Business Scenario

A financial payment company wants to predict fraudulent transactions to prevent financial losses and reputational damage.

Business Case

Executive Summary: The application of data science in the financial payment industry can help prevent fraudulent transactions, saving companies significant amounts of money. Our analysis using the Business Understanding phase of the CRISP-DM framework has identified the key factors that contribute to fraudulent transactions.

Introduction: Fraudulent transactions pose a significant risk to financial payment companies. The implementation of data science can help prevent fraud and protect the company's revenue. Our goal is to use the CRISP-DM framework to identify the factors that contribute to fraudulent transactions.

Business Understanding

Define the problem statement and business objectives: Our objective is to prevent fraudulent transactions and increase the accuracy of the fraud detection process.

Identify the stakeholders and their interests: The stakeholders include the financial payment company, customers, and regulatory authorities. The interests of the financial payment company are to protect its revenue and reputation, while customers and regulatory authorities are interested in ensuring the security and safety of the payment system.

Determine the data mining goals: The data mining goals are to identify the factors that contribute to fraudulent transactions, develop predictive models to prevent fraud, and optimize the fraud detection process.

Assess the current situation: The current situation involves analyzing historical transaction data, fraud cases, and customer behavior data.

Determine the success criteria: The success criteria are to reduce fraudulent transactions by 50% and optimize the fraud detection process.

Results: Our analysis has identified that customer behavior data, transaction history, and payment system data are the key factors that contribute to fraudulent transactions. We have also

identified that transaction history data can be used to develop predictive models that can detect fraudulent transactions.

Recommendations: We recommend that the financial payment company implements a predictive model that uses the previous transaction data to detect and prevent fraudulent transactions in real-time. We also recommend that the company continuously updates its fraud detection algorithms and uses customer behavior data to optimize its fraud detection process.

Conclusion: Our analysis using the Business Understanding phase of the CRISP-DM framework has identified the key factors that contribute to fraudulent transactions and developed predictive models to prevent fraud, which can help financial payment companies protect their revenue and reputation.

References

1. <https://www.kaggle.com/datasets/arunavakrchakraborty/financial-payment-services-fraud-data>
2. <https://www.kaggle.com/code/arjunjoshua/predicting-fraud-in-financial-payment-services>
3. <https://philarchive.org/archive/MEGFFT-2>