Machine learning modelling for enhanced APP scam prevention

Abstract

To safeguard our members and stay ahead of evolving fraud tactics, Nationwide is constantly working to strengthen its prevention of Authorised Push Payment (APP) scams.

Conventional rule-driven criteria which are typically used in the industry to prevent APP scams provide a robust baseline defence for fraud prevention, however, can be limited when it comes to preventing more complex fraudulent behaviour. This is where Machine Learning comes into play.

A Machine Learning (ML) ensemble model can leverage advanced statistical algorithms to learn complex patterns with greater scalability, efficiency, and autonomy. However, a key challenge for this project was the implementation of an advanced model in the existing fraud prevention system. This was overcome by exporting ML models into the Predictive Model Markup Language format, enabling the successful implementation of a transactional level ML model for APP scam prevention. This model is being used in combination with more traditional methods to form a multi-layered approach for APP scam prevention.

This presentation will cover:

• What are APP scams – a high-level overview of what APP scams are, and how they are prevented in financial services.

• The Advanced Analytical approach – summarising the benefits of using ML models to target APP scams and how they are implemented.

• Case Study – an example of how the Advanced Analytical approach has been used to improve APP scam prevention at Nationwide.

This presentation blends business and modelling knowledge together to demonstrate the uplift Advanced Analytical modelling techniques can provide within the area of Fraud.

Authors & Affiliations

Dr Tim Pickering[1], Dr Jack Noonan[1]
[1]Nationwide Building Society, Swindon, United Kingdom