CHANNEL

Volume 005 Issue No. 01

A Special Edition for the Financial Services Global Leadership Summit, 2008

Giving Wings to Opportunity

Controlling Credit Card Fraud through Predictive Analytics

The credit card industry is keenly seeking ways to control and minimize the billions of dollars lost every year due to credit card fraud. If credit card issuers could accomplish that goal, they could reap big benefits not merely by reducing losses and thus increasing revenues, but by lowering their business risks and raising both customer confidence and satisfaction. Predictive analytics is a powerful tool to help achieve that goal.

So far the trend has been to bring in customer analytics to analyze historical data after an event has occurred. This limits its value as far as effective decision making is concerned. For example, credit card issuers use customer analytics to sift through past transaction data to detect fraudulent transaction patterns. However, since the losses have already arisen, the value of that insight remains limited. Predictive analysis, on the other hand, provides intelligence in real time before the event. It can, therefore, be invaluable in the detection and prevention of credit card fraud, by allowing issuers to catch suspicious transactions before they go through, thus actually helping prevent fraud.

Predictive analysis can be invaluable in the detection and prevention of credit card fraud, by allowing issuers to catch suspicious transactions before they go through.

So far, predictive analytics in fraud detection has been constrained by issues of high costs and response times. Therefore, it has not been used in a widespread manner. Now, however, powerful computing hardware and network bandwidth are both widely available and much more affordable. Simultaneously, over the last few years, credit card fraud has been on the rise worldwide and is itself evolving, which makes detecting and preventing frauds an urgent imperative. This confluence of events implies that the time is ripe for credit card issuers to begin implementing fraud detection and prevention (FD&P) systems.

Overview of Real-time Fraud Detection and Prevention

So how does a FD&P system work? It intercepts all relevant transactions before they are approved by the card issuer's existing authorization system and passes them through algorithms that calculate a Fraud Potential Index (FPI), which is a measure of how likely the transaction is to be fraudulent. The card issuer assigns a certain weightage for each algorithm in the set, which can differ based on a broad range of parameters. Both the number of algorithms to be used and their relative weightages can be configured to suit individual card-issuers' policies. Using the FPIs returned by individual algorithms, the FD&P system computes a 'composite FPI' across all applicable algorithms, based on which it derives an action code that it sends to the existing authorization system.

The card issuer can specify different actions depending on the parameters of the transaction. For example, certain transactions can be approved, others declined and still others can be passed but marked for future declines or interventions. Such marking can be performed by amount, or incidence, or by other parameters decided by the issuer. A card issuer could choose to use proprietary or industry-standard algorithms. A good FD&P solution should come with a rich set of industry-standard algorithms along with the ability to be augmented with issuer-specific, proprietary and customized ones.

The Performance Challenge in Implementing a Real-time FD&P System

A key concern for any card issuer seeking to implement a real-time FD&P system is its impact on transaction response time. In the balancing act between satisfying customers with quick service and preventing frauds, every second counts. Since the FD&P system analyzes transactions in real time, it is imperative that the process doesn't delay the transaction too much.

Solution providers can boost the performance of an FD&P solution in three different ways. First, by executing the algorithms in parallel rather than sequentially, the total response time can be limited to that of the slowest algorithm, rather than being the aggregate of response times of all the algorithms. Second, by reducing the number of back-and-forth visits made by the FD&P system to fetch data from the existing authorization system, this overhead can be minimized. Third, by using memory resident data management techniques to improve speed.

A key concern for any card issuer seeking to implement a real-time FD&P system is its impact on transaction response time.

Apart from the above technologies, the performance challenge can be mitigated through an implementation approach of selecting only card-not-present (CNP) scenarios for implementation in the first phase. CNP scenarios such as online shopping provide the advantage that a slight increase in response time does not impact the customer experience too much since there is no "queue" of customers waiting behind. This is unlike Card Present (CP) transactions, such as in a supermarket checkout counter, where the card is physically presented and there is a queue of customers waiting. Since CNP transactions are reportedly the source of over 70 percent of credit card frauds, this implementation approach is, even otherwise, the 'low-hanging fruit'.

Configurability is Crucial

Having addressed the concerns about response time, a card issuer must next ensure that the FD&P solution it implements is highly configurable, so that it is flexible and adaptable to the issuer's needs. The issuer must be able to specify different actions or responses depending on a number of parameters such as geographic region, specific card numbers, or a range of card numbers,

the time of year, and so on. For example, the issuer can specify lenient treatment for important cardholders or can bypass certain algorithms at peak shopping seasons such as 'Black Friday' and 'Cyber Monday'. The ultimately flexible FD&P system would also provide for the option of manual override through a case management console module, which provides real-time reporting of transactions on multiple workstations simultaneously. This allows the case manager to consult the console and manually handle a selected transaction, with the option to change the system's decision to decline or authorize a transaction. The FD&P system can also be configured to involve a case manager in pre-determined situations.

Finally, issuers must consider how the FD&P module will be integrated into their existing authorization system. Naturally, issuers would like to ensure that introducing a risk reduction system like the FD&P does not jeopardize the performance of the authorization system, which is part of their basic revenue earning process. Therefore, smooth and seamless systems integration will be crucial here. A credit card issuer that can successfully implement and integrate a robust, efficient and flexible FD&P solution could lead the race in reducing frauds and reap the benefits of that large opportunity.

S Ketharaman
Program Director
Payments Practice
PrimeSourcing
i-flex solutions