STOP THIEF!

Tackling store losses head on

Run! The iconic 1990s movie "Trainspotting" opens with Mark Renton, played by Ewan McGregor, being chased down an Edinburgh street, having stolen from CD shops to pay for his addiction, to the compelling beat of Iggy Pop's classic Lust For Life.

These days, in value terms anyway, the priority in retail fraud prevention is less about stopping thieves in their tracks and more about card fraud, as detailed on the Financial Fraud Action (FFA UK) website, a leading source of up to date information on card fraud on UK-issued credit and debit cards.

Shopping is now the UK's largest consumer leisure activity, leading to an exponential rise in levels of retail crime. One man who knows about this subject is Professor Joshua Bamfield, Director of the Centre for Retail Research in Nottingham. The CRR provides authoritative and expert research and analysis of the retail and service sectors in Britain, Europe and globally. Its Global Retail Theft Barometer covers 43 countries.

"When Chip and PIN came in," the Professor told The Grocery Trader, "it became much more difficult to commit card fraud. These days, criminals buy PIN data and stolen identities on line from black sites, and it takes skill to commit criminal fraud against retailers."

But retail loss prevention isn't solely about stopping fraud and theft. As Professor Bamfield points out, money handling is another major cost, hence in effect a cause of loss to the business. With an average shopper spend of £14 in a typical convenience store, there is an urgent need to implement contactless payments. Professor Bamfield believes the Co-op is the furthest along the line. "Contactless is like RFID used to be in retail. People were always talking about it at conferences, but doing nothing about it. There is a lot of potential to be realised."

If you'd like to know more, Professor Bamfield's book, "Shopping and Crime," published by Palgrave Macmillan, draws on criminology, behavioral economics and marketing to help understand retail crime as a cultural phenomenon. According to the Palgrave Macmillan website, the book "analyses important new datasets on employee theft and shoplifting to show the nature of the problem, its origins and possible solutions. It explores crime prevention as a management issue, using criminomics, a new concept based on commercial realities rather than maximising arrests. This emphasises communications and persuasion within organisations, supported by a web of collaborative projects between retailers, police and other crime agencies."

Stand by for the feature on Omnichannel Retailing in our May issue.

Lancope® enhances Visibility and strengthens security in StealthWatch System 6

Lancope, Inc., a leader in network visibility and security intelligence, has unveiled the latest version of its context-aware security analytics platform, StealthWatch® System 6.6. With new security algorithms, enhanced network visualization, and more operationalized threat intelligence, the new platform enables enterprises to more quickly and effectively detect and respond to advanced threats.

"Many enterprises have come to realise that if they cannot quickly view the entirety of what is going on within their network, they stand little chance of fending off today's more sophisticated attackers," said Javvad Malik, senior analyst for the Enterprise Security Practice at 451 Research. "Eliminating blind spots in enterprise infrastructure, gaining an in-depth look at network activity, and applying advanced analytics that enable users to more easily pinpoint suspicious behaviors indicative of an attack are key capabilities needed."

StealthWatch System 6.6 extends Lancope's already-robust network visibility and security intelligence offerings with several key new capabilities. New feature highlights include:

Expanded Cisco Technology Support and Mitigation with Cisco ISE

Lancope is leveraging the latest Cisco ISE 1.3 platform to deliver even more extensive network visibility and new mitigation capabilities to joint customers. Through the integration, Lancope's StealthWatch System delivers in-depth identity/device awareness, and users can also take quarantine actions directly from the StealthWatch Management Console (SMC) by using Cisco ISE's dynamic network control capabilities. Additionally, new support for Cisco UCS Blade Servers provides greater visibility within enterprise data centers, and support for Cisco NBAR2 improves application performance monitoring and root cause analysis.

New Security Algorithms for More Precise Analytics

In version 6.6, Lancope has added a set of new security algorithms that provide increased defense against increasingly prominent attack behaviors, such as machines communicating with phantom hosts, applications traveling over non-standard ports, brute force login attempts and suspect quiet long flows, just to name a few. These security algorithms set the StealthWatch System apart from other technologies, allowing for more precise analytics and actionable alarming on today's top threats.

Enhanced Visualization and More Operationalized Security Intelligence

More operationalized security intelligence and an actionable Host Report enable users to more quickly extract and visualize the exact data they need to solve problems. New alarm categories have been added to the main StealthWatch Security Insight Dashboard for faster threat investigation, while the StealthWatch Host Report has been completely revamped to display more dynamic and visual analysis of host data.

Additional advancements in StealthWatch System 6.6 include:

- **Extended system scalability** to 6 million flows per second with the introduction of the new FlowCollector 5000
- **Increased capacity for cloud deployments** with new FlowCollector™ Virtual Editions (VE) 2000 and 4000
- **Assisted Network Classification (ANC)** to help with background discovery and segmentation of new network assets
- Faster, more streamlined querying with job management enhancements

Protecting your business against fraud

Fraud and theft are unfortunate facts of life in the grocery business. However, knowing what to be mindful of can help you reduce your potential exposure. As one of the world's largest card payment processors, we have compiled a list of the most common frauds we have encountered through our time working with the grocery trade, along with how to best protect your business. By Chris Davies, Managing Director, Global Payments.

1. **Multiple cards used and declined attempts:** Fraudsters often buy batches of card details and will try to place orders over the phone or online, continuing with each set of card details until one works. If you get multiple declines, be careful with the order.
2. **Requests to refer an authorisation request:** If the message 'CALL AUTH CENTRE' appears on the terminal, you should call the authorisation centre immediately so checks can be made that your customer is the genuine cardholder and they can supply you with an authorisation code. Never accept codes provided by customers.
3. **Split sales:** If a transaction declines for the full amount, do not split the total into smaller amounts, or spread it over several cards. Fraudsters are frequently unaware of the available balance of stolen cards and will ask you to try various amounts until they can get a transaction to go through.
4. **Mag stripe fallback transactions:** Be cautious if a customer says that the chip on their card doesn't work or that they have forgotten their PIN.
5. **Customer distraction:** A fraudster may attempt to distract you when they are entering their PIN, so they can enter a dummy auth code. Be wary of any customer who holds onto the terminal for longer than is necessary.
6. **Third party delivery addresses:** Take care when you are given an alternative delivery address. One option is to send a letter to the billing address requesting confirmation the order is genuine before it is dispatched. Or you can use sites such as 192.com and Google Streetview to verify customers and delivery addresses.
7. **Phishing calls:** If anyone calls your business saying that they're a terminal engineer or a card company and ask for details of the last few transactions you processed, do not give them any information. This is one way fraudsters get hold of card details, which they use to commit Cardholder Not Present, or CNP, fraud.

Chris Davies, Managing Director, Global Payments.

By ensuring both you and your staff are alert to these common frauds and working in partnership with your card processor, you will be able to better protect your business from these threats and their repercussions.

GLOBAL PAYMENTS
www.globalpaymentsinc.co.uk

Jordan launches enhanced GCMS

Jordan Media Ltd (JML) has launched version 2.5 (v2.5) of its unique Gift Card Management System (GCMS). Used under licence by leading retailers including Asda, the GCMS allows retailers to offer delayed activation and remote loading and reloading of gift cards sold into the corporate arena, where businesses are giving retail gift cards to staff and customers as a benefit, reward or incentive. Funds can be loaded onto gift cards remotely and at a time to suit the corporate user. This means business users can hold a stock of retailers' blank gift cards, and choose when to have them activated/loaded via the GCMS.