

Fractals: Adaptive Solutions to Hi-Tech Financial Crime

Intelligent Fraud Detection

The Changing Face of Consumer Banking

Banking institution's strategies have developed dramatically over recent years. The huge growth in individual current accounts has been accompanied by an increased use of debit cards – now being widely used by current account holders at the point-of-sale and at ATMs worldwide.

The growth in retail banking accounts, together with widespread consolidation in the industry and the merging of smaller banks into larger entities, have been highly beneficial trends for both banks and their customers. But it has also introduced an Achilles Heel into the banking system by creating the precise conditions in which organized criminal gangs involved in card fraud like to operate.

Technology advances have made it easier for criminals to obtain both card PIN numbers and the sensitive data held in the magnetic stripe. Gangs will place realistic looking false fascias containing magnetic stripe readers on the front of genuine ATMs to collect information, and install mini-cams masquerading as security cameras in order to record PIN numbers as they are entered on the ATM keypads.

Armed with this information, they can gain ready access to an individual's current account, compromise it and then withdraw large amounts of cash. In doing so, the fraudsters are striking at the very core of the victim's finances. Whereas each customer may have a number of credit cards, he or she will normally only have one debit card. Loss of funds from a current account creates a major loss of confidence – not just in that one bank, but in the whole banking system.

Banks need to act now to implement systems able to react to rapidly developing hi-tech threats.

Taking the Heat Out Of Rising Debit Card Fraud

The medium-sized banks are those most affected by the debit card fraud phenomenon. Unlike larger banks, they do not necessarily have the detection measures already in place to combat these new card attacks. Moreover, they may not have the volume of transactions to enable fraud detection models to be created based on neural network technologies.

Banks worldwide can draw on the experience of the European institutions in the late 1980s and early 1990s, where similar problems were experienced. The key to tracking fraudulent card use where smaller numbers of cards are in circulation is to install detection solutions which use sophisticated techniques such as Bayesian probability theory. These systems work effectively with smaller portfolios and provide equal, if not better, results than neural network solutions.

If banks are to fend off this major threat from debit card fraud, they must act quickly to employ the most effective and appropriate fraud detection solutions. They must ensure the fraud detection models are kept up to date on an ongoing basis because criminals will continue to look for new ways to compromise the system and perpetrate fraud to different and changing patterns. Banks must ensure that they are able to block each new fraud tactic, because if they do not, they will not only lose the confidence and trust of their customers, but also, ultimately, their competitive edge.

The Origins of Card Fraud Detection

Credit scoring, as a business practice, began as a technique for assisting in loan underwriting. Early scorecards had relatively few variables with associated scores and weights and the resultant composite scores were simply calculated. By the end of the 1980's regression modelling was firmly established as the 'natural' method of managing credit risk. At the same time card fraud had started to become a sizeable problem for banks and other card issuers. In the early 1990's card fraud was relatively unsophisticated and patterns of fraud did not change very quickly.

What made card fraud difficult to detect, however, was the sheer volume of overall transactions and the relative sparsity of fraudulent transactions. The typical method of fraud detection used at the time involved fraud managers manually reviewing lengthy print-outs of the previous day's transactions in the hope of spotting anomalies.



Neural network methods were created in the 1940's but remained in the province of academia for fifty years because of the unavailability of adequate computational power at a commercially-affordable cost. In the early 1990's pioneers such as Hecht-Nielsen began to make available proprietary general-purpose neural networks which could be used for a wide range of applications. This was possible because of the advances in price/performance of the micro-chip. Before long Hecht-Nielsen Corporation had developed proprietary neural networks built specially to model the inter-relationships between data variables related to the classes of fraud that were common at the time. Since that time the processing power of computer chips has continued to develop, but apart from being able to handle larger training sets more quickly, the underlying technology has not advanced. Hence neural network solutions for card fraud are firmly based on 1990's technology.

The Advantages of Bayesian Methods

Alaric has taken advantage of the increase in computer power to apply a much more principled statistical approach to the problem of fraud detection. Computer data storage, cpus and memory are cheap today. Consequently, when faced with a large data set, it is no longer necessary to extract a sample that approximates the behaviour of the entire population. Alaric simply takes the entire data set and loads it into a single database for analysis. This eliminates entirely any issues associated with sampling. Moreover, Alaric's Bayesian approach is deterministic as opposed to iterative - as in the case of neural networks - training a Fractals model requires a defined number of passes through the tagged historical data to produce a calibrated model, which leads to fast model calibration. Training a neural network involves an indeterminate number of passes through such data and often requires an analyst's intervention to control the process.

This means that when calculating the relative occurrence of infrequently occurring events, i.e. fraudulent transactions with particular combinations of data variables, the results are precise probabilities based on actual transaction history. It also means that the combination of variables indicative of fraud are made explicit and can be displayed on an alert screen for the user to see. The logic of the alert is transparent to the user.

Alaric has developed unique small sample statistical methods for dealing with very sparse data sets. This avoids unrealistically high scoring based on the limited occurrence of particular combinations of predictive variables. Significant events are retained within the modelling process where, with other methods, they would probably be overlooked or discarded.

The method employed by Alaric involves counting the occurrence of fraudulent transactions and calculating the frequency with which they occur. On today's computer equipment this is done very quickly indeed, which means that model re-training (or re-calibration as it is termed by Alaric) happens very rapidly and can be performed as frequently as necessary. A complete re-calibration of Fractals' strategies on a large data set takes a few hours instead of months.

The business impact of this last feature is that Fractals will pick up very quickly a shift in fraud patterns, where a neural network would not recognise such a shift for many months.

Finally, a key advantage of the Bayesian approach is that it makes immediate, incremental model adaptation feasible. As transactions are tagged by fraud analysts as being fraudulent, the underlying model can be updated immediately to reflect this new knowledge. Much higher fraud detection rates can be achieved as the model will be able to react instantly as changing fraud patterns are recognised.

Summary

Financial crime is an evolving issue driven by the creativity of the criminal mind. It is the responsibility of the banking and retail industries to continually set measures in place to detect the changing nature of card misuse. The Bayesian method, implemented by Alaric in Fractals, provides a higher probability of identifying card misuse, while having the ability dynamically to adjust to changing fraud patterns.

