**Literature review**

Credit card default prediction is described as an application of classification techniques within data mining. Financial and lending institutions employ probability of default (PD) models to calculate expected loss associated with default, and more generally identify individuals who are more likely to default on a payment. Similarly, fraud detection is another component within risk management employed to mitigate loss. Prediction of both credit card default and fraud see the application of similar binary classification algorithms. Due to the similarity between the two applications of classification, research dealing with both will be explored to more fully understand the current state and emerging state-of-the-art techniques. Also, the techniques highlighted address the challenges created by class imbalance in the outcome variable where the majority of cases (non-default or legitimate transactions) can significantly outnumber minority cases.

Universal to all literature in this area is the cited challenge with the lack of real-world data. Most available data is simulated or anonymized due to legal restrictions. Consequently, research development and the pool of available literature are somewhat limited or constrained by the limitations of the datasets. However, a key point is that the ability to apply accurate models within these risk management contexts can represent a huge potential savings for financial institutions.

Pasha, Fatima, Dogar, & Shahzad (2017) in their research explore the predictive accuracy of six algorithms for default prediction – linear discriminant analysis, Naïve Bayes, C4.5 decision tree, Logistic Regression, Neural Networks -MLP, and k-Nearest Neighbor (KNN). Their work evaluates performance using metrics such as accuracy (correct classification, incorrect classification, precision, and recall. The results show that the relatively newer algorithm of Multilayer Perceptron within the class of neural networks proves to be the best algorithm with an accuracy rate of 81.7%. It is worth noting that logistic regression is a close second in performance at 81%.

The use of MLP and KNN algorithms are the focus of Koklu and Sabanci’s research (Koklu & Sabanci, 2016) on estimation of credit card customer’s payment status using classification within data mining techniques. Specifically their research uses Multilayer Perceptron (MLP) and k-Nearest Neighbor (KNN) algorithms using the open-source WEKA data mining platform. The performance of these algorithms is evaluated in the context of accuracy, MAE (Mean Absolute Error), and RMSE (Root Mean Squared Error). Similarly results were found where the MLP algorithm outperformed the KNN.

Altabrawee (2016) examines fourteen classification models and their predictive accuracy in default prediction. He notes the importance of a successful model’s ability to avoid underfitting or overfitting training data. In particular, the appropriate amount of regularization in the model should be used to limit under or overfitting. Performance results are evaluated in terms of average accuracy, precision, recall, and F score. The partial decision tree algorithm PART is determined to be the most accurate while Naïve Bayes-related algorithms are at the bottom in performance.

Butaru et al. (2015) research the application of machine learning techniques to the problem of credit risk. Their focus is on decision tree, random forest, and logistic regression models. Logistic regression models are noted to be the more traditionally used models for assessing credit risk. Regularization is used in their logistic regression model in order to be more in line with the anticipated performance of the decision trees and random forest models. Performance is evaluated using precision, recall, F score, and the kappa statistic. Their research determines that, although all three models performed well, decision trees and random forest outperform logistic regression especially within short time horizons.

Within the broader context of risk modeling and applications of classification techniques, Lusis (2017) compare machine learning techniques for credit card fraud detection, analyzes fraud detection classification approaches using Logistic Regression (LR) and Random Forest (RF) algorithms. Their findings are compared to results from previous research conducted using SVM or Support Vector Machine algorithms. Citing the challenge of lacking real word data, Lusis’ analysis is constrained to simulated data for legal reasons. Both the LR and RF models are tested using PCA (Principal Component Analysis) and without PCA, which is a technique used to reduce the dimensionality of data. Of these models, Random Forest without PCA and K=3 had the best predictive performance as determined by accuracy, sensitivity, and specificity. They observe that applying a Preprocessing step helped the performance of the LR models whereas Preprocessing was not necessary for the Random Forest model.

Seeja et al. (2014) propose a novel approach to handling the class imbalance problem by using a frequent itemset mining approach based on an Apriori algorithm. The authors, also citing challenges with real world dataset availability, compare their itemset mining approach to SVM, K-nearest neighbor (KNN), Naiive Bayes (NB), and Random Forest algorithms.

Evaluation of each model’s performance is done using Matthews correlation coefficient and BCR (and Balanced classification rate). Seeja et al. (2014) itemset approach outperformed all other test models as measured by sensitivity, false alarm rate, balanced classification rate, and Mathews correlation coefficient. It worth noting that the authors attempted to use SMOTE to address the class imbalance within the data and ultimately saw this lead to performance degradation so it was abandoned.

Padmaja et al. (2007) approach fraud detection as an unbalanced classification problem and research addressing class imbalance by using hybrid sampling techniques. They approach their research applying a “combination of random under-sampling and over-sampling using SMOTE.” SMOTE: Synthetic Minority Over-sampling Technique. Classifiers used are k-NN, Radial Basis Function networks, C4.5 and Naive Bayes.

Zareapoor and Shamsolmoali (2015) in their research also note that the lack of real world data for researchers has limited the amount of published literature available on the topic. They approach their research using five classification techniques – (1) SVM, Naive Bayes (NB), KNN, and Bagging ensemble. Their premise is that ensemble learning techniques are superior to the other techniques tested. To assess model performance, Zareapooret et al. (2015) also use the metrics of Fraud Catching Rate, False Alarm Rate, Balanced Classification Rate, and Matthews correlation coefficient. They discount using accuracy and error rate, citing these as biased metrics. Their analysis shows that a bagged ensemble classifier using decision trees ­outperforms KNN, NB, and SVM.

Sahin and Duman (2011) focus on Neural Networks and Logistic Regression (binomial and multinomial) classification models. They too raise the challenge created by class imbalance and recommend the use of under and oversampling techniques. Specifically, Sahin and Duman (2011) employ a stratified sampling “to under sample the normal records so that the models have chance to learn the characteristics of both the normal and the fraudulent records’ profile” (p. 5). Their research shows a clear performance advantage of Neural Net models over LR models and cites the overfitting behavior of logistic regression. Among the logistic regression models, stepwise MLR is the champion in both accuracy performance and catching fraudulent transactions except the last case.

The review above of available research shows many relevant models, techniques, and insights useful for our own research. While regression modeling is our main focus, we feel it important to consider techniques beyond logistic regression to more fully understand strengths and limitations of traditional techniques within the context of emerging state-of-the-art techniques. Clearly seen in the research though is that higher predictive accuracy is being driven through the use of ensemble machine learning techniques. While important to understand, ensemble techniques are outside the scope of this research.

**References**

Altabrawee, H. (2016). Performance Evaluation of Fourteen Machine Learning Algorithms on Credit Card Default Classification. Education College Journal, 463-473

Butaru, F., Chen, Q., Clark, B., Das, S., Lo, A., & Siddique, A. (2015). Risk and Risk Management in the Credit Card Industry. doi:10.3386/w21305

Koklu, M., & Sabanci, K. (2016). Estimation of Credit Card Customers Payment Status by Using kNN and MLP. International Journal of Intelligent Systems and Applications in Engineering, 249-251

Lusis. (2017, April 20). A Comparison of Machine Learning Techniques for Credit Card Fraud Detection. Retrieved from http://www.lusispayments.com/uploads/4/4/8/2/44826195/a\_comparison\_of\_machine\_learning\_techniques\_for\_credit\_card\_fraud\_detection.pdf

Padmaja, T. M., Dhulipalla, N., Krishna, P. R., Bapi, R. S., & Laha, A. (2007). An Unbalanced Data Classification Model Using Hybrid Sampling Technique for Fraud Detection. *Lecture Notes in Computer Science*, 341-348. doi:10.1007/978-3-540-77046-6\_43

Pasha, M., Fatima, M., Dogar, A. M., & Shahzad, F. (2017, March). Performance Comparison of Data Mining Algorithms for the Predictive Accuracy of Credit Card Defaulters. Retrieved from <http://paper.ijcsns.org>

Sahin, Yusuf &Duman, Ekrem. (2011). Detecting credit card fraud by ANN and logistic regression. INISTA 2011 - 2011 International Symposium on INnovations in Intelligent SysTems and Applications. 10.1109/INISTA.2011.5946108.

Seeja, K. R., & Zareapoor, M. (2014). FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining. The Scientific World Journal, 2014, 252797. <http://doi.org/10.1155/2014/252797>

Zareapoor, M., & Shamsolmoali, P. (2015). Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier. *Procedia Computer Science*, *48*, 679-685. doi:10.1016/j.procs.2015.04.201