

# Catching the crooks

With consumers strapped for cash and morale among retail staff often at a low ebb as store closures loom, many are predicting a High Street crime wave. Penelope Ody looks at how retailers are fighting back

Those who steal from shops – argue some experts – can be divided into two groups: the ‘hardened criminals’, be they staff or customers, who will steal at every opportunity and the ‘essentially honest’ who may help themselves to the odd paperclip or ballpoint but may occasionally be driven by circumstances to steal on a larger scale. Given the ease of shoplifting or dipping into the till – and the minimalist penalties – the ‘criminals’ are increasingly targeting retail, while some of the ‘honest’, who see their jobs disappearing as store closures mount, are more inclined to help themselves before the shutters finally come down. In the US, the organised crime element is already significant: truck loads of goods are stolen and then teams of accomplices blitz outlets across the country on the same day ‘returning’ the merchandise for a 100 per cent refund – a far more profitable option than selling the goodies on eBay.

Earlier this year, Joshua Bamfield, director at the Centre for Retail Research, which produces the annual *Global Retail Theft Barometer*, was surveying retailers across Europe on increasing theft: “Around 40 per cent said that shoplifting is increasing,” he says. “And in general violence is also up. These retailers were also seeing a change in the sort of goods that are stolen with more household goods – such as meat or cheese – taken, possibly for personal consumption rather than resale, while many reported an increase in trolley push outs. Staff morale is also often very low with lack of confidence about long term prospects and that can coincide with an increase in shrinkage.”

While store theft – by both staff and customers – appears to be on the increase, retailers are also keen to cut costs and improve the bottomline: hardly surprising then that most vendors of loss prevention systems are reporting healthy orderbooks and numerous enquiries. With ROI on loss prevention data mining systems often counted in weeks rather than months, the sector is seen as delivering quick wins and clear benefits. “Retailers can achieve ROI in three to six months,” says Malcolm Peden, CEO at IntelliQ. “And our sales are up 60 per cent this year.”

While the IntelliQ user group has not been reporting massive growth in fraud detection – probably because they already have good systems in place, argues Peden – they are seeing a rise in collusion. “There is growth in transactions where the customer

takes maybe eight or nine items to the checkout, the cashier appears to ring them all through but actually then deducts perhaps six or seven of the items from the sale so that the shopper pays for one item but to anyone watching it looks like a rather good sale is taking place. The goods can then be sold on eBay and shopper and cashier split the proceeds.”



Such transactions obviously come to light using the sort of data mining techniques provided by companies like IntelliQ, although the crooks may get away with a sizeable haul the tactic is quickly spotted and a new report added to the application to pick up any repetition. According to Peden, H&M - an IntelliQ customer for around five years - is still adding a new report almost every month as the fraudsters come up with new wheezes.

**In demand**

While centralised data mining systems like these are often preferred by the audit department, store-based loss prevention tools are also proving popular with operational teams helping to pinpoint training and systems errors as well as fraud. Smart Store from PCMS - used by the likes of Boots and Waitrose - comes into this category. "The system analyses every transaction and produces a report for the store manager which he or she can then discuss with staff in the usual morning round," says sales and marketing director, Richard Goodall. "Many of these can be genuine errors or inno-

given away free to friends or sometimes bulk supplies are disappearing through the back door - one of our users said that he had an entire pig missing."

**"Many retailers are now realising that they must broaden their areas of loss prevention activity as the criminals are getting very clever"**

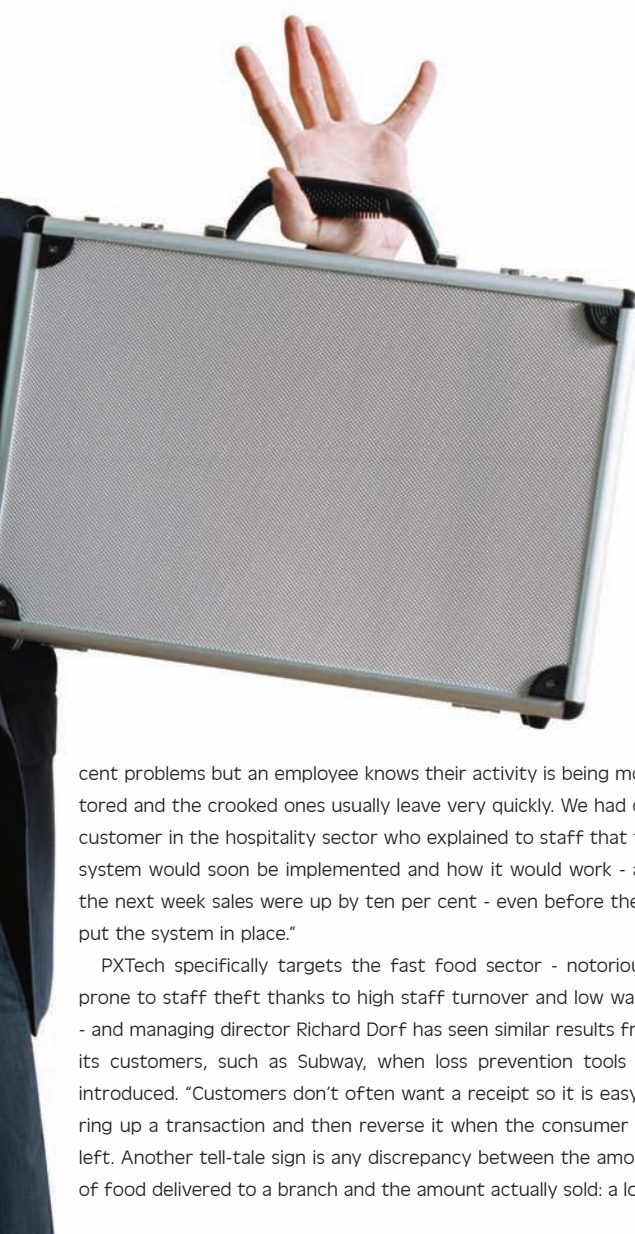
Sysrepublic - founded by four members of Marks and Spencer's rapid application development team back in 2002 - focuses, like PCMS, on real-time store-based information. Back in its M&S days, the team was behind an award-winning application which highlighted dubious transactions at the checkout and alerted security staff via SMS, so that the crooks were often caught before they left the store. The core application has moved on since then and - given the risk of violence - it is hardly surprising that no current users want to send text messages to staff demanding instant action. Current users include Tesco, Sainsbury, Asda, HMV as well as M&S giving Sysrepublic an impressive database of transactions. "Dishonest people exhibit certain characteristics at the checkout and we've defined a series of such behaviours so that checkout activity can be monitored in real-time, although most retailers prefer to work in batch mode. Rather than wading through reports generated by extensive data mining, the system provides the loss prevention team with precise, targeted information."

Sysrepublic's user group - the Secure Alliance - has also helped the company identify a new and growing target for the fraudsters: electronic gift cards. Again it can involve collusion with shoppers or a dishonest sales assistant may simply accumulate a surplus in the till during the day using time-honoured tactics and then simply transfer the balance to a fully authenticated gift card at the end of the day and walk out with the takings. A refund followed soon after by a gift card transaction for the same value is a rather obvious indicator of potential fraud.

While many loss prevention analytics focus on EPoS data, IDM Software - whose customers include Jaeger and Monsoon - finds growing interest in adding other data feeds to the analytics engine - taking information from time and attendance, or stock records for example. "These crooks are not all stupid," says CEO Khuram Kirmani. "Many understand retail systems and they can disguise their activities between several events. If you bring data in from multiple sources then you can see where fraudsters have covered their tracks."

"Shops are still the main focus," adds commercial director David Snocken. "But many retailers are now realising that they must broaden their areas of loss prevention activity as the criminals are getting very clever."

Well, some of them are: PXTech's Dorf recalls one user, rightly concerned about a raft of unauthorised price adjustments that kept appearing on the system from one branch. CCTV analysis soon found who was to blame - an innocent staff member polishing the touchscreen without turning it off and causing all sorts of alterations in the process.



cent problems but an employee knows their activity is being monitored and the crooked ones usually leave very quickly. We had one customer in the hospitality sector who explained to staff that this system would soon be implemented and how it would work - and the next week sales were up by ten per cent - even before they'd put the system in place."

PXTech specifically targets the fast food sector - notoriously prone to staff theft thanks to high staff turnover and low wages - and managing director Richard Dorf has seen similar results from its customers, such as Subway, when loss prevention tools are introduced. "Customers don't often want a receipt so it is easy to ring up a transaction and then reverse it when the consumer has left. Another tell-tale sign is any discrepancy between the amount of food delivered to a branch and the amount actually sold: a lot is

# Meeting deadlines

Will Hadfield takes a look at retail's attempts to comply with the multi-faceted security standard that is PCI DSS

Over the last two years, the world's biggest banks have caused a global recession through their reckless lending. They prove their interdependence with the rest of the economy in other ways too. For example, every retailer on the planet that wants to give their customers the option of paying for goods using credit or debit cards has to comply with the Payment Card Industry Data Security Standard (PCI DSS) - a wide-ranging set of guidelines designed to prevent criminals obtaining credit and debit card data from retailers' computer systems. Every two years, the three main card issuers - American Express, Mastercard and Visa - issue a new set of standards. The card issuers use the banks to monitor retailers' compliance and, if necessary, take enforcement action against them. The banks can fine retailers and even prevent them from carrying out card transactions.

PCI DSS is a major imposition on retailers and their IT departments, but it has succeeded in changing criminals' behaviour. Before the first set of regulations were introduced in October 2006, criminals - understandably - concentrated their attacks on large retailers. The bigger the retailer, the larger the number of credit and debit cards available to steal. "In terms of the frequency of attacks on big retailers, they are going down," comments Steve Wilson, a director at Visa Europe. "The criminals have moved from trying to attack big merchants to going for smaller retailers and e-commerce merchants. We think that's because of the focus we put on the merchants three years ago."

The most valuable pieces of data for fraudsters are card numbers, the information held on the magnetic strip, and the CV2 - the three-digit security code on the back of every card issued by Visa and Mastercard (American Express uses a four-digit number on the front of the card for the same purpose). According to Visa, some 92 per cent of the largest retailers in Europe comply with the most important part of the regulations: they do not hold any of the three most attractive types of data on their IT systems. E-commerce retailers, who are more exposed to attacks because their systems touch the internet, are even more compliant with some 98 per cent holding none of the three most desirable types of data. Among medium-sized retailers, the level of compliance is 87 per cent.

Wilson describes the standard as "a sensible approach to the issue of criminals trying to steal valuable customer data". PCI DSS covers most parts of a retailer's IT estate. For example, a well-known High Street retailer with 3,000 stores, which processes six million card transactions a year, is currently writing its IT roadmap for the next three years. The roadmap is broken down into three-month chunks. The IT department is responsible for implementing all the projects set out in each three-month block. PCI DSS covers payment applications and the network that



connects the stores together. But its reach extends throughout the retailer's infrastructure, including end-user computing, server platforms and mid-range applications.

#### Wary outlook

During a recession that is hammering consumer spending, implementing PCI DSS is a massive challenge. However, large retailers must comply with the regulations, or at least be able to

demonstrate that they are on track to comply, because the Payment Card Industry Security Standards Council - the body that writes the rules - insists on annual inspections for the largest retailers. Adam Knowles, a consultant at Xantus, who is helping draft the roadmap for the retailer with 3,000 stores, says that the card industry is deliberately ambiguous about what action it will take against non-compliant companies. "We do not know the extent to which they will try to enforce their September 2010 deadline. The standards will be enforced through the acquiring banks rather than directly through Visa and Mastercard," says Knowles.

The downwards pressure on IT spending because of the recession is not the only reason why retailers are wary of PCI DSS. They need to make their IT systems as efficient as possible so that they can maximise sales, both in stores and online. "A lot of retailers want the checkout times to be in seconds rather than minutes," says Knowles. "They need to host their own systems for processing that data to maximise speed. But, if you think of a large network, to build in the security required by PCI DSS is not a small undertaking and it's made worse because the standard is evolving." A retailer with 3,000 stores might need the two years allowed by the Security Standards Council just to roll-out software upgrades to all of its stores.

"The criminals have moved from trying to attack big merchants to going for smaller retailers and e-commerce merchants. We think that's because of the focus we put on the merchants three years ago"

In the US, some retailers have called for the card industry to pay for securing their own data. David Hogan, the chief information officer at the National Retail Federation, the trade body for American retailers, has called the current system of onerous standards impractical. "If the goal is to make credit card data less vulnerable, the ultimate solution is to stop requiring merchants to store card data in the first place," Hogan says. "The bottomline is that it makes more sense for credit card companies to protect their data from thieves by keeping it in a relatively few secure locations than to expect millions of merchants scattered across the nation to lock up their data for them."

Retailers could decide to stop holding sensitive information on their systems, but they could only do so by purchasing a hosted service for their payment systems. Inevitably, they would have to spend more money. "There are cost savings from leveraging existing resources," says Knowles. "To put something dedicated for card payments into your infrastructure is always going to be more expensive." Retailers around the world have until September next year to introduce the second set of PCI DSS regulations which came out in October 2008. Unless they can find a way of securing card data more cheaply than by doing it themselves, they should get ready for a third set of PCI DSS rules in October 2010.





# The invisible touch

Recent figures have shown that card-not-present (CNP) fraud is on the up. Hannah Prevett asks: is introducing a specialist payment solution the answer?

**F**raudulent behaviour is nothing new. The inherently human act to deceive another for personal gain has always been commonplace. Yet fraudsters now have a new weapon in their armoury: the internet. And they are firing on all cylinders. In recent times, the advent of chip and PIN has brought about a reduction in cardholder present (CP) transactions. This system works in two ways: the chip proves that the card is genuine; entry of the PIN ensures that the person presenting the card is the true owner. However, in the non-physical world, such as in the realm of the internet, chip and PIN is of little use against fraudsters.

The most recent figures from the UK payments association, APACS, showed that card fraud losses totalled almost £610 million in 2008, which means that of every £1 spent using cards, a tenth of a penny is lost to fraud. The data also revealed that CNP fraud losses have increased by an eye-watering 13 per cent over the last year, accounting for 54 per cent of all card fraud losses. The evidence shows a clear correlation between the soaring popularity of internet shopping and escalating fraud levels. From 2001 to

2008, CNP fraud losses rose by 243 per cent; in the same time period, the total value of online shopping transactions increased by 524 per cent.

In the light of such sobering statistics, how can online retailers best protect themselves? The key is not to panic, says Garreth Griffith, head of risk management at payment solution provider PayPal. "I think there's a perception of complexity because the internet is still relatively new; people are still figuring it out to some extent," he perceives. "They need to go onto the web with their eyes open. There are lots of processes and people out there to keep websites protected."

Steve Davis, executive vice president and international president at GSI Commerce, says it's an "urban myth" that online retailing is less secure than offline trading. "In fact, with Bricks and Mortar retailers there is usually a higher rate of fraud and shrinkage. In-store, inventories are much more difficult to track and there are considerably higher cases of internal theft," he attests.

Added to this, there are many methods by which online

merchandisers can shield themselves from the negative effects of fraud, explains Michael Norton, managing director at cash payment service provider PayPoint.net. "One way for retailers to protect themselves from fraud is to use a payment platform that supports PCI DSS – the card industry's data protection standard – and 3D Secure, a Visa and Mastercard scheme which requires cardholders to provide an additional password before the transaction completes," he suggests.

Such platforms have in-built real-time fraud management capabilities designed to spot any fraudulent transactions before any funds change hands. This gives retailers a certain peace of mind, says PayPal's Griffith. In addition, the provider usually helps manage compliance and regulatory burdens. However, Tom Boardman, co-founder and technical director at Firebox.com, a leading e-tailer of toys and gadgets, says responsible retailers will already be aware of their regulatory obligations. "Anyone that processes credit card transactions, like we do, has to be PCI DSS compliant," he explains.

Luckily for Boardman, fraud levels and chargeback rates at his company are incredibly low – just 0.05 per cent. But he is not complacent. "We manage to keep fraud levels relatively low due to in-house fraud detection systems that we've developed over many years," he explains. For Boardman, a technology whiz kid, designing and implementing a back-end payments system wasn't particularly problematic, but for others it can be a minefield. "Setting up your own system to take money on the internet is more complex than many merchants first think," says Griffith. Certainly, many consumers and retailers have been persuaded by this rationale: the numbers speak for themselves. "We have two million accounts in the UK now," he claims. PayPal also maintains a very low loss rate due to fraud – 0.33 per cent.

Despite early stage trials of PayPal on Firebox.com, Boardman remains unconvinced of the benefits. "We are currently trialling

PayPal to see if it provides an increase in conversion rate that makes up for the increased transaction processing cost. It's too early at the moment to assess the benefits, if any." Like many, Boardman wants proof that the elevated costs associated with alternative payment systems such as these can be offset by increased sales.

**Attractive prospect**

For PayPoint's Norton, there is another, simpler way to exchange funds and goods and services, without a credit card in sight, thereby removing the opportunity for fraud to occur. "There is one way to avoid card fraud altogether, of course, and that is to accept payment in cash for goods purchased online," he suggests. In this instance, a consumer would order goods online where they would be given a code. They would take this code to a PayPoint kiosk and pay for the product, at which time it would be dispatched.

This certainly is an attractive prospect for merchants. One clued-up entrepreneur reveals his company is seriously considering PayPoint as an alternative to PayPal. "It's certainly interesting," he comments. Up until now, PayPoint is best known for its foray into the utilities market, with customers topping up electricity meters at allocated payment terminals. Payments are worth around £7 billion a year. But the use of PayPoint looks likely to become more widespread, says Norton. "A handful of payment service providers offer this capability at present, but since it offers real peace of mind to consumers and retailers alike, it is likely to become a mass-market phenomenon soon."

Whether retailers decide to implement a payment platform or build their own, education and protection against fraud is essential because internet fraud and e-crime isn't going to be eliminated any time soon, says Griffith. "It's a fact that in the real world, no matter what you do there's going to be a bit of shoplifting or pick pocketing – it's the same on the internet."

