

'Schadenfreude' is no laughing matter!

People love it when the guy with the swanky new car ends up in a river because he followed his sat-nav. But there's no sense of Schadenfreude when you're dealing with massive fraud. Ironically, a 'sat-nav' type approach can help financial institutions and their customers keep out of hot water, believes risk expert Bart Patrick, SAS UK.

Sat-navs make the odd mistake...the software knows there's a ford across a river but it won't know that the river's swollen by recent heavy rain. What they are good at though is constantly re-calculating the best way forward if you take a wrong turning or change your mind about your destination.



Something similar is helping the finance world to combat fraud that cost the UK £428 million last year on plastic cards alone. Fraud is adapting and exploiting new possibilities 24hrs a day, much in the same way that your sat nav adapts to your changing route to a final destination. What is needed is fraud detection software which can match this ability for evolutions in fraud.

These are called 'neural networks'. They can observe what's happening to a transaction, create likely 'route maps' of where it is heading and predict whether it is fraudulent – all dynamically.

This is done by correlating data against known patterns of behaviour and creating mathematical models of fraud with the aim of nipping crime in the bud. Neural networks and sophisticated software are 'egg-head' stuff and a long way from the con-tricks that Arthur Daley used to play on TV. But fraudsters are getting smarter these days so financial institutions need to keep at least one step ahead.

Fraught about fraud

There are basically two types of fraud – internal and external.

An example of the former was highlighted in BBC documentary earlier this year about a high street bank. Undercover reporters gathered evidence of ruthless mis-selling by call centre agents (an operational risk), and further proof of activity which pointed directly to some employees working with criminals outside the organisation to commit fraud by enabling them to draw down money from fraudulently set up accounts.

A spectacular example of an external fraud attempt came to light when it emerged that hackers had stolen information from 45 million payment cards used by customers of US retailer TJX, which owns TK Maxx in the UK.

The TK Maxx scam started in 2002 before most people's cards were replaced with the much safer Chip and PIN system. As a result the damage is likely to be far less severe than the huge number of hacked card details might suggest but, at the time of writing, had yet to be fully assessed.

The latest figures from APACS, the UK payments association, show that the pattern of card fraud is changing but still represents a huge problem. The advent of Chip and PIN has almost halved fraud in face-to-face transactions because a stolen card is useless without a correct PIN number.

Losses incurred by UK retailers have plunged by £146 million over the past two years, but criminals are still 'cloning' the data held in the magnetic strip of stolen cards because they can be used in countries that have yet to adopt Chip and PIN.

Getting away with it

On the other hand, 'card-not-present' fraud used to make transactions over the Internet and through mail order has shot up 16 per cent over the previous 12 months because it is easier to get away with.

Whilst it's true that signature verification in the old face-to-face days was a bit of a joke – indeed you could probably scribble 'Mickey Mouse' and still receive your purchase – there are still flaws in current card-not-present methods because a stolen card shows details of its rightful owner's name, account number, code and expiry date.

The three-digit 'security code' on the back of the card is little more than sticking plaster because if you've got the card in your hand you've got all you need to buy something over the Web.

Much more needs to be done to guard against fraud, and the banks who invested £1.1 billion in the roll-out of Chip and PIN, know just how important reputation is, in an industry that has become more 'commoditised' than ever before – meaning that customers can switch allegiance with a quick phone call.

There are, however, five basic ways of fraud detection:

- Intelligence – somebody tells you that a crime is going to happen
- Validation – used a lot for cards whereby details are checked against a database verified by the likes of CIFAS, the UK's Fraud Prevention Service
- Visualisation – looking at unusual activity and spending patterns on an account
- Rules and scorecards – internal measures that can flag up that it's unlikely that a customer could buy something in Colchester and, two hours later, make another purchase in Kuala Lumpur
- Analytics – top end software that can create the neural networks or financial 'sat-nav' that can pre-empt fraudulent behaviour through the use of mathematical models.

Within a financial institution, the necessary steps are simpler and revolve around people, process and systems.

The people aspect is handled by the HR department. They are responsible for not hiring known felons - but there are plenty of people out there who just haven't been caught yet! Preventative remedies include analysing their behaviour, work patterns and computer usage to see if they might present an on-going risk post employment.

Process involves good housekeeping such as what an employee is allowed to take into or out of the office on their laptop or memory stick – a single USB stick, for example, would have the capability to contain all 45 million of TJX's stolen card records.

Systems should encompass a high-tech look at the correlations between inputs and have the ability to dynamically model likely frauds. Further to this, the use of visualisation techniques to understand and consolidate all available data, then bring likely cases of fraud to the attention of the bank's operator.

In essence, only a truly robust system, which embraces the entire chain of people, process and systems, can monitor potential fraud in real-time and stop it before any damage is done. This is what the public should demand of their financial institutions.

A 'sat-nav' approach to predicting fraud and avoiding its consequences is a good start. But you need a good system to avoid ending up in the drink!

Bart Patrick, Head of Insurance Practice, SAS UK.