Experiment – Finding the best Privacy Technology & ML for predicting credit card fraud

# Overview

PTFI provides state of the art AI solutions to combat financial crime. It offers pretrained model as a service. On top that it is using privacy enhancing technologies to keep sensitive data private for all parties involved.

# Scenario (Use Case)

In this experiment scenario, there is a lot of credit card data that has been sent to AUSTRAC from different financial institutions around the country. With this data AUSTRAC is seeking to build a machine learning model which can detect credit card fraud. The experiment aims to build a fraud detection machine learning model without privacy technologies. A second model will then be built with each of the four main privacy enhancing technologies first used on the credit card data.

# How the Experiment will be run?

First Part (Building ML Model to predict credit card fraud):

1. Generate synthetic bank credit card transactional data using an appropriate library;
2. Encrypt the synthetic data of the banks by removing personally identifying characteristics such as name and address;
3. Send the encrypted test data (bank data) to the server (ours);
4. Create **five copies** of the data (four for each prominent privacy technology) and one for no privacy technology being applied;
5. Train credit fraud classifier model on server (our) using the encrypted synthetic data (***That is why we need a synthetic data related to credit transactions with a target variable being fraudulent credit transaction***);
6. Select the best ML model for each privacy technology;
7. Use model parameters for testing if transactions are fraudulent.

Second Part (Reporting):

1. Report on test inferences for each of the five models. This is which works the best, which is easiest to use etc.;
2. Encrypt and send the best model with example predictions of credit card fraud back to the bank;
3. The bank will decrypt output predictions and calculate accuracy.

# Conclusion

We have a pretrained classifier model that predicts credit fraud. We specialise in building state of the art models to combat financial crime. We will report to the mock bank or AUSTRAC the best privacy technology and machine learning model to predict credit card fraud from their data.