Credit card fraud is a serious and growing threat in the digital economy, with global financial losses projected to exceed $34 billion USD by 2025 [1]. As the volume and speed of digital transactions increase, traditional fraud detection systems struggle to keep pace with the sophistication and adaptability of modern fraud activities. This gap highlights a critical need for more intelligent solutions capable of identifying subtle patterns in large, noisy, and highly imbalanced datasets.

Our project seeks to address this issue by developing a machine learning based fraud detection system that classifies credit card transactions as fraudulent or legitimate based on features like time, amount, and behavioural patterns. Reducing fraud is important to society, as it directly benefits financial institutions, e-commerce platforms, and consumers by lowering financial losses, enhancing trust, and improving user experience.

Through this project, we contribute to the broader effort of building safer and more resilient financial systems. We will apply and evaluate a range of supervised learning models, drawing from both academic and industry-standard approaches, and ensure our methods are robust to class imbalance and real-world deployment challenges.

We will be sourcing our data using Kaggle, a widely used and trusted platform in the data science community [2]. However, since not all Kaggle datasets are based on real-world data—some may be generated or simulated—we will take extra precautions in selecting one that is authentic and suitable for our project. As we are working with third-party data that we are not fully aware of how it was collected, preprocessing and cleaning of the data are essential to ensure data quality for training. This project aims to classify whether a credit card transaction is fraudulent, with the classification determined by other feature values such as amount and time. This makes it a supervised learning task. We plan to experiment with various machine learning techniques introduced in class and commonly used in industry, including linear regression, logistic regression, K-nearest neighbours (KNN), support vector machines (SVM), decision trees, and other methods we may find worthwhile throughout the project [3]. We will then select the best-performing models for our final implementation.

Since fraudulent transactions represent a small minority of the dataset, test error can be misleading in this setting, as it does not differentiate between types of misclassification errors. Instead, class-sensitive metrics that are robust to class imbalance will be used to evaluate and compare the performance of fraud detection models. Precision, recall, and F1-score will be employed to assess how well the models identify fraudulent transactions while minimizing false positives and false negatives. Precision measures the proportion of correctly identified fraud cases among all predicted frauds, while recall reflects the proportion of actual fraud cases that were successfully detected. The F1-score provides a balanced evaluation that is especially useful when both false positives and false negatives carry serious consequences.

To benchmark model performance and ensure consistent evaluation, baseline comparisons and validation strategies will be applied. Baseline models will include a majority class predictor that always outputs the non-fraud class, a random classifier, and a logistic regression model. These provide simple reference points to assess whether more advanced methods, such as ensemble models or anomaly detection techniques, offer meaningful improvements. Stratified k-fold cross-validation will be used to preserve class distributions across all folds and reduce variance in performance estimates. Random seeds will be fixed for all randomized processes, and version-controlled code will be used for data preprocessing, model training, and evaluation.

Our project has several potential risks that may compromise its execution and outcomes. One major concern is the reliability of third-party data sourced from Kaggle, since many datasets could be synthetically generated or have limited transparency with their collection methods. This could adversely affect model performance or limit how general our findings are. In response, we'll review the dataset quality closely and do extensive preprocessing to clean and normalize the data. An examination of several machine learning algorithms like logistic regression, KNN, and SVM may also be computationally intensive, particularly when parameter tuning and validation are involved. We plan to mitigate this by narrowing our focus to the most promising models and using efficient tools and libraries. Finally, since we have multiple team members contributing to the project, coordination and time management will be essential. We'll schedule regular team touchpoints and keep shared documents to facilitate communication and maintain progress at a steady rate.

We're following a structured but flexible plan to keep our project organized and manageable. Once we decided to work on credit card fraud detection, we reviewed multiple datasets and agreed on a well-known Kaggle dataset that reflects real-world challenges. Before diving into implementation, we discussed possible machine learning models and evaluation metrics, which helped us develop a rough timeline and division of tasks.

We plan to work in phases. First, we'll focus on understanding and cleaning the data to ensure it's usable. After that, we'll implement several models and compare their performance using standard metrics like accuracy, precision, recall, and F1-score. We'll refine our approach and focus on the best-performing methods based on our initial results. This way, we stay open to changes without getting off track.

For collaboration, we use GitHub to share and manage code, Google Docs/Sheets for planning and writing, and Discord for quick communication. We'll meet weekly to check in, make decisions, and help each other out with any blockers.

We divided responsibilities based on each member's interests, strengths, and experience. Early in the planning stage, we discussed which parts of the project we felt most confident in or wanted to explore further. From there, we assigned roles that allowed everyone to contribute meaningfully while learning something new. We ensured the workload was balanced and each team member had a clear area of ownership. This approach helps us work more efficiently and stay accountable while encouraging collaboration when tasks overlap.

References

[1] The Nilson Report. (2025, January 6). *Payment card fraud losses approach $34 billion*. GlobeNewswire. https://www.globenewswire.com/news-release/2025/01/06/3004931/0/en/Payment-Card-Fraud-Losses-Approach-34-Billion.html

[2] Alexandre, “Kaggle : All you need to know about this platform,” Data Science Courses | DataScientest, Feb. 20, 2023. https://datascientest.com/en/kaggle-all-about-this-platform

[3] MathWorks. “Choosing the Best Machine Learning Classification Model and Avoiding Overfitting.” Www.mathworks.com, www.mathworks.com/campaigns/offers/next/choosing-the-best-machine-learning-classification-model-and-avoiding-overfitting.html