OPTIMISING APP FRAUD DETECTION:

THE PROVEN FORMULA FOR INCREASING AI'S EFFICACY

AUTHORISED PUSH PAYMENT (APP) FRAUD RUNS DEEPER THAN MOST OF US IMAGINE AND COME OCTOBER, WHEN 50/50 MANDATORY VICTIM REIMBURSEMENT KICKS IN, VERY FEW PSPS CAN AFFORD TO MISS EVEN A SMALL VOLUME OF APP SCAMS.

IT'S A SITUATION THAT HAS MANY PSPS LOOKING TO AI AS A KEY TOOL TO BOLSTER THEIR APP FRAUD DEFENCES.

As a co-pilot, AI is already transforming how fraud prevention experts deal with risk and criminal activity. AI can make sense of vast amounts of data astonishingly quickly and decipher connections that indicate risk, but due to their subtlety, would otherwise be missed.

This enhanced capability is crucial in combatting APP scams – which are often part of complex economic crime webs, whereby the scammer is rarely the orchestrator, and many perpetrators are first-time fraudsters.

But is AI enough when wider context is critical? Working with Pay.UK, Visa and Featurespace, Synectics set out to answer that question, with a focus on combing AI with authoritative syndicated reference data.

These are the results.

STRATEGIC OBJECTIVES

To explore the potential of an AI + syndication approach, we were asked to **assess the viability and value of introducing a new fraud overlay service that could analyse money flows and use predictive intelligence to proactively detect APP fraud and prevent financial crime.**

With mandatory reimbursement now an operational imperative, PSPs are under immense pressure to "know their customers" in a far greater depth, and intercept expertly-masked fraudulent payments before money leaves an account.

Crucially, Synectics wanted to see the impact of pairing syndicated data – transactional and point of application – with the AI models used, testing the AI + syndicated data formula.

THE THREE APPROACHES TESTED

As part of a pioneering data-sharing agreement, Synectics was given access to 12 months' worth of syndicated Faster Payments transactional data from participating banks and other PSPs. Using this we tested 3 different approaches to AI modelling using our Precision solution, which references data from the authoritative and ethical National SIRA risk intelligence syndicate.

APPROACH 1

This AI model used core transaction data, focused on learning the key characteristics potentially indicative of fraud risk, with features of the model engineered accordingly.

APPROACH 2

Still industry level, this AI model also incorporated syndicated transaction data including account history features - used to test any added value of syndication within the transaction dataset.

APPROACH 3

We then moved to a client specific model. As well as using data points from Approach 1 & 2, this also leveraged Point of Application (POA) and other data from an organisation's own specific customer base.

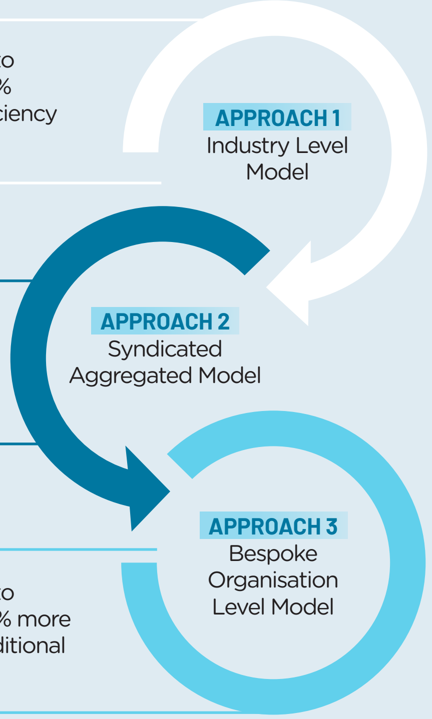
THE RESULTS: A FORMULA THAT WORKS

Working alongside industry partners and based on extrapolating results for 2023's APP fraud levels, the Pay.UK PoC **showed that AI trained on shared payments data could see £273m more fraud detected each year.** Of the AI model "rules" utilised in discovering the APP scams, 2 of the top 3 related to syndicated matching within National SIRA, and 7 of the top 10 related to syndicated transaction data.

Going from **Approach 1** to **Approach 2** captured 13% more scams with an efficiency gain of 23%.

Going from **Approach 2** to **Approach 3** added an additional efficiency gain of 45%.

Going from **Approach 1** to **Approach 3** captured 13% more scams and added an additional efficiency gain of 68%.



Our 3-step process helped us identify that Approach 3 - **combining core, syndicated and client specific data - yielded the best results.** The performance of AI was boosted by including the right type of consortium intelligence, a detail which clearly supports the need for data sharing in the payments space in tackling APP fraud.

ADDITIONAL FINDINGS

- **False positive improvement:** By combining core, syndicated and client specific data to inform AI modelling, APP fraud detection is possible at a better than **5:1 false positive rate**. This has significant implications for customer satisfaction and avoiding lost revenue.
- **Opportunities for fast tracking:** The results using Approach 3 showed that for every 1,441 transactions fast tracked, only 1 scam was missed, meaning that **98.8% of customer transactions could be safely fast tracked**. This is a promising outcome for automation strategies and customer experience improvements.
- **Focus on high-risk payments:** The PoC focused on payments of £1000 or more. Approach 3, applied to this specific transaction threshold enabled 45% of scams to be detected at a better than 5:1 FPR, equating to **£41m per annum.**

NEXT STEPS: WHAT CAN PSPS DO NOW?

Flagship research has proven that APP fraud detection is significantly optimised when AI is paired with local and syndicated data, at transactional and POA levels.

This will be welcome news to PSPs, who require ongoing PSR-compliant APP fraud strategies capable of preventing scam transactions before payments are authorised. If this does not happen, FSP organisations face consequences of unparalleled severity – reimbursement totalling 50% of the scam value, potential fines and substantial reputational damage.

The fraud overlay service tested with Pay.UK and partners remains, at present, a theory. However, Pay.UK states its interest in working with the payments industry to share the results more widely, and find ways to implement the service for the benefit of everyone in the UK. In the immediate term, **PSPs can take advantage of recent developments in the APP fraud prevention space, which include:**

LEVERAGING MULE-SPECIFIC CHECKS AT POINT OF APPLICATION

Money mules are often used to complete scam transactions, so hindering them is in the best interest of APP fraud prevention. Today, solutions exist that run checks against authoritative reference data, to offer a risk score based on mule propensity.

TRANSITIONING TO PERPETUAL KNOW YOUR CUSTOMER CHECKS

Continuous on-book screening solutions check for need-to-know events that may shift APP fraud risk levels – such as new connections or atypical behaviour between different institutions.

USING SCAM-SPECIFIC AI MODELS

With use-case specific modelling, is possible to flag when a suspicious transaction may be imminent – based on rapidly analysing the details of and relationship between the initiator and beneficiary. AI can also be used to help identify discreet or rapidly evolving risk markers at onboarding or review.

BEING PART OF A SYNDICATED FRAUD DATA NETWORK

PSPs not yet leveraging this as part of customer onboarding and general fraud prevention should investigate options which suit their specific needs. Remember, APP scammers – as well as operating across multiple banks also have a high propensity for involvement in other types of fraud monitored in risk databases.

Protecting your organisation and its customers from APP fraud requires unravelling the complex economic crime webs concealing scams. To achieve this goal, you need targeted technology, the most authoritative data and exceptional experience of delivery. This is precisely what Synectics delivers.

For help developing your APP fraud strategy, contact a Synectics consultant on info@synectics-solutions.com.