Experiment – Federated learning for fraudulent transaction identification

# Overview

PTFI provides state of the art AI solutions to combat financial crime. It offers the ability for participating financial institutions to identify fraudulent transactions in real time via a federated learning approach.

# Scenario (Use Case)

In this experiment scenario, we will aim to apply a federated learning algorithm to multiple synthetics bank transaction datasets. The purpose will be to attempt to train the data from local nodes and to generate global model parameters which will then be applied to new datasets to create predictions. The experiment aims to provide financial institutions with an iterative learning approach which utilises data from a range of data sources i.e. banks instead of a single bank. The focus will be on flagging suspicious transactions which might be fraudulent so that they can be investigated further.

# How the Experiment will be run?

The following steps provide a guide on how the experiment will run:

1. Generate synthetic bank transactional data using an appropriate library (SDV).
2. Build a model for predicting fraudulent transactions.
3. Use federated learning to push the model to the local nodes (other synthetic datasets).
4. Backward pass the parameters to the global model which is updated based on the local node result.
5. Update the parameters and re-build the global model.
6. Push the model to new local nodes (new datasets).
7. Assess the results i.e. predictions.

# Conclusion

The results from this experiment will guide the direction of which types of privacy technology works best for identifying fraudulent transactions. The limitations for this experiment are that it is focussed on only one type of privacy technology (federated learning). However, the novel application of this technology would provide PFTI a distinct product differentiation and early mover status in the privacy technology space.