Payment fraud analytics

Payment fraud occurs when a fraudster obtains sensitive payment information from customers or businesses and uses it for financial gain. This includes but is not limited to stealing credit card details individually or through data breach of a company which stores such information.

In 2022, U.S. businesses faced a staggering loss of $1.59 billion due to payment fraud(Sift, 2024). It is therefore in the interest of businesses to invest in ways to mitigate these losses.

Data analytics is being used extensively and increasingly to do just time in a number of interrelated ways.

Patterns in payment behaviour can be collected by financial institutions themselves since they record the information as they process it. There are of course enormous amounts of data to be processed. There is also a very small number of actual examples of fraudulent behaviour which is comparable to finding a needle of undefined shape and size in a haystack(Boiarskaia, Albert and Lee, 2019). That said, details such as transaction amount, geographic location, time and frequency of transactions, preferred merchant types, and type of purchase can be recorded by financial institutions interested in examining normal behaviour and fraudulent behaviour patterns.

Unsupervised machine learning techniques are currently used to identify patterns that deviate from normal behaviour without labelled data.

Profiles for individual credit card holders can be created by studying their normal payments(Budd, 2016).

Supervised machine learning can be used to train a detection model using the historical data available to payment processors. This in turn can be used when processing payments to permit or deny transactions in real-time.

In this way, anything that falls outside the norm for an individual card holder, such as a sudden increase in transaction frequency, large transactions, or transactions in unfamiliar locations, may result in prohibited transactions.

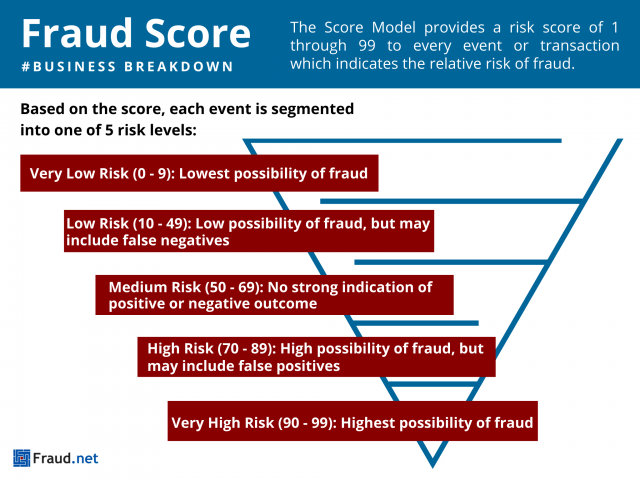
Below is an example of a decision tree which can be used to monitor, permit or deny payments made by individual card owners.

A diagram of a network

Description automatically generated

Each node in the decision tree asks the question, is this behaviour typical of an individual customer? In each case, if the answer is no, the payment will not proceed.

Of course, this is a simplistic view. More accurately, nodes would be assigned an aggregating value depending on their outcome, which would be weighed against a predefined threshold. If the final value is greater than the threshold, the payment will not proceed. It might look something like the graphic below (Fraud.net, 2024).



As mentioned before, also a very small amount of data containing actual fraudulent behaviour exists. To discern normal behaviour patterns experts will define with a set of rules based on what fraud normally looks like. This has led to a rule-based system consisting of predefined criteria determining whether transactions will be allowed or denied.

As new methods of committing fraud emerge, constant analysis is required so that detection systems evolve to meet current demands. Continuous analysis of current data takes place to try to stay ahead of fraudsters. At the same time, considerable collaboration between financial institutions, technology organisations and others also contribute to an ever-evolving rules list.

This has resulted in innovations like two-factor and biometric authentication being used to avoid fraud. For instance, relatively recently many institutions have begun using push notifications on customers mobile devices to confirm the validity of payments.

By combining these approaches, financial institutions can create robust credit card fraud detection systems that effectively identify and prevent fraudulent activities while minimizing false positives. The integration of advanced technologies, such as artificial intelligence and machine learning, further enhances the accuracy and efficiency of these systems.

References:

Boiarskaia, E., Albert, N. and Lee, D. (2019) *Detecting Financial Fraud at Scale with Decision Trees and MLflow on Databricks*, *Databricks*. Available at: <https://www.databricks.com/blog/2019/05/02/detecting-financial-fraud-at-scale-with-decision-trees-and-mlflow-on-databricks.html> (Accessed: 4 March 2024).

Budd, J. (2016) ‘Modelling credit card usage for individual card-holders’.

Fatima, A. (2022) ‘Data Analysis for detecting Credit Card Fraud’, *Medium*, 1 October. Available at: <https://aliya-fatima.medium.com/data-analysis-for-detecting-credit-card-fraud-f55d33c091b3> (Accessed: 8 February 2024).

Fraud.net (2024) *Fraud Score*, *Fraud.net*. Available at: <https://fraud.net/d/fraud-score/> (Accessed: 4 March 2024).

Gautam, A. (2023) *Data Analytics Case Studies: Success Stories from Various Industries*. Available at: <https://www.linkedin.com/pulse/data-analytics-case-studies-success-stories-qyhvf> (Accessed: 8 February 2024).

Sa’adah, S.A. and Hartanto, A. (2023) ‘FRAUD DETECTION USING DATA ANALYTICS IN THE CUSTOMS CONTEXT: A CASE STUDY OF UNDER INVOICING IMPORTATION FRAUD IN Indonesia’, 16.

Sift (2024) *How to evaluate payment fraud analytics and measure risk*, *How to evaluate payment fraud analytics and measure risk*. Available at: <https://sift.com/blog/how-to-evaluate-payment-fraud-analytics-and-measure-risk> (Accessed: 4 March 2024).