Preventing fraud in credit and debit card transactions

Look beyond packaged solutions for a holistic approach

IBM

Contents

Introduction

In economically difficult times, necessity becomes the mother of invention for fraudsters, whether organized or opportunist. Today, fraudulent activity resembles a continuously mutating virus that defies the myriad efforts to eradicate it. Opportunist, nonpattern-based fraud is increasing significantly as the global recession and fiscal downturn affect a growing number of households.

The mutation and evolution of fraudulent activity come in response to major industry initiatives, including chip and PIN, MasterCard SecureCode, Verified by Visa, token-based authentication, and, in the United Kingdom (UK) specifically, the efforts of the industry-funded Dedicated Cheque and Plastic Crime Unit (DCPCU). Experience in the UK illustrates the evolution of fraudulent activity starting during the 2006 migration to chip and PIN and the subsequent liability shift to merchants.

In 2010, counterfeit fraud in the UK dropped to £80.9MM from a high of £169.8MM in 2009—clear evidence of the paradigm shift caused by the adoption of chip and PIN technology.

Almost every other geography continues to experience change in the amount, volume and nature of fraud as fraud prevention initiatives take effect. As in the UK, Canada and Mexico have seen significant shifts in the nature of card fraud as their chip and PIN rollouts mature. As a result, fraud is now migrating from those countries to the United States, where magnetic stripe functionality in cards is easily compromised. Another manifestation can be seen through the explosive growth in the availability of banking services to many more Chinese citizens, which is generating previously unseen levels of fraud in that country as well.

This white paper examines some of the most important issues facing the global card industry's war on fraud and its perpetrators. It is designed to generate awareness and discussion around the wealth of knowledge and technology that can now be integrated to provide enhanced transactional fraud detection. It also recommends strategic and operational changes that should be made to ensure the effective, optimal overlay of industry and domain knowledge with relevant strategies, technology and methodologies. This includes the need to integrate effective detection, decision and monitoring paradigms such as business rule management systems (BRMS) to enable the execution of a holistic and integrated fraud detection strategy.

The growth in mobile funds transfer providers and person-to-person (P2P) payments bring new opportunities for fraudsters too. The most recent figures published in 2011 by the UK Cards Association (UKCA) point to an overall reduction in fraud losses and to the significant changes in the nature of fraud perpetrated. UKCA reported that total card fraud losses in 2010 fell by 28 percent to £440.3MM compared to the previous year—an unprecedented reduction of £170MM. In addition:

- Counterfeit fell by 52 percent.
- Mail-not-received (MNR) decreased by 32 percent.
- Card-not-present (CNP) was down by 19 percent.
- UK domestic fraud dropped 16 percent.
- Fraud committed overseas was down by 47 percent.

While UK credit and debit card usage exhibits significant, country-specific traits, other countries can achieve similar fraud loss reduction by deploying more effective combinations of strategy, technology and knowledge, and adopting industry best practices.

Significant reductions in fraud losses bring the dangerous view that the battle may be over. The achievement may be used as an opportunity to justify reducing investments and shifting focus away from ongoing efforts to further reduce card fraud. Under no circumstances should this be allowed to happen.

Instead of reducing fraud detection efforts, fraud strategy professionals recommend remaining guarded. In fact, countries targeted by migratory fraudsters (that as yet have not experienced a particular type of fraud) are often not as well prepared to evade threats. The antifraud measures they need are simply not yet in place. Preparedness is critical. In any country, an ostrich-like approach is not effective.

Fraud losses—an acceptable cost of doing business?

The public spotlight under which banks and card issuers operate is significant, and financial institutions not only struggle to mitigate financial losses, but also any damage to public perceptions and reputation. Mitigating brand and reputational risk are key drivers for continued vigilance and effective detection efforts. In addition, banks and card issuers also struggle with declines or challenges to legitimate transactions that damage customer confidence and loyalty. From a risk-management perspective, a customer-impact perspective and a brand-value perspective, the obligation to actively and effectively prevent and detect card fraud is absolute.

Yet all businesses—whether financial or otherwise—are facing a grim reality: the insidious growth of organized crime and terrorism and their need for significant funding has underpinned the ingenuity and increasing sophistication of criminals in their

attempts to defraud organizations of significant sums worldwide. Manifestations of fraud are seen in money laundering, ID theft, internal/collusive fraud, account takeovers and transactional fraud on cards and checking accounts.

Effectively countering fraud requires a swift response based on an effective, coherent, multilayered approach.

The need to reduce fraud losses is also driven by compliance. For example in Europe, fraud prevention and detection for credit and debit cards and other financial transactions is mandated in the Single European Payments Area (SEPA). This evolving mandate imposes additional requirements on all European financial institutions and instruments. Yet industry operators want to know how to mitigate the costs associated with compliance projects and derive business benefits by leveraging these requirements.

Clearly, agility and flexibility are key to achieving potential benefits, and these capabilities may not be available or accessible through existing, packaged detection solutions. Regulations are a fact of life, and it is incumbent on businesses to find ways of turning regulatory overhead into commercial advantage. The possibility that SEPA may be replicated in southern Africa only endorses the point.

The challenge is to reduce compliance costs without compromising the quality of the deliverable. That said, compromising the "deliverable," in this case effective fraud detection, will lead to significant increases in attempted and actual fraudulent activity.

Credit and debit card fraud detection: Challenging the status quo

Over the past 20 years, the card industry worldwide has continued to espouse neural network (NN)-based solutions as the gold standard for preventing and detecting transactional fraud. Given the prevalence of such systems and the significant outlay for implementation costs and ongoing licensing and maintenance fees, it has been difficult for providers of alternative systems to make a strong case for consideration against incumbent NN solutions. The mystique woven around a "black-box" solution had condemned alternatives to the periphery. In addition, organizations are hesitant to consider component-based capabilities for fear of having to modify incumbent operational strategies and workflow dictated by NN solutions.

However, outdated attitudes are changing as global card schemes and issuers begin to actively explore and implement best-of-breed components. The results will be manifested in new or enhanced capabilities or functionality within an incumbent detection system. One of the prime reasons for this shift in thinking is increased knowledge within the fraud detection community, which mandates the requirement for enhanced, configurable capabilities to address specific nuances of a card portfolio

and its users. Packaged solutions are not always best equipped to respect and respond to such requirements, much less to respect operational differences that must be accommodated to maintain effective detection strategies.

Another major consideration is the potential capital outlay associated with the acquisition of a NN-based or other, packaged solution. It is difficult for small- and medium-sized issuers to make a business case against the high cost of acquisition and ongoing maintenance. This can also be true for major issuers. The high cost of replacement is leading issuers to look to enhance or complement existing capabilities or to investigate the powerful, hosted offerings that are available. "Rip and replace" is rarely an option. Just as fraud itself evolves, the means, methods and strategies for detection have evolved to adapt to changes in budget and investment availability. In itself, this is significant enough to reconsider alternative ways of maintaining or improving detection capabilities.

Neural networks and packaged solutions: Time for change

Organizations can no longer overlook the value of a modular approach to transactional fraud detection. Significant enhancements and changes in algorithmic technology, processor technology and the effectiveness of detection paradigms, and the ability to implement these paradigms as individual components, can yield both cost savings and detection benefits.

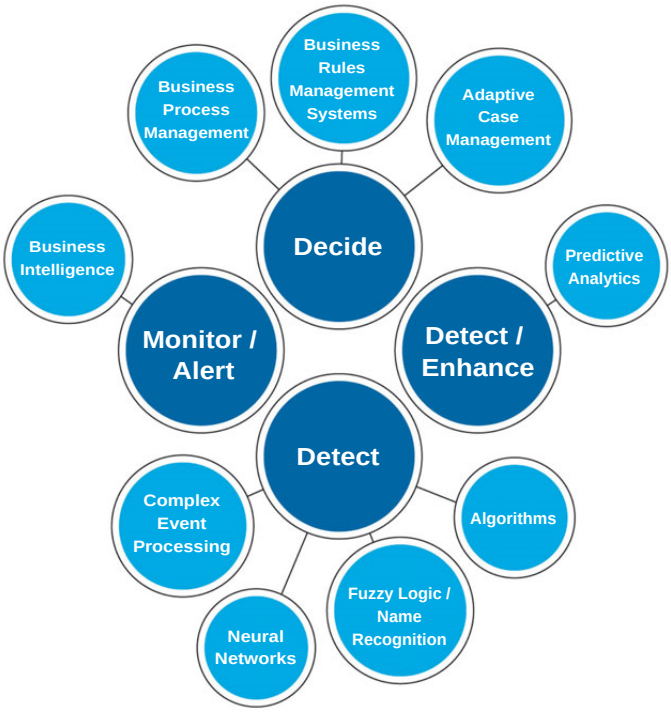
Increasingly, organizations are considering the value of acquiring best-of-breed components to enhance existing capabilities. Following are some drivers for change or enhancements to existing functionality:

- Inability to trust the score of a NN-based solution that may use a model that does not represent the cardholder base or demographics.
- The high cost and limited availability of appropriately trained, geographically and demographically relevant NN models.
- Customer retention and loyalty that is impacted by high false positive rates (FPRs) and wrongly declined transactions. This consideration appears to drive a growing number of commercial decisions, which compromises prudential risk management. The provision of viable FPRs is a pre-requisite. NN technology does not provide adequate certainty around false positives.
- The threat of fraud-associated reputational risk to the organization.
- NN models cannot be adapted swiftly to significant behavioral changes (as was experienced when chip/ PIN cards were introduced).
- Adding business rules to supplement NN-Models to detect new forms of fraud, such flash frauds and evolving scams e.g. multiple test transactions at an online store to validate a cloned card's details, followed by high-value fraudulent transactions at jewelry stores in different countries.
- Transposition of a NN-model from credit card fraud detection to a debit card or an anti money-laundering environment is not feasible, and vice versa.

This does not mean existing solutions are completely ineffective, but paradigms and components are evolving and improving to allow integration with existing capabilities. Deploying new assets is critical to maintaining effective prevention and detection capabilities.

Card Fraud Detection Component Paradigms

Card Fraud Detection Component Paradigms include but are not limited to:



Seek technologies that enable business flexibility

A business rule management system (BRMS) is an example of a technology that provides both ease of installation and business-use flexibility. BRMS delivers a common platform to address fraud issues across an organization, removing the need to identify different solutions and platforms to tackle credit card, debit card, check and money-laundering fraud. Organizations can integrate this best-of-breed capability with complex event processing and adaptive case management to improve detection capabilities, productivity and customer satisfaction.

Fraud and risk managers are increasingly caught between the demands of reducing losses to fraud and balancing the requirements of customer value management and marketing. With FPR a significant driver of fraud detection operations, it is vital that a solution offers realistic FPR values that enable updates to the fraud prevention and detection strategy as well as performance monitoring. BRMS offers the ability to make better decisions on appropriate FPR and mitigate negative customer experiences with significantly lower implementation and running costs than a NN-solution—a compelling argument for the re-evaluation of the systems deployed today.

Using BRMS as a major component of a fraud prevention and detection solution affords:

- Superior transparency and understanding of processes
- In-house control of detection targets
- Significant flexibility to respond quickly to evolving fraud types

- A noncomplex migration path to allow parallel existence and integration with incumbent solutions
- Business users complete control of strategic and tactical decisions
- The ability to implement rules that reflect risk and commercial business drivers

In essence, using a BRMS as a solution component for card fraud prevention and detection allows credit and risk personnel to interact effectively in both strategic and tactical efforts with the commercial and customer-value requirements of their organization while staying focused on reducing fraud losses.

Look beyond packaged solutions

Fraud detection practitioners and strategists need to look beyond the capabilities provided by packaged solutions. By partnering with an expert consultant, organizations may confirm that existing software capabilities and associated operational practices are adequate. If not, a consultant can also provide an effective review and recommendations for operational enhancement. Enhancement efforts should complement existing capabilities, and existing budgetary constraints, while providing a nondisruptive path to improved detection and prevention.

The fraud detection industry must develop an understanding of the enhanced capabilities provided by predictive analytics, pattern and name matching/recognition, complex event processing, business rules, content analytics and, most importantly, the means to implement such paradigms.

IBM and its broad partner ecosystem are uniquely positioned to assist institutions embarking on the journey described above and stand ready to engage with those who understand that challenging the status quo is not a bad thing.

Conclusion

The fight against fraud is continuous and evolves at a rapid pace, with the sophistication of fraudulent attacks ever increasing. New and more effective ways to monitor and detect fraud allow issuers and institutions to better position themselves for success. IBM and its partners stand ready to assist with strategy development aligned to technological capability to position your organization for success in its ongoing fraud prevention efforts.

For more information

For more information about fraud detection solutions from IBM, contact your IBM representative or IBM Business Partner, or visit ibm.com

Email the author, Richard Collard at richard.collard@uk.ibm.com

For more information about fraud in the United Kingdom, visit the UK Cards Association at theukcardsassociation.org.uk

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

About the author

Richard Collard
IBM Worldwide Subject Matter Expert
Transactional Fraud Detection, AML & Risk Management

Richard Collard comes to IBM as part of the 2009 acquisition of ILOG. He draws on a business-based career with major global fraud analytics organizations and specializes in the provision of fraud detection solutions and consulting for credit and debit card issuers and for AML. Prior to joining ILOG, he worked to develop a radical, new approach to rules-based fraud detection through the automated generation of rules using genetic algorithms and evolutionary computing techniques. This technique is holistic and nonprescriptive, espousing the belief that there is no such thing as a "one-size-fits-all solution," and is aligned with IBM's modular approach to the challenges facing the card industry.

Richard's operational reviews for card issuers in South Africa have generated significant savings and operational efficiencies. They have also been instrumental in the recent adoption of business rules management systems (BRMS) technology as a major component of a hosted fraud detection solution. Richard's ability to draw on global experience allows significant knowledge transfer of global best practices. His approach is consultative and respectful of geography and culture, ensuring that the thought leadership that he provides is positively received—traits that have earned him significant respect through his engagements.

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
June 2011

WSW14166-USEN-00