

At ACI, we are passionate about helping the financial industry combat fraud. We're working with more than 150 organizations around the world to help them protect their customers, giving us a real insight into the fraud threats institutions face - and the tools to protect them.

Charlie Brown
Customer Relationship Manager, Omaha, USA



Stopping card fraud in its tracks

An industry guide from ACI

Contents

- 05 Foreword
- 07 Global card fraud overview and current strategies
- 12 Anti-fraud strategies
- 16 Best practice for combating card fraud
- 23 Conclusion
- 24 Putting the theory into practice... Nationwide Building Society
- 26 References

The questions this guide will answer

This guide discusses the key challenges facing banks around the world when it comes to payment card fraud. It also provides advice on how banks can combat the problem, specifically focusing on real-time prevention.

1. What types of fraud are currently experienced by other countries that could hit us next? Are we the weakest link?
2. What are the latest techniques to combat card fraud?
3. Are we currently investing in the right technologies to combat card fraud?
4. Fraud is becoming more complex in the current economic climate, but we have to work with the same budget and resources. How can we effectively combat new card threats?



Foreword

“With changing consumer spending patterns, the global card market has expanded rapidly in recent years. As TowerGroup predicted in 2008, the number of U.S. credit card and debit card transactions continues to grow and is expected to reach 21.7 and 34.6 billion respectively in 2009. However, it is not just the Western markets that have seen increases in the use of bank cards – emerging markets, such as Brazil and Mexico in particular, have seen the number of credit cards more than double from 2004 to 2007.¹

As the number of bank cards and the number of payments made with these cards increase, so too have associated fraud levels including identity theft on cards, stealing of cards in transit/mail, physical theft, counterfeit and skimming. As such, card fraud has become a significant problem for the global retail banking sector. Debit and credit card fraud alone is estimated by Visa and MasterCard to exceed US\$10 billion worldwide in 2009 and financial institutions are facing an ongoing battle to beat fraudsters while protecting their customers.

Around the world, fraud managers are confronted with the daunting task of reducing card fraud to prevent financial losses and the associated repercussions on the bank’s brand and reputation. While fraud in general has always had the potential to affect the way in which customers perceive their financial institution, the current so-called ‘recession crime wave’ comes at a time when they are under even closer public scrutiny. In addition, banks are under particular pressure to reduce costs and retain their competitive edge as much as possible. Fraud detection and reduction is one area where financial institutions are able to take decisive

and positive action to reduce losses, improve their image and provide better customer service.

Nationwide Building Society, like all other financial institutions, has experienced the impact of the growing problem of fraud across the industry, especially concerning its debit card portfolio. However, outstanding customer experience is at the forefront of Nationwide’s ethos and the right fraud prevention tools have enabled us to keep customer satisfaction high. We now have some of the lowest loss per card and lowest blocking levels in the industry – which benefits us as well as our customers.

The ACI Worldwide Guide to stopping card fraud in its tracks highlights the issues faced by financial institutions in the fight against fraud and offers solutions to minimize card fraud in today’s challenging environment.”

Pete Corrie
Head of Financial Crime, Nationwide Building Society

→ In Germany, there are over 90 million debit cards in circulation.



Global card fraud overview and current strategies

Europe

With changing consumer spending patterns, the European card market has expanded rapidly in the last few years. According to a report sponsored by Payments, Cards & Mobile, there are approximately 322 million credit and debit cards in circulation across the U.K., Spain and France and around 92 million in Germany. In Poland, the number of credit cards tripled between 2004 and 2007. Fraudsters have spotted this growing market as an opportunity and banks have seen their card fraud losses increase substantially as a result. However, the tactics used by fraudsters and their levels of sophistication as well as the counter-measures used by financial institutions still vary widely across Europe.

France

With 82 million credit and debit cards in circulation in 2007, France is one of the pioneers of smart cards which have been rolled out en masse to control fraud. By 1992, all French bank cards were chip-enabled² and during the first year following the introduction of Chip and PIN, total card fraud losses halved and domestic counterfeit fell by 78 per cent.³ In France, issuers are also provided with industry fraud scores by organizations such as Carte Bleue, which has successfully helped drive down some forms of card fraud.

The French have taken enthusiastically to online shopping, with a report in early 2008 showing that 94 per cent of French internet users had made at least one purchase online. In October 2008, liability for fraud-related losses incurred in online credit or debit transactions shifted from the merchants to the banks.⁴

Germany

Germany has not traditionally reported the same levels of card fraud as, for example, the U.K., perhaps in part due to the fact that German society remains very cash-based. However, use of cards, particularly debit cards, is growing and fraudsters are becoming increasingly sophisticated with ATM and non-domestic fraud currently being the key target areas.

Key stats

- The fraudulent use of card numbers and losses from altered and counterfeit cards accounted for 90 per cent of losses in 2007.⁵
- Card-not-present (CNP) fraud is booming with some French issuers reporting up to 70 per cent of CNP fraud coming from abroad.
- Cards are now systematically equipped with a microprocessor, resulting in an exceptionally low level of card fraud at the national level – 0.029 per cent of the value of transactions in 2005.⁶
- It is predicted that by 2012, cards will account for just under half of total payments by volume in France, up from 38 per cent in 2007.⁷

Key stats

- There are over 90 million debit cards in circulation in Germany.⁸
- Total debit card transaction value grew from €82.9 billion in 2000 to €106.3 billion in 2007, a CAGR of 3.6 per cent.⁹
- Germany had 1.13 debit cards per capita in 2007 with 1.74 billion transactions worth €106.3 being executed.¹⁰

→ In Italy, the value of credit card fraud jumped from €55 million in 2005 to €64 million in 2006.

Italy

Debit, credit and charge cards are referred to collectively as credit cards in Italy, which currently has over 30 million in circulation, almost two-thirds of which are debit cards.¹¹ In terms of combating fraud, Italy's Oversight Office is working with the Ministry of the Economy and Finance to establish a regulatory framework for a database to prevent the fraudulent use of cards and to create a mechanism to prevent identity theft in the field of financial services, particularly in the consumer credit sector.¹² Banks in Italy have proactively monitored both the card and ATM or point of sale (POS) devices for fraud for a number of years now. In addition, point of compromise and user-defined rules are used to combat fraud schemes.

The Netherlands

Similar to Germany, the country has traditionally not reported high levels of card fraud. Increasingly, however, CNP and overseas fraud is becoming an issue for customers and banks alike. Where skimming does occur, it is often at places such as railway ticket machines with limited additional security such as cameras. The country has also experienced problems with skimming at both ATM and POS devices. ATM devices have quickly been upgraded to add extra protection and, in 2007, the process was started to replace merchant POS terminals across the country with more secure (EMV) devices.

For online shopping, customers in The Netherlands increasingly use a system called iDEAL. With iDEAL a merchant website links directly to the consumer's secure online banking environment. From here the consumer creates a credit transfer to the merchant to make a payment, rather than using a credit or debit card. Although this trend has a positive effect and ensures the safety of internet transactions made by Dutch cardholders at Dutch online merchants, it does not address fraud problems like skimming.

Key stats

- Payment cards account for 34.6 per cent of the volume of non-cash payments in Italy¹³
- The value of credit card fraud in Italy jumped from €55 million in 2005 to €64 million in 2006.¹⁴
- Domestic fraud levels are still high due to the slow rollout of Chip and PIN.

Key stats

- Nine per cent of the population were victims of card fraud in 2006.¹⁵
- In 2007, skimming in The Netherlands cost €15m,¹⁶ rising to €31m in 2008,¹⁷ however this is still low in relation to the total volume of electronic payments.
- In 2008, 40 per cent of all internet transactions in The Netherlands were paid for with iDEAL, an increase of 87 per cent from 2007.¹⁸



Guglielmo Di Lorenzo
Technical Leader, Naples, Italy

Spain

Despite the 75 million credit and debit cards in circulation in 2008,¹⁹ Spain is still heavily reliant on magnetic stripe cards. In terms of anti-fraud strategies, the Spanish banks are real advocates of advanced analytics to control fraud losses. Advanced statistical techniques such as neural networks, profiling and user-defined rules are successfully used by the majority of financial institutions in the country.

Turkey

The frequent crises and bouts of high inflation that have historically characterized the Turkish economy have delayed the adoption and widespread use of credit cards. However, according to Lafferty, Turkey has more recently been propelled into the top ten global card markets in terms of profitability with profits of \$1.8 billion before tax in 2007. The country has also emerged as a leading innovator in combating fraud, implementing automated fraud detection processes and customer alerting via SMS messages.

In addition, some banks in Turkey have introduced live monitoring at ATMs to enable banks to contact the police immediately if they are compromised.

U.K.

There are 170 million credit and debit cards in circulation in the U.K., twice that of France or Spain in 2007.²³ One in four people in the U.K. have now been victims of card fraud²⁴ and credit card fraud costs the U.K. more than £1 million a day.²⁵ As a result, the U.K. banking industry has actively sought to combat fraud. This has led to U.K. banks emerging as early adopters of card fraud transaction monitoring solutions, such as neural network technology and multi-channel monitoring approaches being rolled out in places, in a bid to prevent potential card fraud.

Key stats

- 99 per cent of magnetic stripe transactions are made with online card issuer authorization.
- Card theft was responsible for the largest volume of fraud on cards in Spain, accounting for 41 per cent of purchase fraud alone.²⁰

Key stats

- Card numbers reached 36 million in 2007, up from 15 million in 2002.²¹
- Turkey has previously been found to be the country where British holidaymakers most often experience credit card fraud.²²

Key stats

- Crime and card fraud losses reached £609.9m in 2008, up from £535.2m in 2007, driven by card-not-present crime.²⁶
- There was a 63 per cent increase in reported financial crime in March 2009 compared to the same month in 2008.²⁷
- According to figures from APACS, the U.S. was the worst location for international fraud on U.K. cards with losses of £25 million in 2007, reflecting the greater use of e-commerce by U.K. cardholders.



Debi Harrison
Director Customer & Operations Manager
Watford, U.K.

—> In Dubai, credit and debit card fraud cases doubled from 2007 to 2008.³⁰

Middle East and North Africa

With the economic boom over the past few years, particularly in the Middle East, the total number of credit cards in the Middle East and North Africa region jumped by 24 per cent in 2006 to 6.23 million.²⁸ However, this has not only drawn businesses and developers to the area, but it has also increased its attractiveness to criminals. As a result, the region is seeing the effect on consumers' attitudes and consequently anti-fraud strategies of Middle Eastern and North African banks are likely to evolve in the coming years.

Sub-Saharan Africa

As the number of unbanked consumers in Africa is still high, levels of card use are still relatively low. However, EMV is being rolled out in places, in a bid to prevent potential card fraud.

The Americas

According to data from the U.S. Census Bureau, there were 173 million credit card holders in the United States in 2006. This number is projected to grow to 181 million U.S. Americans by 2010. In addition, the emerging markets such as Brazil and Mexico in particular have seen the number of credit cards more than double between 2004 and 2007. While solutions such as the EMV card standard or PIN technology have been introduced in most European countries, as well as in Canada and Mexico, it is not commonplace in the U.S. What's more, payment card risk management systems have traditionally focused on credit and debit cards; however, prepaid card processors have recently enhanced existing risk applications.

Across Latin America, statistics for the scale of the fraud problem are hard to come by, with estimates varying widely. In Mexico, for example, some say fraud hit a record \$62 million in 2003, with other reports saying it hit \$85 million as far back as 2001. However, card skimming is so widely recognized as a problem in the country that the U.S. State Department warns travelers to exercise caution.

Key stats

- In 2006, Jordan saw the highest growth of card use, with credit card numbers jumping by 61 per cent to almost 275,000. Tunisia had the second highest growth, up 55 per cent to 55,000.
- Credit card fraud losses in the Middle East grew 20 per cent from Dh1.8 billion in 2007 to about Dh2 billion in 2008.²⁹
- In the United Arab Emirates, it is estimated that financial fraud losses are running at an equivalent of US\$45 million per year.
- In Dubai, credit and debit card fraud cases doubled from 2007 to 2008.³⁰

Key stats

- The total South African rand value of credit card fraud losses over 2007/2008 was R420 million.
- The increase in credit card fraud figures is consistent with the large-scale rollout of credit cards by the banking industry in 2006, when there were already over 25.5 million debit cards and 7.2 million credit cards in South Africa.³¹

Key stats - Canada

- In 2008, \$104.5 million was stolen from customers' debit card bank accounts in Canada.³⁴
- Once Canada adopts EMV, which is expected to reach critical mass by 2010, the U.S. is expected to experience a rise in card fraud levels.

Key stats - Latin America

- While MasterCard ranks Argentina as the safest country in Latin America from a credit card fraud point of view, Chile scored more than double on the "fraud-o-meter" scale, with Brazil five times higher.³⁵
- Mexican acquiring banks have introduced Verified by Visa and MasterCard® SecureCode™ and, as a result, Mexican banks and merchants have seen an immediate reduction in online credit card fraud – in some cases by up to 85 per cent.³⁶
- In Chile there are 4 million branded, bank-issued cards, such as Visa and MasterCard, but there are 12 million private-label store cards.³⁷

Key stats - USA

- Consumers carry more than 1 billion Visa cards worldwide, more than 450 million of those cards are in the United States.³⁸
- Nearly one in every three consumer purchases in the United States is made with a payment card, including credit, debit and prepaid products.³⁹
- The number of U.S. credit and debit card transactions continues to grow. In 2008, TowerGroup predicted that by 2009 credit card transactions will have risen from 18.9 billion in 2006 to 21.7 billion, and debit card transactions will have risen from 25.3 billion in 2006 to 34.6 billion.⁴⁰
- Credit and debit card fraud is the number one fear of Americans in the midst of the global financial crisis.⁴¹
- U.S. credit and debit card losses continue to increase; in 2004 credit card losses accounted for \$1.8 billion and rose to \$2.04 billion in 2007. Debit card losses accounted for \$810 million in 2004 and rose to \$1.05 billion in 2007.⁴²

Asia

Due to the sophisticated technology, such as phone line hacking, which is used by organized crime rings, Asia has emerged as one of the more advanced and innovative regions in terms of combating card fraud. In addition, there have been a number of high-profile, large-scale internal fraud cases in Asian banks, which has led to financial institutions across the region taking all forms of fraud very seriously.

In China, the use of real-time monitoring tools that filter each transaction against user-defined rules has become prominent. What's more, moving away from a long-standing tradition of IT solutions built in house, there is now an increasing adoption of common international technology standards, tools and techniques to combat fraud.

Pacific - Australia and New Zealand

Although rates of card fraud are low, banks in the region are very proactive in the fight against card fraud, investing heavily in anti-fraud systems with well-established peer networks to share information, discussing potential fraud sharing strategies and tactical countermeasures, such as rules.

Australia's rate of card fraud is still low compared to the rest of the world and the country should see a further decrease in the next three years as most of the cardholder base moves to chip authentication.

Key stats

- In Asia, there is a mixed spread of credit card penetration, with the card base covering about 14 per cent of the working population in China, compared to 75 per cent in Malaysia.⁴³
- The bank card market in China consists mainly of debit cards.⁴⁴ Out of 961 million card instruments issued by the end of 2005, less than two per cent are credit cards.
- Scholars at Beijing's prestigious Tsinghua University have estimated that the equivalent of 16 per cent of China's GDP is lost to fraud and corruption each year, compared with an estimated four per cent fraud rate in the United States.⁴⁵
- Starting from a very low base in the 1980s, the growth rate of credit cards in India is one of the strongest in Asia. By 2010, India will have 35 to 40 million credit cards, according to industry players.⁴⁶
- In 2006, Singapore had 5.09 million credit cards, up from 3.23 million in 2002.⁴⁷

Key stats

- From June 2007 to June 2008, there were 2.1 billion debit card transactions in Australia, with a value of \$209.8 billion.⁴⁸
- In the same period, there were 1.8 billion credit card transactions on Australia-issued cards with a value of \$262.5 billion.
- From 2007 to 2008, debit card fraud in Australia dropped slightly from 7.2 cents in every \$1,000 to 6.6 cents.
- However, in the corresponding period, Australian credit card fraud increased from 44.7 cents in every \$1,000 to 53.2 cents, mainly due to an increase in card-not-present fraud and counterfeit skimming, of which there were a number of highly publicized incidents.⁴⁹



Yasuyuki Endoh
Senior Engineer, Tokyo, Japan

Anti-fraud strategies



The challenges

Numerous types of card fraud have developed over the years and are perpetrated regularly throughout the world. The most prevalent and commonly known type involves skimming card details. However, as new banking channels have opened up and grown in popularity, and the use of credit and debit cards has risen, fraud has evolved both in its sophistication and scope.

The industry has come a long way in terms of developing techniques to prevent card fraud from transaction monitoring through to the introduction of Chip and PIN or the implementation of CAP (Chip Authentication Program) devices, which authenticate users and transactions online and in telephone banking. However, banks are now facing increasing pressure to

cut costs and ensure maximum return on investment, particularly in the current economic environment. Yet banks cannot take their foot off the pedal when it comes to introducing anti-fraud strategies. Indeed, 2009 research from Datamonitor into financial crime⁵⁰ reported that despite efforts to combat fraud, the global financial crisis could accelerate a wave of financial crime with the banks being the main targets for criminals.

In order to protect themselves against potential fraudulent attacks, financial institutions need to find ways of implementing effective anti-fraud strategies while maintaining efficiency and keeping costs to a minimum. But the first thing they need to do is to address the challenges they face in the fight against card fraud.

Generally speaking, there are five main challenges facing financial institutions today in their fight against card fraud:

1. Accurately defining payment fraud

Fraud definitions and the labeling of reported payment fraud differ widely throughout the industry, from region to region and even from institution to institution. Consequently, there is little consensus of how fraud levels are measured and what the cost of fraud is within a country or the industry. As such, it is impossible to find comprehensive figures on global payment fraud levels. Levels of fraud are typically reported in purely financial terms and then broken down into the various sub-categories making up that fraud – e.g. card, check, online and identity fraud. This type of reported fraud data is often aggregated and untimely.

This leads to a number of problems. First, out of date information means that the fraud strategists are always one step behind the fraudster. Due to a lack of detailed fraud reporting, it is difficult for experts within banks to assess modus operandi and apply appropriate countermeasure techniques. For example, it is useful to know that CNP fraud levels are rising, but what does the actual fraud look like?

Secondly, non-granular high-level 'loss reporting' is good to gain a snapshot view of the extent of a fraud situation, but it does not give clues that will help pinpoint weak spots in an anti-fraud strategy. More sophisticated ways of measuring the true performance of a fraud prevention strategy, such as false-positives, detection rates and point of detection can be used to drive improvements.

Finally, reported fraud can be inaccurate. This is partly due to confusion in fraud definitions. For example, some banks may declare lower levels of fraud if first-party fraud is written off under different categories such as bad debt.

In order for the industry to accurately determine levels of fraud, a number of changes need to be made:

- A global fraud reporting mechanism should be put in place
- A definition and labeling guide needs to be agreed and provided
- Real-time information sharing should become the norm

→ Financial institutions need to co-operate and start to share information.

2. Fraud departments remain in silos

Typically, banks have supported each new delivery channel and, sometimes, each new product or service, with its own system within the IT infrastructure. This, combined with the recent flurry of M&A activity, has meant that banking systems can be a confusing mélange of different technologies. This approach has been mirrored within fraud departments where different teams and systems deal with different types of payment fraud. Card fraud teams are often isolated from teams dealing with other types of fraud conducted via different payment tools or access points – such as internet banking. This makes it difficult to gain a comprehensive overview of customers' payment patterns or to identify fraud that crosses payment types. In a case of account takeover as a result of phishing, a fraudster who goes online and changes the account address and then requests a new card to use for fraudulent purchases may not be picked up within a siloed system. The address change may be viewed by one team and the card transaction by another team. In isolation, this may appear to be normal activity, but when combined, it looks abnormal.



Card fraud teams are often isolated from teams dealing with other types of fraud conducted via different payment tools or access points.

3. Current techniques do not detect fraud quickly enough

The current techniques and metrics deployed by banks to fight fraud often only highlight a problem once a card has been used for fraudulent transactions once, twice or even several times. Without real-time transaction decisioning, the fraud monitoring solution may not be keeping up with the pace of the fraudster. By the time the fraud has been detected, the money has been taken and the customer experience has been affected.

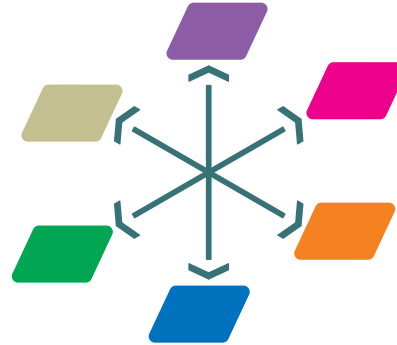
In order to protect their customers, it is crucial for financial institutions to consider real-time detection methods which can prevent losses from being sustained on customers' compromised cards. These tools allow institutions to monitor and immediately recognize suspicious transaction patterns, allowing them to act as soon as the fraudster makes an attempt and thereby prevent any losses.

4. Too often, fraud is considered a competitive issue

Traditionally, banks have considered their fraud prevention techniques as proprietary and therefore a competitive issue – one where they worry about exposing potential loopholes in transaction security. However, fraud is a good example of an area where financial institutions need to co-operate and start to share information.

Embracing the idea that fraud is a non-competitive issue is one of increasing importance for the entire banking community, particularly in Europe with SEPA becoming a reality. Technology, regulation and fraudsters will all continue to evolve and an industry-wide view of fraudulent activity will be pivotal in making in-roads into the ongoing fraud battle.

The effectiveness of solutions against fraud in the SEPA landscape will be similarly bolstered by the banking industry's adoption of a community spirit. As cross-border payments become easier, the sharing of anti-fraud techniques needs to become accepted and easy to facilitate.



Fraud is a good example of an area where financial institutions need to co-operate and start to share information.

5. Optimize working practices

With fraudsters adapting their techniques from one payment channel to the next, banks need to look at the current structures of their fraud departments, their expertise and the adequacy of the staffing levels.

With the appropriate workflow system in place, including a combination of the right levels of expertise and automated fraud detection tools, financial institutions can ensure they target fraud quickly and efficiently. And this should be done by adopting a variety of performance metrics as well as transaction queuing and automation technologies.

- A survey conducted by ACI in July 2009 found that 18 per cent of consumers questioned have been victims of card fraud in the past five years. The research, of more than 2,400 consumers across eight countries, also found that if an individual or someone they knew was hit by card fraud, half would consider changing banks.

Best practice for combating card fraud

With card fraud and its associated challenges recognized as a thorn in the side of financial institutions around the world, the industry needs to set about reviewing and, if necessary, updating its anti-fraud strategies and techniques. Today, the goal of any anti-fraud strategy should be a real-time detection and prevention system spanning all channels. The way in which fraud now effortlessly spreads across channels and regions, and the introduction of real-time payment processing channels, demand security measures that allow banks to detect and prevent fraud as it happens across the enterprise.

Real-time enterprise-wide fraud monitoring, combined with the automation of fraud analysis, means that banks can effectively fight sophisticated and complex fraud while also demonstrating efficiencies and return on investment.

An effective anti-fraud strategy must consist of two main parts: proven fraud prevention tools combined with proven fraud management techniques.



ACI Worldwide's top tips on how to combat fraud

Let's start with fraud prevention tools...

1. Detect potential fraud before it occurs, so you can prevent it

Preventing fraud losses can be achieved via a variety of anti-fraud techniques. Real-time, automated fraud prevention is not about catching the criminals after the activity has taken place, but instead it is about identifying fraud while it is happening and preventing the transactions from being authorized in the first place. Real-time scoring, profiling and rules can work with the authorization system to make a real-time fraud check and if deemed out of profile for the cardholder, the authorization attempt can be declined. Automated fraud prevention such as auto blocking can complement real-time transaction monitoring by blocking the card from subsequent fraudulent

transaction attempts. This ensures the bank and its customers do not suffer further financial loss, and helps protect the organization's reputation and brand in an unsettled market.

Top tips

- Use a real-time, automated fraud detection system which analyzes transactions during the authorization stage so that fraudulent transactions can be prevented before they occur.

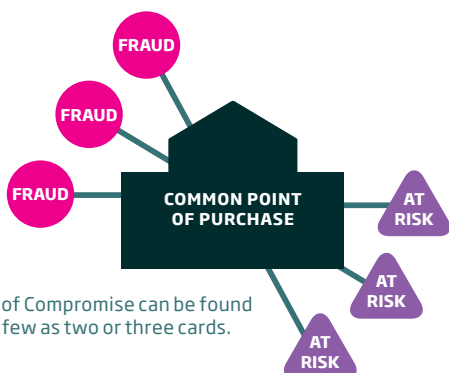
2. Know at what point your customer's card was compromised

Point of Compromise (POC) detection is an incredibly important preventative fraud action that a financial institution can take when addressing card fraud. The POC is the location at which the card skimming – the illegal copying of card numbers and PINs for the purpose of stealing money from bank accounts – has taken place.

Identification of a POC is important, as it allows the financial institution to recognize trends and apply action to detect and prevent future fraud attempts on skimmed cards. By identifying cards that may have been compromised early enough, the bank will have time to take preventative action on vulnerable cards before any money has been lost.

In order for a bank to identify a POC, it must have a sufficient number of cards that have experienced confirmed fraudulent transactions. The fewer the cards, the more difficult it is to identify the fraudulent location, but a Point of Compromise can be found with as few as two or three cards. The cards which have been used fraudulently will provide invaluable information on spending history and a common point of purchase across all cards should start to emerge. After a common location and time-frame have been found across a number of the cards, it is essential that other cardholders who may be at risk are quickly identified.

Once a list of cards at risk has been collected, the bank can decide a course of action. However, striking a balance between customer inconvenience and fraud prevention can prove difficult. The more action relating to fraud prevention that a bank takes, the more customers it will affect. Depending on the location of the POC, the bank may choose to 'block' or 'watch' cards at risk, choose to do nothing or a combination of the two.



A Point of Compromise can be found with as few as two or three cards.

→ Sophisticated fraud analytics enable more precise fraud management.

The techniques mentioned above can have a huge effect on a bank's fraud losses, but they can also affect staff workload. Identifying Points of Compromise and taking action on large numbers of cards using manual processes is very time-consuming and difficult, but when managed efficiently, such as by using the right tools to identify compromises and potentially vulnerable cards, these techniques can save many customers from fraud.

3. Improve customer service and detection with auto alerting

Automated alerting of transactions, for example using SMS or auto dialing, enables the bank to contact customers when a transaction occurs that meets their pre-set parameters; such as when it is over a certain amount or outside their usual spending habits. The customer receives an alert about the transaction which gives them the opportunity to immediately reply and block their card if it is fraudulent. Alerts can also be used for any transaction that the bank thinks is suspicious, even if it is within the customer's usual limits. Auto alerting can be cheaper, simpler and a more real-time method of managing potential card fraud compared to the traditional customer letters sent to potential victims. While the reported 'recession crime wave' explains why, more than ever, banks need to take a proactive approach to managing and preventing fraudulent transactions, this cannot come at the expense of great customer service.

Taking this a step further, by allowing customers to set the security parameters that they feel most comfortable with and sending an automated alert that doesn't require human intervention when these are breached,

Top tips

- Source as little as two to three cards which have experienced confirmed fraudulent transactions to find the Point of Compromise. These cards will provide invaluable information on spending history and a common point of purchase across all cards should start to emerge.
- After a common location and timeframe have been found across a number of the cards, identify other cardholders who may potentially be at risk.
- Write rules to monitor compromised cards for unusual spending activity.
- Use real-time decline or automatic blocking to reduce monetary fraud loss if fraud attempts are made on compromised cards.

banks can put the control back into the hands of the customer and deliver a more personalized banking service. The customer experience will be improved through reducing the number of false positives, while also minimizing the risk of genuine fraud being masked.

Top tips

- Use automated alerts to decrease fraud staff workload and enable more efficient work practices.
- Use auto alerting to allow customers to set their own security parameters so they receive a more personalized banking service.

4. Invest in fraud analytics

As fraud is now a global phenomenon perpetrated by highly organized criminals, it is essential that banks also ramp up their effort in the fight against fraud. A like-minded approach needs to be deployed such as the investment in a data analytics strategy. A well organized professional fraud analytics team will help banks to constantly track their customers' transaction patterns; identify, analyze and track fraud; measure current fraud strategy success; and make recommendations on the appropriate counter-fraud techniques.

A well-run fraud analytics team is made up of individuals who are skilled at data analysis, and are responsible for analyzing existing techniques and case by case transactions. They make recommendations for countermeasure strategies, such as new

rules, on a daily basis. Some of the more sophisticated fraud analytics groups also create their own profiling and neural modeling techniques to bolster existing fraud detection systems.

Top tips

- Invest in expert fraud analytics to keep up-to-date with the latest fraud trends.
- Establish customer profiles using data mining and neural network technology to identify transaction risk.

Fraud prevention metrics

- Point of Detection (PoD)
- False-positive ratio
- Basis point – a ratio used in the fraud industry to assess overall anti-fraud performance. It shows the ratio of fraud losses to sales turnover as a percentage. One basis point is one hundredth of one percent.
- Savings through fraud prevention – measured as the “open to buy” at time of fraud identification, or alternatively the fraudulent transactions declined as a result of blocking

And here are our recommended fraud management techniques...

1. Consider Point of Detection as a crucial fraud prevention success metric

Levels of fraud are typically reported in purely financial terms and then broken down into the various sub-categories making up that fraud. However, often the data that comes from the banks' fraud departments is purely loss based and does not include more sophisticated ways of measuring the performance of a fraud prevention strategy, such as false-positives and Point of Detection (PoD). The false-positive ratio is the number of transactions the system flags as suspicious, compared to the number of transactions that are actually fraudulent. Despite keeping a low false-positive ratio, many organizations find that their losses continue to escalate. PoD in combination with other metrics such as the false-positives ratio, therefore provides a more cohesive approach to an industry-wide anti-fraud strategy.

PoD measures how many missed fraudulent transactions occur prior to the system generating its first alert on an account. PoD is the metric that is most closely tied to fraud losses as it directly describes the number of lost transactions that occur before an analyst, or system, has the chance to stop a fraud.

2. Place more value on the customer experience

There have been a number of studies published recently about consumer attitudes to online banking or shopping, and there is a persistent theme of consumers still being worried about security and fraud. If banks implement the above strategies, they will be doing their utmost to protect their customers. Yet, there will always be some fraud that slips through the net.

When this occurs, what is essential is the customer experience after they have been a victim – how the bank reacts to the fraud and the inconvenience to the individual concerned. If the bank gets this bit right, by identifying the fraud quickly, informing the customer, and providing an efficient recovery or investigative service, customers actually report very good experiences. It tends to be very positive for the

A PoD of five means that, upon the fifth transaction, the system detected suspicious activity and an alert was generated within the bank. The four transactions prior to the PoD are all losses as is the fifth potentially depending on whether the detection system has real-time prevention capabilities.

PoD currently plays the biggest role in direct loss avoidance – the sooner banks can detect fraud on an account, the sooner they can take action on it and stem their losses. Based on an average loss per fraudulent transaction, it is easy to see the potential savings if detection is targeted at earlier transactions in the fraud cycle. Even a small drop in the average PoD of half a transaction per account can make more difference than increasing detection rates by a large percentage.

Top tips

- Start using PoD alongside more established anti-fraud techniques such as false-positives and detection rates.
- Use PoD as a key measure of your anti-fraud systems to get a better understanding of your performance and to improve customer service.

banks and really can promote loyalty. If, on the other hand, it is not handled well, then it is probably one of the greatest motivators for attrition.

Most consumers know that fraud might happen to them or someone they know, and they do not automatically blame the bank when it does. But they certainly do blame the banks if that fraud turns out to cost them significant amounts of time or money.

Top tips

- If fraud does occur, identify and inform the customer immediately by using a variety of communication mechanisms – SMS, email, letter, phone.
- Automate communication via auto-actions linked to fraud detection system alerts.
- Remember that by reacting appropriately to fraud, banks can promote customer loyalty.

3. Share key fraud information with your peers

The industry across many parts of the world is on the cusp of changing its attitude towards sharing data and it should be a long-term goal for financial institutions worldwide. Through information sharing, banks can learn about and protect against a new fraud before it hits them which means that the consequences will be far less than if it is dealt with blindly. Fraudsters always take the path of least resistance – they will operate their scam on a few institutions until they are blocked and then they will move on to the next banks and start the process again. At present, there

is very little sharing of information between peers, so the subsequent targets are just as susceptible to the attack as the first batch. Sharing information about fraud can dramatically reduce losses, but it can only be made possible if information sharing is promoted by the public and regulatory barriers are lowered.

Top tip

- The best defense is a good offense – share key fraud information so that you can learn about and protect against new types of fraud before they actually hit you.

4. Implement an enterprise-wide anti-fraud strategy

Adopting an enterprise-wide fraud prevention framework that allows for customer transaction monitoring within one system will help address a multitude of fraud reduction and cost efficiency requirements. Enterprise fraud management takes a holistic view of a financial institution's relationship with a customer by collectively viewing every product or service the customer uses, including non-financial transaction information.

With this type of approach, fraud losses can be managed more effectively by enabling complex fraud to be identified more quickly before substantial losses are sustained. With complex cross-channel fraud, such as identity theft where fraudulent transactions transcend product boundaries, a holistic approach is crucial. By having a complete view of the customer and their normal spending behavior, fraud is more readily picked up than with a silo approach where customer transactions on one product (such as a debit card) are monitored in isolation. An enterprise-wide anti-fraud strategy also helps fraud analysts manage and resolve cross-channel alerts and cases faster and more efficiently. Having a wide variety of cross channel data available within one business user interface provides analysts with the information they need in one place – without having to toggle back and forth between systems. ACI customers have reported a 66 per cent improvement in the speed in which they analyze alerts and work cases, translating to more cases worked and more potential fraud stopped earlier. An enterprise

approach can also reduce costs through IT consolidation and enables standardization and flexibility on platform applications.

In times when banks have to increase operational efficiencies, applying an enterprise-wide and automated approach to fraud enables banks to reduce costs both in terms of potential fraud losses and the analysts and systems involved in managing it.

Top tips

- Centralize the monitoring of card, ACH, check and wire activity occurring at a POS, ATM, branch, by phone and online to have a customer-centric view of activity and facilitate more effective cross-channel fraud analysis.
- Build customer profiles that aggregate customer activity, such as preferred ATM locations, typical ATM withdrawal amounts, frequency of out-of-country activity, online banking patterns including frequency and timing of sign-on and bill payments – to reduce false positives and better identify abnormal activity.
- Analyze the ROI that can be realized from an enterprise fraud management system – in terms of stopping fraud faster, improving analyst efficiency, and reducing hardware, software and labor costs from redundant systems.



5. Implement an automated case management system

The task of identifying and investigating fraud is a constant challenge and banks need to define processes for researching and resolving individual cases, including investigation activities, resources, timeframes, escalation paths and process alerts. An automated case management system provides a framework to better manage and automate activities and processes for various types of fraud including card fraud. It enables fraud prevention teams to track the success of their loss avoidance techniques, manage recoveries and quickly assess where countermeasures need to be deployed to help stay ahead of the criminal. In combination with alerting features and queue management, sophisticated case management tools provide a complete end-to-end fraud and risk management solution to banks globally.

Top tips

- Add automated case management techniques to streamline the investigative process.
- Leverage case management workflow processes to associate steps, tasks and activities with the different investigation types, compliance requirements and business policies.
- Work cases more efficiently when templates are used to identify required data elements and associated research activities by fraud type.
- Implement automated case profiling techniques to uncover open and closed cases that are related but do not generally appear to have an association.

*“Initially we just used **ACI Proactive Risk Manager™** to monitor credit cards. But when internet banking fraud started to increase slightly a few years ago, we utilized the software to accept online and telephone banking transactions. We quickly identified internet banking transactions that didn’t fit the customer’s normal usage profile... and we are now detecting almost all of our fraud. The flexibility in writing rules in Proactive Risk Manager is virtually unparalleled. There’s no possible way that we could have made the changes we’ve made within any other product. Proactive Risk Manager is pretty much the only tool that will allow you to do that.”*

Brett Small

Head of Consumer Banking Fraud, National Australia Bank

Conclusion

Across the globe, card fraud is not only leading to losses, but is also impacting brand, reputation and loyalty, at a time when banks are under particular public scrutiny.

As such, fraud detection and reduction is one area where financial institutions are able to take positive action to reduce losses, improve their image and provide a better customer service experience. Working together to increase awareness of the threats and understand the impact that fraudulent attacks can

have on the industry and wider economy will put banks in a stronger position to implement the latest card fraud technologies.

If you can answer all of the below questions with 'Yes' then consider yourself one of the few on the true front line of fraud prevention. If not, then use this list as a high level roadmap to identify current gaps and develop strategies to get you to the next level of fraud prevention.

So, how do you stack up? Ask yourself these questions:

1. Do I place resources into analytics and data-mining?
2. Do I use alternative measures of fraud performance such as Point of Detection?
3. Do I take advantage of a cross-channel fraud solution to break down my internal silos?
4. Do I automate as many processes as is appropriate?
5. Do I act proactively to stop fraud before it affects my customers?
6. Do I take advantage of new communication methods like automated alerts to interact with my customers?
7. Do I share information with my peers and use that information in my prevention strategy?

Putting the theory into practice...

Nationwide Building Society

Situation

Fraud on U.K.-issued cards has been increasing steadily, and financial institutions are facing an ongoing battle to beat fraudsters while protecting their customers. Nationwide Building Society, like all other financial institutions, experienced the impact of the growing problem of fraud across the industry, especially concerning its debit card portfolio.

As such, Nationwide Building Society initially approached ACI to build a database of debit card transaction history to reduce debit card fraud. After the initial phase of the project was complete, it became clear that ACI Proactive Risk Manager would be able to deliver many more benefits for the building society in terms of detecting and preventing fraud.

In May 2008, Proactive Risk Manager was implemented with a feed from ACI's BASE24® product that Nationwide uses for processing debit card payment transactions. Proactive Risk Manager is a comprehensive fraud detection solution to help card issuers, merchants, acquirers and financial institutions combat fraud schemes. From strategic user-defined rules to powerful neural network technology using custom modeling techniques, Proactive Risk Manager provides the means to cost-effectively reduce losses and limit an organization's risk exposure. Proactive Risk Manager was implemented with the tieback functionality, allowing selective rules to automatically change card statuses on BASE24, along with card blocking capabilities.

ACI also assisted Nationwide in adding a real-time feed to its fraud analysis system, allowing the team to deploy real-time rules that are able to decline transactions during the online authorization process. This element went live in December 2008, following a twelve-week project delivery.

In addition to providing the Proactive Risk Manager solution, ACI also provided project management, business consulting and technical assistance to Nationwide during the integration and implementation of the solution.

Benefits

ACI Proactive Risk Manager was chosen to monitor member accounts for potential fraud and apply preventative measures once fraud is identified for a number of reasons. These include: the solution's ability to quickly analyze transactions for fraud without impacting response rates; its flexible rules that allow Nationwide to create and deploy on the fly; the sophistication of its rules that allow Nationwide to be accurate in its fraud detection; and its automatic blocking functionality that can free up Nationwide's employee time for other fraud mitigation tasks.

Using Proactive Risk Manager, Nationwide is now able to accurately identify potential cases of fraud via custom defined rules and apply an automatic block to a card when the rule fires, preventing money from leaving the members' accounts.

This solution also allows Nationwide to decline card-not-present, Point of Sale, ATM or cross-border transactions, stopping fraud immediately before the criminals have raided an account. Nationwide is thus able to apply prevention measures such as a block without impacting genuine customers.

ACI Proactive Risk Manager at Nationwide

ACI Proactive Risk Manager is a complete fraud detection solution to manage risk in online and offline card environments. It combines the power of expertly defined rules with automatic blocking and decline messages to the authorization system BASE24 for fast, accurate and flexible response to the evolving and growing nature of issuer card fraud.

Through its sophisticated rules technology, Proactive Risk Manager compares the characteristics of each Nationwide member transaction with fraud identifying features, it then assesses and flags the transaction for fraud in real time or near-real time. In real time, once a transaction is identified as fraudulent, a message is automatically sent back to BASE24 via tieback integration to apply preventative blocks.

Results

Following the implementation of ACI Proactive Risk Manager, the fraud levels on Nationwide's debit card fraud portfolio dropped by around 80 per cent, with most fraudulent activity being stopped no later than the second transaction.

In February 2009, Nationwide's debit card fraud losses were the lowest for over four years and reversed the trend experienced by the industry of 18 per cent year-on-year increases.

Nationwide's fight against card fraud has been recognized by Visa as "an incredible story" and puts ACI Worldwide at the forefront of card fraud detection.



References

1. Market Research, Global Credit Card Industry - Emerging Markets, <http://www.marketresearch.com/product/display.asp?productid=2043042>
2. Online and Overseas: Payment Card Fraud - France, Spain and U.K., Payments, Cards & Mobile
3. What is Chip and PIN, <http://www.greenwichmeantime.co.uk/time-zone/europe/uk/website/financial-services/banks/retail-banking/credit-cards/credit-cards/smart-cards/index.htm>
4. Electronic Payments International, November 2008, 'Slowly breaking the cheque habit'
5. Online and Overseas: Payment Card Fraud - France, Spain and U.K., Payments, Cards & Mobile
6. Payment and securities settlement systems in the European Union: euro area countries, ECB Blue Book 2007 / 2008
7. Electronic Payments International, November 2008, 'Slowly breaking the cheque habit'
8. Wikipedia, Debitkarte, <http://de.wikipedia.org/wiki/Debitkarte>
9. Electronic Payments International, May 2009, 'Uphill battle against cash's dominance'
10. Electronic Payments International, May 2009, 'Uphill battle against cash's dominance'
11. Debit, Credit & Charge Cards, Just landed, <http://www.justlanded.com/english/Italy/Italy-Guide/Money/Cards>
12. Payment and securities settlement systems in the European Union: euro area countries, ECB Blue Book 2007 / 2008
13. Payment and securities settlement systems in the European Union: euro area countries, ECB Blue Book 2007 / 2008
14. Major surge in confiscation of counterfeit Euros, 25th November 2007, Life in Italy, <http://www.lifeinitaly.com/node/2389>
15. Report suggests U.K. is 'card fraud capital of Europe', 22 November 2006, CreditSearcher, <http://www.creditsearcher.co.uk/features-1164214457.html>
16. <http://www.nu.nl/economie/1531023/15-miljoen-schade-door-skimming-in-2007.html>
17. Currence Annual Report, 2008
18. Currence Annual Report, 2008
19. Online and Overseas: Payment Card Fraud - France, Spain and U.K., Payments, Cards & Mobile
20. Online and Overseas: Payment Card Fraud - France, Spain and U.K., Payments, Cards & Mobile
21. Turkey's credit card debt surges over 500 percent since 2002, 9th January 2008, Lafferty, http://209.85.229.132/search?q=cache:hCo_rm5K110J:www.lafferty.com/pdf/Press%2520Release%2520Turkey%2520Jan%25202008%2520_Final_%2520_2_.pdf+%2336+million+in+2007,+up+from+15+million+in+2002%22&cd=1&hl=en&ct=clnk&gl=uk
22. Turkey tops card fraud table, U.K. Net Guide, http://www.uknetguide.co.uk/Business/Article/Turkey_tops_card_fraud_table.html
23. Online and Overseas: Payment Card Fraud - France, Spain and U.K., Payments, Cards & Mobile
24. Recession crime wave hits Britain, 6 March 2009, Daily Telegraph, <http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/4948903/Recession-crime-wave-hits-Britain.html>
25. What is Chip and PIN, <http://www.greenwichmeantime.co.uk/time-zone/europe/uk/website/financial-services/banks/retail-banking/credit-cards/credit-cards/smart-cards/index.htm>
26. 2008 fraud figures announced by APACS, 19 March 2009, http://www.apacs.org.uk/09_03_19.htm
27. Recession crime wave hits Britain, 6 March 2009, Daily Telegraph, <http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/4948903/Recession-crime-wave-hits-Britain.html>
28. Explosion in popularity of credit cards in the Middle East, 18th June 2007, ameinfo, <http://www.ameinfo.com/123890.html>
29. Credit card fraud could rise in 2008, Gulfnews, 14th January 2008, http://archive.gulfnews.com/business/Banking_and_Finance/10181723.html
30. Credit card fraud doubled in past year, police say, Gulfnews, 14th March 2009, <http://archive.gulfnews.com/articles/09/03/15/10294931.html>
31. Credit card fraud up 60%, Moneyweb, 24th November 2008, <http://www.moneyweb.co.za/mw/view/mw/en/page38?oid=238587&sn=Detail>
32. Meeting the Demands of a Diverse Society, Electronic Payments International, May 2009
33. Meeting the Demands of a Diverse Society, Electronic Payments International, May 2009
34. Less-secure Canadian debit cards a target for fraud: analyst, 8th May 2009, CBC Canada, <http://www.cbc.ca/technology/story/2009/05/08/tech-debit-card-fraud-chip-magnetic-stripe-interac.html>
35. Venezuela top of the charts with x 10 times more internet Credit Card fraud, 19th September 2003, http://www.vheadline.com/printer_news.asp?id=11093
36. First Atlantic Commerce Collaborates with Prosa to Reduce Online Credit Card Fraud in Mexico, 3rd June 2009, <http://www.newswiretoday.com/news/51994/>
37. Electronic Payments International, January 2009, 'A market ripe for major expansion'
38. Credit card statistics, industry facts, debt statistics, <http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php#marketshare>
39. Credit card statistics, industry facts, debt statistics, <http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php#ownership>
40. Consumer Banking Fraud Trends: Welcome to the No-Hype Zone, 7th August 2008, TowerGroup
41. Credit card statistics, industry facts, debt statistics, <http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php#ownership>
42. ABA Deposit Acct Fraud Report, 2007
43. The Asian Banker - Indian Banking Industry: Outlook and Opportunities Assessment 2006-2007
44. The Asian Banker -Industry Assessment Report 2006-2007, China Banking Industry: Outlook and Opportunities Assessment 2006-2007
45. Chamber Eye - Magazine of the British Chamber of Commerce Guangdong - Summer 2008: China's Booming Fraud Industry,
46. The Asian Banker - Indian Banking Industry: Outlook and Opportunities Assessment 2007
47. Electronic Payments International, August 2008, 'Asia's pocket-sized powerhouse'
48. <http://www.bankers.asn.au/APCA-fraud-data-Australian-fraud-rates-low-UK-four-times-higher/default.aspx>
49. Australian Payments Clearing Association (APCA), 30th May 2008
50. Banks more vulnerable to fraud, Computing, 26th March 2009, <http://www.computing.co.uk/computing/news/2239316/banks-vulnerable-fraud-reprt>

About ACI Worldwide

ACI Worldwide powers electronic payments for financial institutions, retailers and processors around the world with the broadest, most integrated suite of electronic payment software in the market. More than 75 billion times each year, ACI's solutions process consumer payments. On an average day, ACI software manages more than US\$9 trillion in wholesale payments. And for more than 150 payments organizations worldwide, ACI software ensures people and businesses don't fall victim to financial crime. We are trusted globally based on our unrivaled understanding of payments and related processes. We have a definitive vision of how electronic payment systems will look in the future and we have the knowledge, scale and resources to deliver it. Since 1975, ACI has provided software solutions to the world's innovators. We welcome the opportunity to do the same for you.



ACI Worldwide

Offices in principal cities throughout the world
www.aciworldwide.com

Americas +1 402 390 7600

Asia Pacific +65 6334 4843

Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright **ACI Worldwide 2010**

All product names are trademarks or registered trademarks of their respective companies. ACI and the ACI logo are trademarks or registered trademarks of ACI Worldwide Corp. in the United States, other countries, or both.

ABR4414 10-10