

by Alaric Systems Ltd.
& Stratus Technologies

Real-time, All the Time

Is this the future for Fraud Risk Management
across the payments industry?



Advances in payment methods increase opportunity for fraud in cards and retail banking

Growth and change in card payments

The payments industry strives continuously to offer new and more convenient payment methods to consumers and merchants. Cards have replaced cash and checks to a great extent, but not all consumers have access to plastic and not all merchants want to give up part of their turnover in merchant service charges. In August 2007, for example, UK merchants won a battle to prevent MasterCard from increasing debit card merchant service charges (MSCs) from fixed fees per transaction to percentage-based calculations.

Prepaid cards. With increased competition and tighter margins, all players are trying to find ways to maximize their share of the payment value chain. Merchants issue closed-loop prepaid cards. These can be loaded with funds from a variety of third-party sources, but their value can only be used in the merchant's own group of stores. They can also be safely issued to customer groups who are unable to obtain credit cards or other forms of credit; offering a risk-free way to attract new business. This keeps consumer spending in the merchant's own back yard and eliminates MSCs. To address the same market segments, the card associations have introduced open-loop prepaid cards that may be used at any retail outlet, and ATMs. In each case, the prepaid model reduces issuers' credit risk and broadens the appeal of their branded products.

Contactless cards. Although cards have made little impression on low value payments, where cash is still preferred for speed and convenience, debit card use has increased. Now contactless cards are bidding to gain a greater share of traditional cash payments and overcome merchant objections to delays at point of service.

Mobile payments. Mobile phone companies are exploiting their communications skills and ubiquity to deliver low value payment services – first for their own products and, most recently, to third party, general retailers. The mobile phone is now a candidate to join RFID-enabled plastic cards and keychain fob devices, all of which can be used for contactless payments.

Exploiting multiple products in the card fraud value chain

Pre-paid cards have become a popular vehicle for fraud. The largest ever mass theft of credit card data to date was uncovered in March 2007 when it was discovered that hackers had accessed the processing systems of discount retailer TJX. The personal information of an estimated 45.7 million cardholders was compromised. Following the theft, a Florida fraud gang was caught using the stolen data to create tens of thousands of counterfeit credit cards. These were used to purchase and load US pre-paid store cards. These could then be sold or traded on Internet swap sites to realize their cash value. This last mechanism combines the ultimate act of theft (of the retailer's money or goods) with an act of Money Laundering to hide the original hackers' and fraudsters' tracks.

Growth and change in retail banking payments

Faster Payments. The style and speed of bank payments is also changing. Consumers have become accustomed to accessing their accounts online over the Internet and already some banks permit customers to initiate electronic payments, both instant and future-dated. In Europe, the Single European Payments Area ('SEPA') creates new rules and service levels for inter-bank payments. Regulators and legislators have reacted to public demand for more

T.J.Maxx Fraud Ring Leader Gets Five Years in Prison

*The 18-year-old who
pleaded guilty in March
was also ordered to pay
nearly \$600,000
in restitution*

*InformationWeek
September 14, 2007*

responsive and less costly banking services by introducing the Payment Services Directive, which mandates that consumers should be able to initiate real time payments both nationally and cross-border with a maximum settlement time of 'B+1', which means no later than the end of the next business day.

For national payments, this turnaround time may be even shorter. In the UK, from Spring 2008, consumer-initiated inter-bank transfers ('Faster Payments') may be delivered in real time in as little as 15 seconds, and these transactions will be irrevocable. For fraudsters exploiting security data stolen in 'phishing' attacks, these new payment channels offer fraudsters opportunities to steal the customer's funds and then use the payments network itself to money launder the proceeds of their crime.

To protect themselves and their clients, banks will have to secure the new payment channels with anti-fraud software and make real time Anti-Money Laundering checks before the funds are transmitted, otherwise they would be in breach of AML legislation. New business requirements like this will make a big impact on back office systems that historically have only supported batched-based reporting and manual review processes.

Increased diversity in banking service delivery channels

Meanwhile, banks – the custodians of most of our cash - are offering their customers new and more convenient ways to manage funds. Telephone banking, Internet banking and Mobile banking have been added to traditional branch service delivery. In each case the goal is to deliver information and payment services as quickly as possible. And, every time a new delivery channel or payment service is made available, it has to be secured with encryption, usernames, passwords and PINs. This means more identity information that must be remembered, recorded and stored, compounding the already large amounts of data with the potential for compromise.

Fraudsters know their real financial opportunities lie in consumer and business bank accounts, where the combination of compromised access security data and on-line electronic payments offers them instant access to funds. Stolen electronic money, like ATM cash, delivers 100 cents on the dollar, a much higher return than stolen goods that must be resold at highly-reduced prices.

Phishing attacks have grown exponentially over the last several years. Millions of spam emails are delivered every day. Although many are blocked by spam filters, it is inevitable that the best-designed emails can still get through and deceive unwary recipients. Even a small number of consumers tricked into compromising their bank account details and passwords can generate millions in losses and the effect on these individuals is traumatic. In some countries, liability for losses resides with the victims, because laws and regulations requiring refund of stolen money from credit or debit cards do not cover retail bank accounts. In 2006 two UK banks announced that they were not obliged to refund their customers' stolen funds if it was discovered that the customer had given away their own secret data. It is much more likely however, that a customer's details will be compromised by organized hacking attacks or the action of bribed, threatened or criminal insiders who have direct online access to customer records.

In the absence of universal, proven biometric identification methods institutions have to admit that new ways must be found to secure customer transactions. European banks are now looking at two-factor authentication devices that generate one-time passwords to secure online banking access. The device illustrated only works with the issuer's own cards, which means

A typical two-factor authorization device for on-line banking access security



**Alaric Systems Ltd.
Stratus Technologies**

multiple card owners might require more than one device. Already other issuers are proposing ‘out-of-band’ password generation – by mobile phone for example – to avoid the need for bulky physical devices.

With every new payment device or service, comes potential security weaknesses – and now compliance requirements

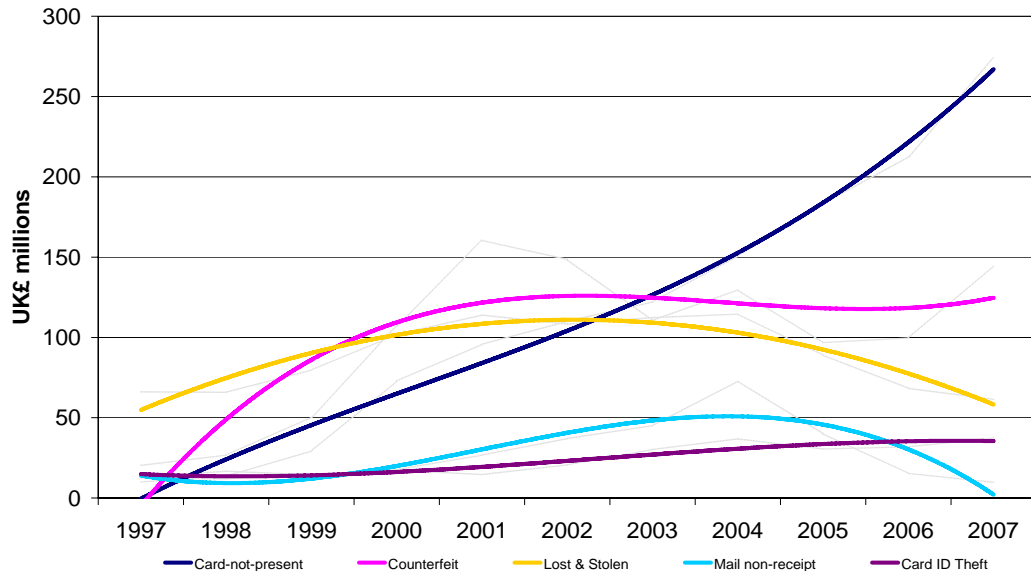
Thieves and fraudsters work diligently to find the weak points in payment systems and to compromise the security of cash locations. Once the hidden keys to these locked doors are found, everything behind them stands to be lost. The vulnerabilities of magstripe cards secured by signature were quickly overcome by counterfeiters who used electronic skimming, combined with cameras, to effectively bypass magstripe and PIN at the ATM. Card security has been found wanting especially for non face-to-face transactions and card-not-present (CNP) is now the largest card fraud category. Even the outstanding success of Chip & PIN in Europe and Asia – which decimated lost & stolen fraud and leveled off the growth in counterfeit –spawned a backlash in cross-border ATM fraud. This was partly due to the growth of Chip & PIN POS terminals around the world, which offered criminals literally hundreds of thousands of new potential points of compromise for magstripe skimming and PIN capture.

Building the defenses: strategies for fraud avoidance, detection and prevention

Fraud deterrence and avoidance: the cards industry defends itself

In order to increase card security and reduce fraud losses, the latest methods in card verification and authentication need to be implemented globally. The global rollout of Chip and PIN, particularly in Europe and Asia, has been deemed to have been successful in reducing fraud in card present transactions, but has resulted in displacement to CNP fraud where the physical prevention devices are ineffective. A combination of new security measures will be needed to deliver protection from fraud in many, different payment channels. This will entail multiple preventative strategies.

Figure 1: UK Card Not Present Fraud Soars After Chip & PIN Rollout



The most recent development in Europe, intended to secure both e-commerce and online banking access, is two-factor authentication. One example is the Chip Authentication Program

(CAP), which uses a portable card reader that interfaces to the Chip & PIN application on an EMV card to create a one time password unique to each transaction. As of summer 2007, two UK pilot programs are already under way using card-based schemes. Scheme monitoring will soon reveal if consumers find carrying and operating an additional physical device an acceptable trade-off for increased access security for Internet banking and online purchases.

Other controls developed to oppose card not present fraud (CNP) include Card Verification (CVV2/CVC2) and the Address Verification Service (AVS). These have had some success, but are not universally implemented. Thus CNP fraud continues to escalate. Visa and MasterCard offer 3D-secure authentication such as 'Verified by Visa' and 'SecureCode' as optional, additional security for e-commerce transactions. Unfortunately, although uptake by e-merchants is at 30% in UK (spurred by liability shift in favour of compliant merchants) consumers have been much less enthusiastic, put off by the inconvenience of registration and another password to remember. Increasingly, merchants have begun to implement their own risk-monitoring tools to recognize fraud indicators like high risk IP addresses or suspicious patterns of product ordering. Although primarily aimed at e-commerce applications (eBay specifically), PayPal is an example of sidestepping the card fraud problem altogether by providing a secure means of payment via a third party payments scheme that does not require direct entry of card details online. Even so, conventional cards may be used to prepay and top up PayPal accounts.

Best practice in Data Protection: removing compromise opportunities

Mass data compromise has become more prevalent as fraudsters look for maximum return on their attacks and we have seen a number of highly publicized examples of this in the past year in the US and Europe. This situation has been addressed by the introduction of comprehensive requirements for enhancing payment account data security. Payment Card Industry Data Security Standards (PCI DSS) have been developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. The standard applies to all organizations that handle payment transaction data including all processors, issuers, acquirers, merchants and payment application vendors. It restricts the retention of magnetic stripe data, CVV2/CVC2 and PIN information.

Phishing, identity theft, account compromise and insider fraud

Risk managers must not focus entirely on external threats as insider fraud is surprisingly common and can be equally damaging. Increased staff access to technology, organized crime and inadequate employee screening practices are the main contributors to employee fraud. Reports have shown that over 80% of financial institutions in the US and UK have been affected by employee fraud, while 65% see the threat becoming more serious in the future.

The technologies enabling new payments channels are also empowering the fraudsters with the means to source and auction consumer information to perpetrate payment fraud. Attacks on consumers range from identity theft to lost and stolen cards to the production of counterfeit cards. With the introduction of advanced data capture techniques such as phishing, pharming and man in the middle, these consumer-focused tactics have migrated into large-scale attacks on banks, processors and merchants. The aftermath results in mass data compromise, with ramifications that include increases in card fraud in weaker, more easily exploitable markets.

Identity Theft is best stopped at source.

Industry best practice is embodied in the card associations' guidance for protection of sensitive cardholder data: PCI DSS.

**Alaric Systems Ltd.
Stratus Technologies**

With the criminal gangs becoming smarter, card security and risk controls must be continually enhanced to stave off persistent attacks to breach systems. This should be a multifaceted approach combining proactive organizational vision, flexible fraud detection solutions, compliance with regulatory guidelines and a drive to heighten consumer awareness. Fraudsters will alter their behavior to avoid establishing fraud patterns that can be detected by automated card transaction analysis systems. This highlights the importance of having a readily adaptable fraud detection solution which can incorporate evolving fraud patterns and customer profiling strategies to identify transaction anomalies.

Real time transaction monitoring: today

Real time card fraud detection is essential for most large issuing institutions. Improvements to payment services, such as the planned introduction of Faster Payments in the UK, will reduce clearing times on electronic payments between banks from days to seconds. This requires a wide new range of transactions to be processed in real time, a change that necessitates enhancement or replacement of legacy payment applications. The need to comply with draconian Anti-Money Laundering regulations places an onerous burden on the payer's institution, which, by law, must avoid emitting transactions that appear to be suspicious. The service level agreements for Faster Payments will leave very little time for fraudulent or suspicious transfers to be intercepted and blocked. It follows that if those transactions are customer-initiated in real time, they must be risk-scored in real time and queued for review by fraud and/or compliance officers before the transaction continues to completion. Suspicious transactions will be blocked and vetted transactions re-submitted. Suddenly fraud case management systems must assume the role of a transaction referral application.

To achieve real time fraud detection it is necessary for the fraud scoring engine and the institution's card authorization system to be intimately integrated, so that the fraud scoring engine sees and processes transactions as they appear, on-the-fly in real time. Historically, real time fraud risk management has been the expensive option, applied only to 7-10% of transactions deemed to be at the highest risk. To deter today's dramatic increases in fraud, a vastly larger number of critical transactions may need to be monitored. This will place a premium on ultra-high performance systems (software and hardware) that can return decisions to the requesting authorization system in the millisecond range, scale to match transaction volume growth, and deliver flawless 24 * 365 service.

Fraud patterns in card transactions are well understood and occur in volumes that make statistical analysis viable for automated decisioning. However, cards are a highly specific silo in the banking business. Therefore the banks will need to build a holistic view of behavior on customer accounts and transfers to identify and alert suspicious patterns and intercept fraud in real time.

The Chief Risk Officer: role and responsibility for the group head of fraud and risk

Here we can see clearly just how far the goalposts have moved for fraud professionals in the institutions.

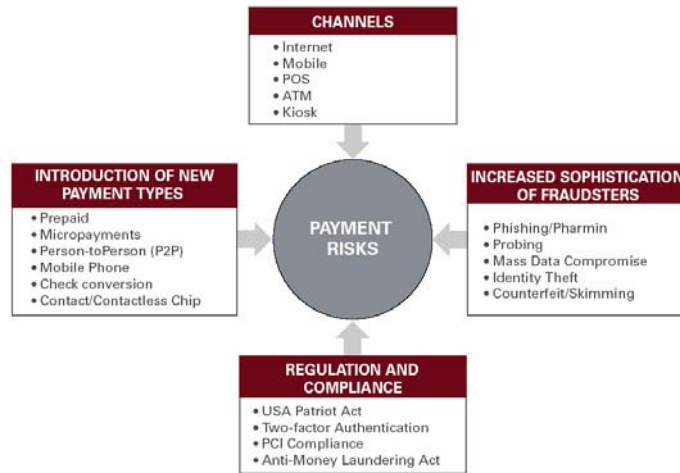
From an organizational perspective, Risk Managers now have a far more diverse and broad role and must be knowledgeable in not only fraud risk, but also technology, legal and regulatory issues and product variations. With expanding payments channels and products, they must be proactive in assessing threats prior to market adoption in order to remain ahead of the fraudsters. This is likely to involve developing a more holistic, enterprise-wide view of the

Real time processing will quickly progress from the luxury option of today to become the normal mode of transaction monitoring in the future.

organization's payments landscape. There is a necessity to expand the profiling capabilities by integrating multiple payment data streams. This will enable a customer account transactional view (card transactions, standing orders, direct debits, savings accounts, etc.) rather than purely card-based transactional monitoring. The implementation of an enterprise-wide payments view requires flexible system integration and message transformation in order to easily access data in the respective application silos.

The goalposts have moved a long way in a short time for risk management professionals. Fraud and compliance issues have attracted the attention of C-level management due to the reputational fallout of fraud cases

Figure 2: Payment Risks Have Increased



Source: Edgar, Dunn, & Company

Organizing for effective response and holistic fraud risk management

Consider a full-service retail bank that is a credit and debit card issuer and offers a full range of current (DDA) and savings accounts. How will the newly-appointed Chief Risk Officer implement a plan to cover all areas of payment risk and ensure regulatory compliance in databases and systems?

With the continuous development of new payment channels, the historical methods of detecting fraud by monitoring single-payment channels in isolation are giving way to methodologies that can monitor ALL of the channels through which transactions can occur on an underlying account. The new approach combines traditional card payment fraud analysis with other types of risk analysis, such as Anti-Money Laundering and Insider Fraud, all of which manifest themselves in unusual patterns of activity on the underlying accounts.

Here are some new items for a Chief Risk Officer's To Do list as an institution moves towards a holistic, real time fraud and compliance strategy:

Comprehensive account view. Gain a holistic view of account activity with the primary account or possibly the customer as the monitored risk entity. This presupposes an understanding of complex customer account relationships that may not be evident elsewhere in the bank

Transaction and event tracking. Track not only significant transaction activity, but also a range of account events such as address changes, account open dates, password changes and the relative timing of these events

Transaction profiling. Profile transaction activity over time and be able to monitor and review transaction patterns

Delivery channel monitoring. Monitor delivery channels as risk entities in their own right, including relevant parameters such as IP addresses, Calling Line IDs and password attempts

Payments handing. Score and – according to risk thresholds – intercept, queue and manually approve on-line, real time payments

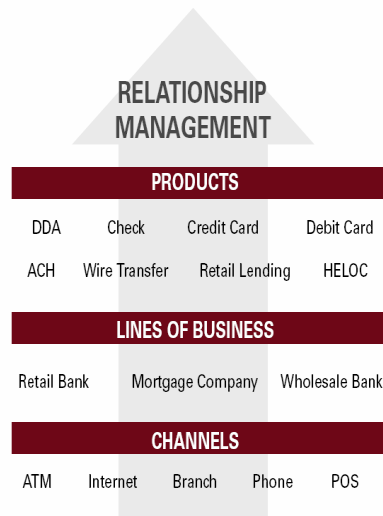
Recurring and future-dated payments. Track future-dated and recurring payments with the same importance and urgency formerly used only for card transactions.

These requirements are clearly beyond the capabilities of conventional card fraud detection systems which are optimized to process one transaction stream and only single-ended payments. AML systems process a wider variety of payments, but most are not a viable way forward to real time processing because they only offer manual alert reviews or at best daily batch reporting.

Empowering the real time, fraud-risk professional: the right tools for the job

Alaric specializes in innovative applications for the payments industry. Its family of products is designed to meet the requirements above for more sophisticated and effective approaches to fraud detection and prevention.

Figure 3: Holistic Approach to Relationship Management



Source: Edgar, Dunn, & Company

Alaric's Fractals fraud risk management solution set

The Fractals fraud detection system is a modular, scalable and real time solution that can grow with your business. The ideal platform for a holistic view of account activity, Fractals is flexible enough to provide monitoring and detection for the wide variety of payment channels

in use today. In combination, the powerful rule builder and the use of statistical modeling methods allow users to benefit from much faster model training times than traditional techniques. Fractals models deliver industry-leading detection results with low false-positive ratios that maximize the efficiency and effectiveness of the fraud team.

User Rules: on-line configuration of rules strategies

Fractals powerful User Rules capture expert knowledge, enabling users to build sophisticated rules for profiling account behavior and providing extremely accurate warnings of unusual activity patterns. Rules can be created easily through a ‘point-and-click’ graphical user interface specifically designed for end users. This eliminates any need to code rules in SQL or some form of pseudo programming language, making it the ideal tool for business experts to leverage their knowledge base quickly and effectively.

Traditionally, card-centric fraud systems offer a range of transaction parameters plus a selection of customer and account information to rule writers. In an enterprise environment, with more complex transactions and multiple delivery channels, users need a much broader range of information to work with. For example, the rise in account takeover frauds, including those perpetrated with insider assistance, drives the need for a solution that adds yet another level of protection. Fractals enables financial institutions to use non-financial data (for example, call center operator, branch teller and e-commerce system audit logs) to identify unusual patterns of account activity in advance of frauds.

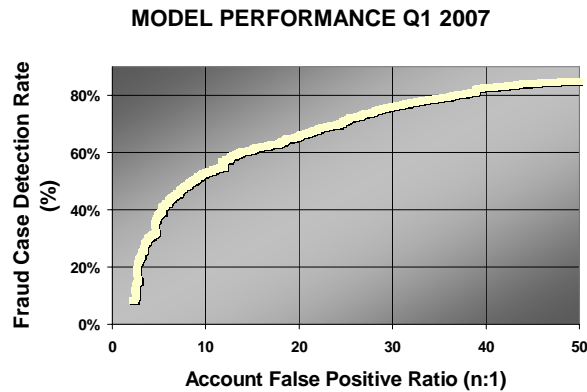
Fractals combines the additional non-financial information with the transactional data to identify internal points of compromise on accounts that may be at risk. For example an address change in close proximity to a credit limit increase might be a predictable fraud attempt as might the request for issue of a replacement card or check books.

Monitoring all of the transactions and events affecting a customer account provides users with additional profiling capabilities and allows for early notification of suspicious activity. It also enables a more sophisticated approach to proactive fraud prevention. Resources are targeted to respond to alerted activities instead of "second guessing" the areas where problems might occur. The flexible and powerful rules component of Fractals allows financial institutions to create effective monitoring rules for alerting of unusual activity. This is achieved by profiling activity from the audit logs and alerting fraud professionals when unusual patterns of non-financial transactions occur.

Adaptive Classification Engine: intelligent, probabilistic fraud scoring

The Adaptive Classification Engine (ACE) is the intelligent detection component of Fractals. It generates fraud alerts by executing mathematical models against incoming transactions to produce a fraud score or “probability of fraud”. ACE is calibrated using a dataset that contains a customer’s historical transactions, enabling ACE to rapidly detect fraud patterns present in new data. To implement the calibration, the customer provides several months of recent transaction data, with frauds tagged. In runtime, the ACE assesses each incoming transaction against these profiles to ascertain the risk posed by an individual transaction in light of profiled historic fraud as well as known customer behavior for that account. As a result, the ACE generates low false positive values and is an extremely effective and efficient mechanism for identifying compromised transactions.

Figure 5: Mathematical Modeling for Fraud Probability



Alaric’s use of Bayesian statistical techniques means that users benefit from much shorter model build times and faster tactical response to rapidly changing fraud patterns than traditional neural techniques where models can only be updated annually.

Fraud Analyst Workbench

Fractals provides fraud analysts with a powerful, browser-based user interface for processing alerts and reviewing cases. Analysts can work their own queues of alerts and interrogate transaction history and statistics so that they can fully understand cardholder and merchant patterns of behavior when analyzing each alert. This data is available at the click of a mouse so that they can quickly determine what problem has been identified and take the appropriate corrective action.

Alert prioritization and queuing

The Fractals Rule Engine and ACE generate alerts and fraud team managers can configure user and queue definitions to route alerts according to urgency and importance. Fractals implements the concept of an alert group which is a way of grouping alerts that meet common selection criteria, such as fraud scores, transactions locations, product types or transaction amounts.

Figure 5: Alert Generation

Merchant ID	Value	Group Value	Rule Code	Updated By	Updated On
950346028	40%		MAA01	MRA	01/01/2005 12:05:00
950346058	2000%		MAA01	MRA	01/01/2005 12:05:00
950346058		CHF 789	MTA07	MRA	01/01/2005 12:05:00
95034104		57%	MAA01	ADMIN	01/01/2005 12:05:00
95034104		45%	MAA02	ADMIN	01/01/2005 12:05:00
95034104		250%	MAA39	ADMIN	01/01/2005 12:05:00
950346029		CHF 789	MTA07	ADMIN	01/01/2005 12:05:00
950344846		57%	MAA01	ADMIN	01/01/2005 12:05:00
950344846		45%	MAA02	ADMIN	01/01/2005 12:05:00
950344846		250%	MAA39	ADMIN	01/01/2005 12:05:00
950346098		CHF 789	MTA07	ADMIN	01/01/2005 12:05:00
950360111	200%		MAA01	ADMIN	01/01/2005 12:05:00
950360111	80%		MAA02	MRA	01/01/2005 12:05:00

If necessary, alerts can be routed to designated specialist staff for action based on the nature of the originating transaction or fraud that has been identified. Each analyst has his or her own alert queue but an alert queue can be linked to multiple alert groups to provide a high degree of configurability in meeting operational requirements.

Authentic Gateway: taking the pain out of payment application integration

Fractals is designed to run as a real time system and is sufficiently scalable and efficient to allow organizations to monitor all of their transactions in real time. This is a vast improvement over monitoring a limited sub-set (typically 10%) of transactions in real time, which has been the norm with older, slower fraud applications. Because it is possible to integrate Fractals into the real time transaction path and potentially score all transactions, it is more likely that it will intercept fraudulent or suspicious payments. This means that users will derive maximum fraud loss savings from Fractals' monitoring capabilities.

Having a high performance fraud monitoring system is only part of the story. The ideal solution needs to integrate tightly with authorization systems and payment hubs.

Accomplishing such tight integration is a lengthy, expensive process for other vendors and over the years, many projects have failed because the cost of systems integration exceeded the cost of the fraud-monitoring system itself. As a result anticipated fraud loss savings were immediately negated.

Alaric's Authentic Gateway is designed to meet the need for a comprehensive and flexible integration tool which can be used to transform messages effectively and efficiently. Otherwise well-recognized vendors follow the traditional approach of hand coding each interface to their systems. In contrast, Alaric's Authentic Gateway offers an innovative, point & click GUI-based configuration process that enables interfaces between Fractals and multiple legacy systems to be set up quickly and subsequently managed at low cost. Indeed, for those institutions moving towards a Service-oriented Architecture, the combination of Authentic Gateway and Fractals enables fraud monitoring to be presented as a Web Service to the institution's other applications. This is another significant advantage of the Fractals solution.

Authentic Gateway reduces the complexity of integrating Fractals into existing environments and also allows acquirers, issuers and processors to introduce new delivery channels and support future payment product lines with minimal impact on legacy payment applications.

Robust, scalable and high performance: the new paradigm for fraud risk-management solutions

Traditionally, fraud detection systems have been just that, systems that can detect fraud after the event. They have not been part of the critical transaction path and have not been subject to the same service level requirements that are now standard for payment systems. The new generation of anti-fraud systems, such as Fractals, must work at the same pace as the payments systems they are helping to protect – addressing hundreds of transactions per second at the same levels of availability that customers have come to expect from EFT systems. Because they are essentially fraud-prevention systems that must interrupt high-risk transactions within the critical path, they require flawless 24/7 operation every day of the year. Fraud detection systems also place higher demands on the hardware than orthodox payment switching systems because they perform a lot of analysis and computation work on each transaction processed.

The Stratus® fault-tolerant ftServer® family provides a robust continuously available platform that is ideal for the Alaric Fractals fraud detection system.

Every Stratus system delivers five nines (99.999%) and greater uptime to Microsoft® Windows® or Red Hat® Enterprise Linux® environments. Powered by Intel® Xeon® multi-core processors, ftServer systems are engineered to effortlessly handle data- and network-intensive workloads and are ideal for enterprises that want to capitalise on the efficiencies and cost savings offered by industry-standard solutions.

Stratus ftServer-based solutions eliminate the complexities of cluster deployment and its ongoing maintenance headaches. Unlike a cluster that is designed to quickly recover from a failure, the ftServer system is designed not to fail in the first place. There is no need for failover scripting, repeated testing or need to make your application cluster-aware. All of the advantages of Stratus' Continuous Processing technology® are automatic and immediate.

Stratus ActiveService™ architecture, built into every ftServer system, combines automatic fault detection and isolation with integrated call-home remote support and online component replacement.

Combined, Stratus availability features ensure a level of reliability, ease of use, and built-in serviceability for the Fractal fraud detection solution that other vendors simply can't match.

About Alaric International

Headquartered in London and with international offices in the U.S. and Australia, Alaric is a leading supplier of advanced technology payments based products and services. Alaric offers solutions for both SOA-based and conventional payments systems integration, card authorization, switching and routing and fraud detection. Alaric's customers include First Data, Euronet, Telecash, Corner Banca, Aduno, Swisscard, Yorkshire Building Society, Cumberland Building Society and Ukash.

Alaric is entirely focused on the payments industry and has a highly qualified team of payments and systems professionals which concentrates on designing and delivering sophisticated payment solutions based on Alaric's software products. Visit www.alaric.com

About Stratus Technologies

Stratus Technologies is a global solutions provider focused exclusively on helping its customers achieve and sustain the availability of information systems that support their critical business processes. Based upon its 25 years of expertise in server and services technology for continuous availability, Stratus is a trusted solutions provider to customers in manufacturing, life sciences, telecommunications, financial services, public safety, transportation & logistics and other industries. For more information, visit www.stratus.com.

Stratus, ftServer and Continuous Processing are registered trademarks, and ActiveService and the Stratus Technologies logo are trademarks, of Stratus Technologies Bermuda Ltd.

Intel, the Intel logo and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries/regions. The registered trademark Linux is used pursuant to a sublicense from the Linux Mark Institute, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis. Red Hat, Enterprise Linux, and the Red Hat Shadowman logo are registered trademarks of Red Hat, Inc. in the United States and other countries. UNIX is a registered trademark of the Open Group in the United States and other countries.

© Alaric Systems Ltd 2007; Stratus Technologies, Inc. 2007
X 947