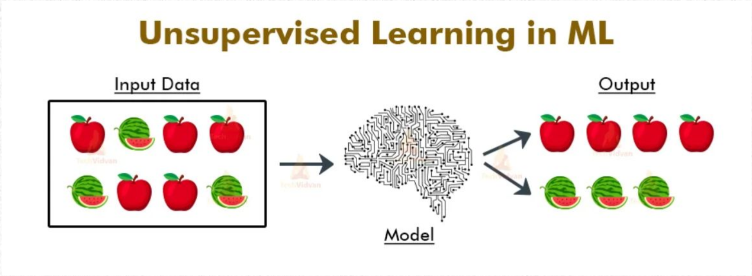
(Image source: Imperva https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/)



How to prevent fraud more effectively without creating operation overhead?

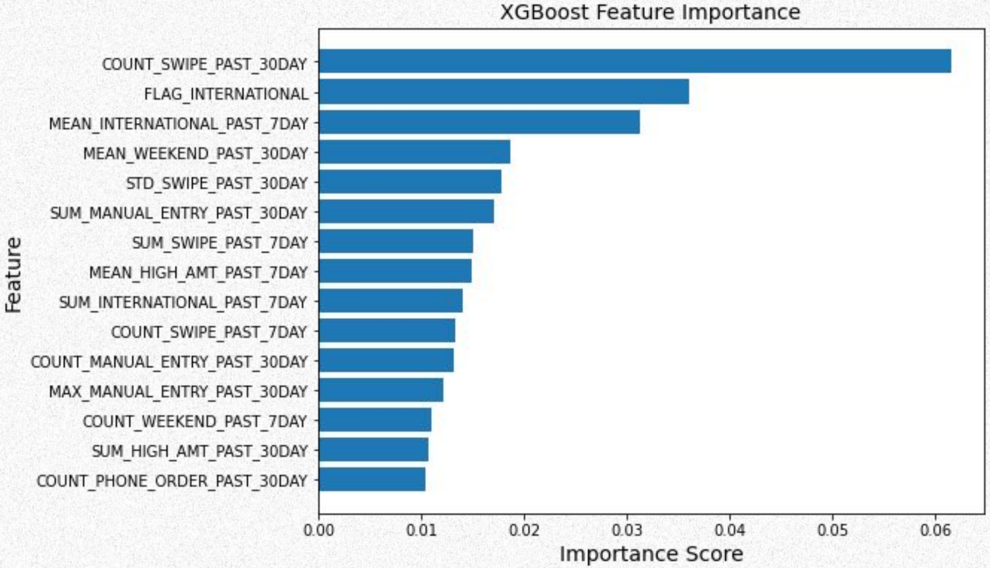
AI & ML: Unsupervised Machine Learning (**UML**) can detect unknown fraud patterns at the time of account registration. Models that use UML are said to detect fraud around **30 days earlier** than other solutions. (Source: SDC Executive https://www.sdcexec.com/transportation/article/21196540/4-ways-to-fight-shipping-fraud-while-reducing-operational-overhead).

Accelerated analysis: Automation & **bulk decisioning** increase efficiency by uncovering clusters of fraudulent activity within the same fraud ring. This eliminates manual reviewing and is said to reduce operation overhead by **40%**. (Source: SDC Executive https://www.sdcexec.com/transportation/article/21196540/4-ways-to-fight-shipping-fraud-while-reducing-operational-overhead).



(Image source: TechVidvan https://techvidvan.com/tutorials/unsupervised-learning/)

What are some key attributes that help to make the decline decision?



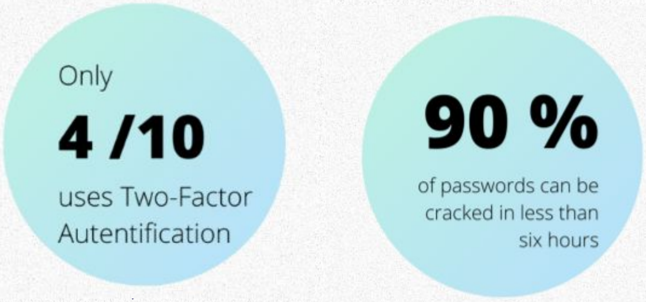
Our model is skeptical of **international transactions,** and places emphasis on the typical means of using the card (history of **swipe/phone order/manual entry** transactions).

When making decline decisions to optimize revenue while minimizing false positives, transaction amount is a key attribute.

Amount	**Decline Rate (%)**
< $150	13.9%
≥ $150	2.3%

Can you make any long-term suggestions?

1. **Being risk-averse pays.** More conservative models that don't necessary achieve the best F1 score are better suited for the business objective of maximizing revenue.
2. **A hybrid strategy to reduce fraud while maintain customer experience.** Using the more conservative model for large transactions and the better F1 score model for small transactions can reduce the false positive rate with little revenue reduction.
3. **Two-factor authentication.** Implementing 2FA for large transactions can reduce false positive rates and improve revenue.
4. **Markers of fraud.** Key markers of fraud used by our model are the "international" flag and the means of which users make transactions. Suggests areas for preventative action
5. **Distribution shift.** The F1 score of 0.62 is achieved when the train-test split is random; irrespective of the time. When we trained the model on data from consecutive months and tested on a holdout set of the next month, the F1 score dropped to 0.5. Real-world data is time-sensitive and the model must be continuously tuned to account for distribution shifts.



(Image source: AdminControl https://blog.admincontrol.com/en/why-is-two-factor-authentication-2fa-so-important)

Thanks for Watching

Hope our project can take fraud detection from 0To∞ :)