Credit Card Fraud Detection using Machine Learning

Our goal is to implement various machine learning models to classify  
credit card frauds from a dataset collected over two days in Europe in September 2013. Logistic regression models, k-means clustering models, and neural networks.  
Some of the challenges observed from the beginning were large imbalances in the dataset. Fraud accounts for only 0.172% of fraudulent transactions. In this case, having a false negative  
prediction is much worse than a false positive. Because a false negative  
means someone escapes her credit card fraud. False positives, on the other hand, introduce complexity and potential annoyance only if the cardholder needs to confirm that the transaction in question was actually completed (not a thief).

The difficulty with the data set was that there were 30 features, but all but 28 were PCA-transformed s in s to protect confidentiality, and the labels were unknown. The known untransformed characteristics were "Time" , which measures the number of seconds between a transaction and the first of the two days, and "Money" (presumably in euros), which represents the cost of the transaction. To compensate for imbalance in the dataset, we oversampled the malformed (class = 1) portion of the data and added Gaussian noise to each row.

Principal component analysis was used for the K-Means model to reduce the dimensionality of the data from 31 to 2 . Only the two features with the largest variance were used for model training. The model was adjusted to have two clusters where 0 is no cheats and 1 is cheats. I also experimented with different values ​​of for the hyperparameters, all with similar results. Changing the dimensionality of the data 2 (reducing it to 2 or more dimensions) made little difference to the final value of the .