Hero Story

Good for Australia: eftpos drives down fraud losses with real-time machine learning

A complex challenge

pre ARIC

While globally more and more businesses and individuals are transacting in eCommerce Card-Not-Present (CNP) environments or using mobile payments, the move to digital has not stopped Australians using debit cards. In fact, debit cards are still by far the most popular payment choice, accounting for around 70 percent of the nearly one billion electronic transactions in Australia each month. Contactless payments are also hugely popular as the country accounts for the highest use of "tap and go" payments in the world.[1]

Most debit cards in Australia are dual-network debit cards. These are cards that enable payments to be made through either eftpos, Australia's national debit card network, or one of two international networks. The fee a merchant must pay to their financial services institution for accepting a debit card transaction depends on which of the three networks handles the transaction. This option to route dual-network debit card transactions through the lowest-cost network route (Least Cost Routing) is driving the exponential transactional growth in both Card-Present (CP) and Card-not-Present (CNP) transactions for eftpos.

However, with debit cards the go-to payment choice for most Australians, criminals have shifted their focus to exploit this payment route, especially CNP transactions. CNP fraud accounted for 91% of all fraud on Australian cards in FY222. CNP transaction fraud requires little effort compared with other fraud typologies. By purchasing stolen credentials on the dark web or obtaining card information, CVVs, and billing addresses under false pretenses, criminals can scale swift attacks to gain considerable rewards. Financial institutions (FIs) – with existing fraud detection systems and strategies in place – often struggle to spot and stop bad actors among the millions of digital transactions without causing unnecessary friction to card holders.

The smart solution(s) to the challenges eftpos faced

eftpos was set-up and is owned by Australia's major issuing banks, known as their members.

eftpos prides itself on investing into innovation for its members and on helping to keep Australians safe in the digital economy. A long-standing staple of the country's financial landscape, it has allowed electronic payments at the point of sale for almost four decades. Evolving with the shift to eCommerce and mobile payments eftpos looked to utilize a full card fraud machine learning solution to complement their members' fraud prevention strategies, covering both CP and CNP transactions, to enable the delivery of secure and seamless transaction experiences.

But herein laid the challenge.

Perhaps the most significant obstacle for any organization looking to leverage machine learning in its business is the requirement to have rich, consistently formatted historical data. eftpos had no historical CNP data upon which to build a fraud prevention strategy. And as eftpos would not issue accept/decline recommendations, the conventional methodology of applying policy driven rules that would deliver binary risk predictions, would not be viable. Instead eftpos wanted to provide a risk score and sub-classification code (SCC) to their members that would enable them to decide on the most appropriate course of action in accordance with their risk-appetite.

[1] Source: RBA Retail Payments data 2021

The smart solution, a new approach to analytics

Although eftpos had no historical CNP data, having visibility of transactions across the debit card network, including transaction data from both the issuer and acquirer was a significant benefit. By utilizing this data, ARIC™ Risk Hub can make inferences on behavior across the entire network rather than having to rely on the data from a singular member.

Powered by Adaptive Behavioral Analytics, a Featurespace invention, ARIC Risk Hub is an award-winning fraud detection and financial crime prevention platform with fully adaptive machine learning models that delivers real-time transaction monitoring for fraud and financial crime. ARIC Risk Hub ingests data across multiple channels to build profiles of genuine cardholder behavior, quickly analyzing the entire payment journey. With this self-learning technology – even as underlying behaviors change – anomalies in cardholder behavior are rapidly understood, evaluated, and acted on.

The solution for eftpos would encompass a bespoke machine learning model for risk scoring CP transactions, a new approach to analytics to deliver a rules-model hybrid (RMH) for CNP transactions and a set of complex rules to cover fraud sub-classification codes.

Delivering business impact, from day one

With this visibility and extent of data within the network portfolio substantially evolving and growing over time – with more transaction traffic and numbers of merchants – careful consideration was given to feature selection within the model – for example changes in data volume should not impact the distribution of the feature.

eftpos planned a phased rollout of their CNP solution with the model live and effective from day 1, able to cope with changes in data without any adverse impact on performance.

Industry game changing results

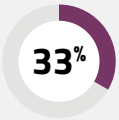
post ARIC

CP Model

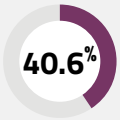
As eftpos had a rich set of historical CP data, they launched ARIC Risk Hub with the CP model first within a set threshold. Any transaction that achieves a risk score above a set threshold will trigger an alert. The threshold can be increased or decreased depending on risk appetite.

At a 0.1% False Positive Rate (FPR) the initial CP model achieved a 33% True Positive Rate (TPR) with a Value Detection Rate (VDR) of 40.6%.

FPR
The ratio between the number of genuine transactions interrupted as suspected fraud and the total number of actual fraudulent transactions

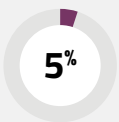


True Positive Rate (TPR)
Within the number alerts raised, more than a third of the alerts were genuine fraud

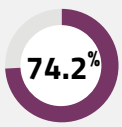


Value Detection Rate
The percentage of monetary savings assuming the fraudulent transactions triggered the blocking of subsequent transactions over all fraud losses

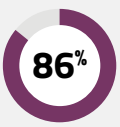
Relaxing the False Positive rate to 5% the True Positive Rate rises to 74.2% and Value Detection Rate is an outstanding 86%.



FPR
The ratio between the number of genuine transactions interrupted as suspected fraud and the total number of actual fraudulent transactions



True Positive Rate (TPR)
Within the number alerts raised, nearly half of the alerts are genuine fraud



Value Detection Rate
Exceptional percentage of monetary savings assuming the fraudulent transactions triggered the blocking of subsequent transactions over all fraud losses

post ARIC

CNP 'Cold Start' Model

To overcome the challenge of no historical data, Featurespace leveraged a 'cold-start' model for eftpos. With CNP transactions significantly riskier than CP transactions, it was paramount for such a model to stay accurate and self-learn, adapting to new streams and growing amounts of data traffic from evolving CNP transactions.

Transferred models are a unique and innovative way to provide high quality scores when historical data is unavailable. Featurespace's data scientists established a set of model input variables/features that had similar probability distributions across a range of datasets from the same domain.

These features were combined in a linear model, and the parameters/weightings applied to each input variable evaluated by averaging weightings learned on the corresponding variable from other data sets in the same domain. The constructed transfer learned model could therefore be applied to a fraud detection problem on any CNP dataset meeting certain criteria, robust to incremental changes in the composition of the data portfolio.

During offline research, transferred models caught **65%-85%** as much fraud as otherwise identical models trained on data drawn from the same source.

eftpos and Featurespace developed its SCC field, shared with members along with the fraud score for greater explainability. Some SCC risk types show accumulating fraud rates that are **10-100 times** higher than the no-risk typology code, evidencing the accuracy of the score.

In numbers based on fraud label eftpos reported:

False Positive Rate	True Positive Rate	Value Detection Rate
0.1%	5.6%	5.3%
1.1%	27.1%	37.2%
5.2%	51.1%	77.4%

0.1%

FPR
The ratio between the number of genuine transactions interrupted as suspected fraud and the total number of actual fraudulent transactions

5.6%

True Positive Rate (TPR)
Within the number alerts raised, more than 6 percent of the alerts were genuine fraud

5.3%

Value Detection Rate
The percentage of monetary savings assuming the fraudulent transactions triggered the blocking of subsequent transactions over all fraud losses

Many automated fraud detection systems today are operationally challenging and timely to implement. Collaborating to guarantee the best possible integration at every level, deploying, structuring, and integrating the complex sets of data feeds and cold start CNP model in this partnership, required just 15 weeks.

Today, the network intelligence that feeds the eftpos model ensures all members benefit from the model's learnings on attacks and new typologies, whether or not their organization is the initial target. eftpos members are achieving strength in numbers against rising global and domestic levels of financial crime.

> *The anti-fraud capability has widespread support from banks and FinTechs across the country and will scale quickly in the Australian market next year to provide real benefits for merchants and consumers as eftpos online market penetration grows."*
>
> Derek Kidd,
> Head of Fraud, Risk & Scheme Compliance

Get in touch to discover how ARIC Risk Hub can help you reduce your market share of fraud and bring down business risk and cost.

info@featurespace.com | featurespace.com

FEATURE SPACE
A Visa Solution