# Internal control accouting system

Finance

Preface Over the past 20 years, financial institutions, governments, insurers and retailers have seen an explosion in the amount and types of fraud perpetrated against them. In the United Kingdom alone, card-fraud losses in 2006 totaled €620. 6 million ( 428 million) and while this total represented a reduction of 3 percent over 2004 and a decrease of nearly €116 million ( 80 million) over the past two years, it was still a considerable loss to business. Of particular concern is the evolution of types of fraud to circumvent the effectiveness of PIN-based domestic transactions.

This has led to a 43 percent increase in fraud committed on UK cards abroad, where perpetrators take advantage of non-PIN environments. Fraud Loss: A Cost of Doing Business? UK banks recently reported their total profits for 2006 amounted to ? 40 billion. Considering the size of this figure, it can be said that fighting card fraud is not wholly related to financial loss but rather to a significant risk to the banks' reputations. The negative press associated with the use of fraudulent card transactions to support terrorism, drugs, prostitution and human trafficking can only result in a negative customer perception.

Therefore, from a risk-management perspective, it is important to actively and effectively prevent and detect card fraud. The growth of organized crime and terrorism and their associated requirements are well documented. Their need for significant funding easily explains the inventiveness and increasing sophistication of criminal gangs and individuals in their attempts to defraud organizations of huge sums on a global scale. The manifestations of fraud are seen in money laundering.

Highlights

ID theft, internal/collusive fraud, threats to homeland security, account takeover, transactional fraud on card and checking accounts -- the list goes on and proves that countering fraud effectively requires a fast response with a multilayered approach. In addition to the prudential requirements of effective fraud loss reduction, an additional compliance driver is coming into existence.

Fraud prevention and detection, as it affects credit and debit cards and other financial transactions, is incorporated into the framework of the Single European Payments Area (SEPA). This evolving mandate will undoubtedly impose additional requirements on all European financial institutions. As a result, financial institutions will need to examine how they address this subject. Credit and Debit Card Fraud Over the last 15 years, the card industry has tended to espouse neural network (NN)-based solutions as the de facto standard for preventing and detecting fraud.

Given the prevalence of such systems and the significant associated outlay in terms of license fees and implementation costs, it has been difficult for providers of alternative systems to mount a case against incumbent NN solutions. Furthermore, the mystique woven around “ blackbox” solutions has contributed to condemning the alternatives to the periphery. But this is no longer the case. NN has drawbacks that are becoming too significant to ignore and warrant reconsideration of more effective alternatives.

Card Fraud Detection Using Business Rules A major Global 500 financial institution has been very successful using a BRMS to detect fraud. Business

rules are used to validate various conditions for detecting anomalies that can indicate fraud. The performance of the rules is high enough to provide real-time detection of anomalies based on several criteria, including multiple sources, transaction values, card-use frequency, merchant and location of the charges.

BRMS provides a user-friendly point and click environment that helps business users to create and modify fraud detection rules ” offline. ” Rules can be created, modified and tested quickly and then deployed to a production system when ready. This enables institutions to react quickly in their effort to keep pace with fraudsters. New detection policies can be activated in hours, instead of months, helping to reduce lost revenue and increase customer satisfaction.

BRMS: Flexibility, Empowerment and Ubiquity The key value of adopting BRMS to provide fraud detection capabilities lies in the flexibility that this methodology offers from an installation and a business-use perspective. BRMS offers the ability to use a common platform to address fraud issues throughout an organization, removing the need to identify different solutions and platforms to tackle credit card, debit card, check and money-laundering fraud.

In essence, a BRMS applied to the task of card fraud prevention and detection helps credit and risk personnel to interact effectively in both strategic and tactical efforts with the commercial and customer-value requirements of their organization without compromising the primary task of reducing losses to fraud. BRMS and Card Fraud Detection: The Way Forward

Advances in BRMS technology strongly suggest that BRMS-based solutions provide a viable way forward to ensure that the fundamental goals of fraud prevention and customer satisfaction are achieved as effectively as incumbent solutions but with a significantly lower cost of ownership. Any non-BRMS-based fraud prevention and detection solution that is commercially available will use rules to supplement the core detection paradigm.

Advances in BRMS technology strongly suggest that BRMS-based solutions provide a viable way forward to ensure that the fundamental goals of fraud prevention and customer satisfaction are achieved as effectively as incumbent solutions but with a significantly lower cost of ownership. To IBM ILOG, significant changes in technology and attitudes toward fraud prevention and detection for credit and debit cards help to present the BRMS approach as an extremely viable ally in the fight against card fraud. To find out more, please visit www. ibm. com