

www.volumatic.com/stolen-knowledge



Stolen Knowledge

Issue No 4

the Collaboration issue

Retail, banks and the police: why we need joined up action on crime against business

Just how much can you share?

Where the law stands on Data Protection



Solving the silo problem

The National Business Crime Forum and beyond...



Retailers:

Can they make collaboration a reality?





Collaboration: the retailers

Greggs' Bruce Duncan on the NBCS

p3



Be part of the solution

An interview with Jason Trigg,
CEO of Cardinal Group

p6



Business Crime: Asda

Claire Rushton gives us a
supermarket perspective

p7



Cybercrime:

the gaping hole in our defences

p8



Collaboration: banks

CIFAS, banking and identity fraud

p10



The NBCS

Paul Broadbent and Richard Stones
on ending silos

p11



Protecting data

Annabel O'Connor, Associate at
Charles Russell LLP, explains the law

p14

A word from our sponsor...

This edition of Stolen Knowledge is dedicated to the subject of collaboration and you will see from the articles within that we have a myriad of organisations in the UK committed to fighting business crime through collaboration.

The National Business Crime Forum and the National Business Crime Intelligence Bureau have spawned the National Business Crime Solution working alongside ACPO. Other intelligence units such as the TUFF database and the Business Community Intelligence Bureau together with local crime partnerships such as ABCP and MRCL, also get special mention. And there's the development of Regional Intelligence Units and the involvement of the British Oil Security Syndicate, FBI, BCC, CIFAS and the NFA Action Fraud service...

This daunting list of acronyms provides an insight into the amount of time and energy being devoted to collaborative initiatives within the arena of retail/business crime. However, this list, whilst including some of the most significant groups involved, doesn't really scratch the surface of the number of affiliations, associations and other bodies that exist to facilitate some form of collaboration to tackle retail crime.

Perhaps it is this very fragmentation that is part of the problem – is it possible that so many disparate collectives can be working effectively towards the same goal? Some might argue that if they are truly effective then why do so many exist?

It has sometimes seemed that it is the criminals who are the most effective collaborators when it comes to retail crime and sharing "best practice" and "intelligence"; but then again they don't have to navigate complex and developing legal frameworks when it comes to sharing data.

Retailers all want a world where business can be conducted safely and profitably, and I hope you find this edition thought provoking and interesting. It has certainly been a very collaborative effort putting it together!

James Harris

Commercial Director, Volumatic Ltd



Collaboration: the retailers

This issue of Stolen Knowledge is all about collaboration, 'joined up' action on crime against business in general, retail in particular. And where better place to start than with the retailers themselves? Bruce Duncan, Retail Loss Prevention Manager at Greggs, is one of a group of retailers who have taken the plunge and decided to share data about crime. We spoke to Bruce about his participation in the 'proof of concept' of this new initiative, the National Business Crime Solution.

The National Business Crime Solution is an initiative created jointly by the police and business in order to benefit from shared intelligence about crime. It's a major attempt to create unity out of what is currently a very fragmented scene nationally with over 250 crime partnerships and shop watch schemes, 43 police forces, industry associations and businesses often acting in isolation.

Retailers are known to be wary about collaboration. But now there are 20 or so 'believers' who have stepped up to the mark and are participating in a 'proof of concept' of the National Business Crime Solution (NBCS). Under the chair of Mick Phipps, Head of Security at Wilkinsons and Vice Chair Tim Edwards, Director of Security JD Sports, this group of retailers is now sharing its security data within the NBCS.

High Street bakery chain Greggs is one of the businesses taking part in the NBCS 'proof of concept'. Stolen Knowledge spoke to their Retail Loss Prevention Manager, Bruce Duncan, about it.

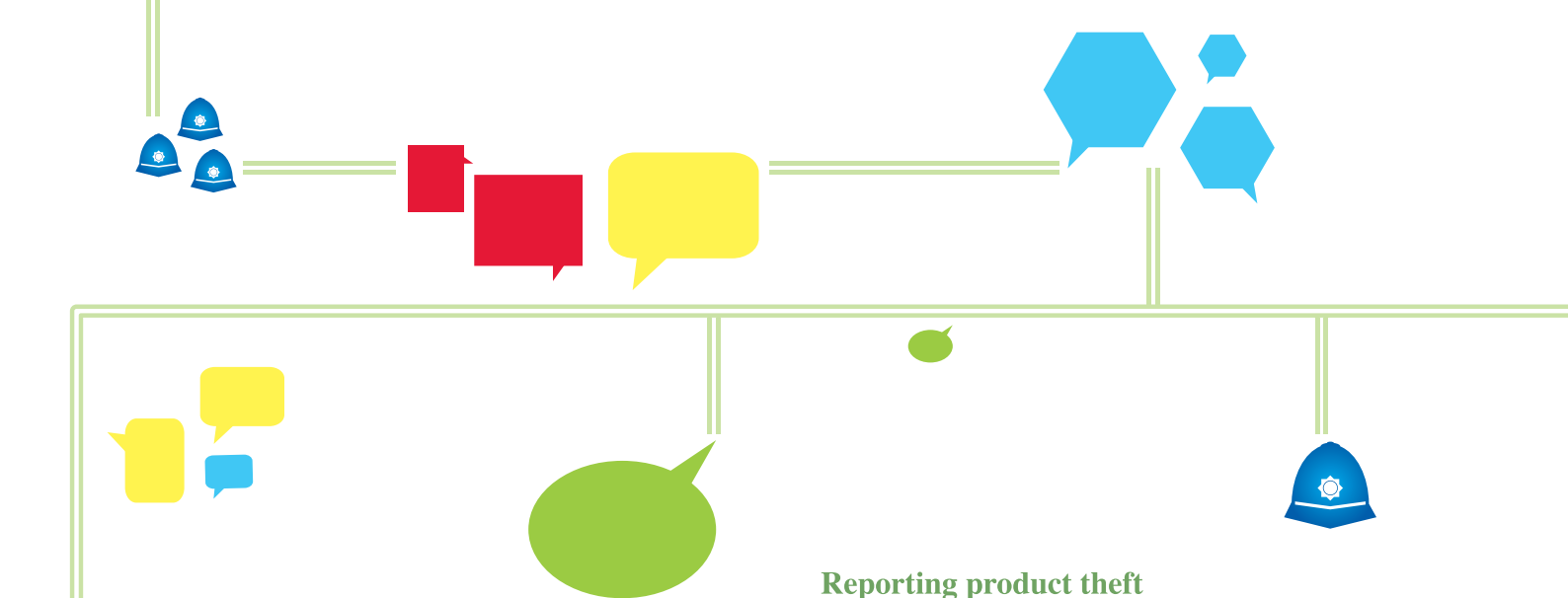
Can retailers overcome their reluctance to collaborate?

Bruce Duncan is hopeful. "Yes, retailers have been known to be nervous about collaboration. However, Cardinal's Jason Trigg has taken the initiative by identifying individuals who believe there is merit in taking part", he says.

"Some retailers are understandably hesitant, waiting to see how things go. Others, like myself, think this approach offers opportunities to use data more effectively", he continues. "My background is in accounting. When I was working as an accountant, information was always very protected. But working within loss prevention I believe there is a need, and an increasing willingness, to share data".

"Those in the High Street such as the Co-op and Wilkinsons are in this first wave of 20 retailers participating in this pilot." Bruce explains. "Some of the larger nationals will be watching to see the outcome".

Some retailers are understandably hesitant, waiting to see how things go. Others, like myself, think this approach offers opportunities to use data more effectively.



Retailers have contributed a sum to take part in the scheme, but the NBCS is not for profit. Those taking part form the executive committee, meeting periodically to review its effectiveness. "Relevant data sharing, data protection and confidentiality requirements were considered and signed off at the start. We have all signed a non-disclosure agreement", says Bruce.

How does crime affect Greggs?

"Like other retailers, within Greggs we're impacted by high street crime, i.e. product theft from our self-selectors in certain more vulnerable locations. We are improving our efforts to report it as a low level crime. For us, the theft of a sandwich is as serious as the theft of a leather jacket to another retailer", Bruce says. "Out of hours burglary is also an unfortunate reality of current times and represents a combination of organised crime and opportunists, which can often be more disruptive and demotivating due to collateral damage. However, proactive and reactive measures have enabled us to minimise the impact from this crime in higher risk areas. Thankfully robbery is very rare due to good cash controls and security vigilance by our shop teams".

NBCS... enables the information to be shared nationally; it also enables trends and patterns in low level crime to be identified, cumulatively.

Reporting product theft

"Previously not much could be done about product theft apart from reporting to the local 'bobby on the beat'. Now, details are able to be collated and uploaded on to the National Business Crime Solution database. This enables the information to be shared nationally; it also enables trends and patterns in low level crime to be identified, cumulatively.

"We are now hoping that a new approach of sharing that information through the appropriate channels/ protocols will help reduce theft for everyone..."

The increased ability to report smaller value thefts, offered by participation within the NBCS, is clearly important to tackling the issue. "It is this ability of the National Business Crime Intelligence Bureau to pre-package information that enables police to use information better with their diminishing resources and budgets. And it is able to give more weight to lower value thefts", Bruce says.

"From my informed conversations with police about the reporting of incidences of low level crime, their view is that by businesses collaborating and collating information, and communicating this information to the police they are better able to identify the severity of a trend and better able to deal with it as a shared problem to them and the retailers".

Reporting burglary/robbery

Reporting of more serious crime on the database has shown clear and immediate benefits to police and retailers. "We upload the details of every burglary/ robbery on to the NBCS database," Bruce explains. "This has a clear cross-border benefit, affording access to information to all relevant police forces. We already have examples of where this availability of information and collaboration has enabled police to identify the criminals and make arrests".

National Business Crime Solution

Key Facts

The National Business Crime Solution is a not for profit organisation. It works with the National Business Crime Forum and is about bridging the gap between police and business in order to combat crime against business.

Its goal is to create a national managed intelligence hub with police Regional Intelligence Units (RIUs) and police forces, retailers and business across the UK participating to provide the most up to date information for crime prevention and support.

The live information and intelligence-sharing platform it uses is already widely used to tackle retail crime in the USA.

The NBCS has adopted the police national intelligence framework of intelligence, prevention, and enforcement strands. Its intelligence arm is the National Business Crime Intelligence Bureau (formerly the BCIB) with 43 memorandums in place across all forces, relationships with SOCA and the national crime agency, and seconded police analysts.

Participating businesses enter business crime data into the central system and this information is then collated, analysed and disseminated to other participating business members locally, regionally, nationally or by sector.

The NBCS formal launch date is 1st April 2013.

How does the system work in practice?

Bruce explains: "Information from the NBCS database provides a national picture of trends and outbreaks of business/retail crime. It means we can put our shops on watch if necessary. We can pass the information to our operational management team who will make individual shops aware of a situation in their area. This is usually just a case of being on the alert, but it does provide us with the opportunity to implement extra measures if needed".

Information about business/retail is anonymised in the system. But what about sharing the identities of known individuals? "We are encouraged to upload images. These are not automatically shared but are sense checked by the NBCS database analysts to ensure that the sharing of an image is legitimate, legally permitted and of value", Bruce explains.

The proof of the pudding...

"Collaboration is the only way forward," Bruce believes, "but there needs to be greater cross working between retailers and the police, with retailers appreciating the challenges police face and police appreciating the impact of smaller thefts on retailers".

"This is not a free service, it costs retailers. So all participants are keenly aware that they will need to make a business case for its effectiveness at the end of this 'proof of concept', and that the value must justify the price". SK



Be part of the solution

Jason Trigg has been doing a lot of joined up thinking lately. The CEO of the Cardinal Group is the driving force behind the National Business Crime Solution.

In a world where business crime is becoming increasingly complex and sophisticated, Jason Trigg finds it self-evident that all interested players should unite in the fight against it. "For me the launch of the National Business Crime Forum was a defining moment", he says. "The future is all about collaboration and sharing information".

He believes that the police, business, the community, crime partnerships and shop watches must all work together.

"There is a resource gap at the moment," he says. "The National Business Crime Solution, working with the National Business Crime Forum, is about bridging the gap. It focuses on industry specific peer groups: they will facilitate the reporting and analysis of collective business crime data nationally through a managed service approach".



"To me, it is about a model with three strands: the technical underpinning, operational (at local, regional and national) and financial (for sustainability)".

The Retail 'proof of concept'

Retail has been the first industry specific peer group to take up the challenge – see our interview with Bruce Duncan about the 'proof of concept' on page 3. Jason: "We are getting good results through our acquisition of the BCIB, leading to action against perpetrators. We are also getting results for retailers who are not part of the initiative. But we are on a big learning curve and we need to manage expectations. The biggest expectations to manage have been my own! I wanted it to be a matter of 6 months but if I am honest it is a 12-18 month initiative.



Stolen Knowledge asked Claire Rushton, Operational Security Senior Manager at the UK's second largest supermarket chain, about collaboration against business crime.

Retailer reservations?

"A lot of retailers are on the fringe, watching. But if you don't put in, you don't get out, and we encourage all retailers to join regardless of their size/number of stores. We now have access to the police database and police analysts, which has answered some retailers' reservations about participation. Other retailers have questioned the cost of participation, but these costs cover the infrastructure, as this is not for profit. The investment is in time and commitment."

Other sectors

In the Logistics arena Truckpol have signed up to the managed service model and conversations are in advanced stages with several other business sectors to follow the retail model, Jason says. There's breaking news, too: "We are in discussions with



BOSS, the British Oil Security Syndicate, for a new collaboration around petrol forecourts".

Jason is well aware that it is a long road to gaining participation from all sectors and stakeholders: but he is up for the challenge. The NBCS is now in discussions with local crime partnership umbrella bodies such as the ABCP, MRCI and the NERCP. "We know the value they bring on the ground and we want to share that", he says. "We are in dialogue with the National Fraud Authority's Action Fraud service... It's about everyone working together". **Sk**

Collaboration: the view from Asda

In what ways does Asda work together with other agencies to counter business crime?

We take business crime very seriously and work with the police and community leaders to make sure we're getting our approach right in each area. Everyone in the team at Asda has police and community engagement at the forefront of their minds when it comes to this.

I also sit on the British Retail Consortium Head of Security group where we support the police business crime strategy.

In what ways you work together with other retailers?

We sit on other national and local business crime groups so we engage with other retailers wherever possible. From these meetings we develop relationships and so when we see crime trends we can pick the phone up to our peers and work together.

What is your view on recent initiatives such as the National Business Crime Solution?

The National Business Crime Solution, in principle is the right way to work. We already collate all our data so I'd want to work closely with them to make sure there isn't any duplication.

We are currently talking to the firm that runs our data reporting platform about how this could be done, potentially linking into the police and sharing data with other retailers who use the system.

We are lucky as we have built great relationships with the police and where there is an issue we can pick the phone up and take action. We also have a fully trained team of investigators who can work on areas such as pulling case information together. **Sk**

How high street stores pose a major security threat to online security

As retailers work to create watertight online systems they are ignoring a gaping hole in their defences.

Everyone is aware of the significant growth in online retailers' sales. Over the Christmas period growth of 38% was announced for Debenhams against a 5% growth in store, and there are other retailers with similar experiences.

However, there is another very significant threat to online retail operations. One that is easily overlooked. And, ironically, that threat starts with the very retailers who seek to have the most robust online systems...

Retailers becoming their own worst online enemies

With online now accounting for as much as 40% of some historically high-street orientated retailers' takings, it is easy to see that the move from bricks and mortar to clicks and mortar is a trend that is likely to continue for the foreseeable future.

And with this online growth comes increasing threats. Anyone in the retail loss prevention, financial and operational arenas will readily appreciate the importance of penetration testing of online systems. Much time and effort is expended trying to anticipate what a hacker or cracker might do in attempting to get into the site. By anticipating what they might try and do those with expertise in IT try to maximise the security of the site so that it can withstand such an attack unscathed.

The easiest way to fool an online system is to use its own information against itself. Many shops store customer data in hard copy formats for bona fide usage in delivering customer requirements. It needs to be realised that the acquisition by a dishonest party of seemingly valueless data may have serious consequences for the customer, the store, its brand and indeed other retailers.

Take for example a simple customer delivery form. Typically such forms will have the name and address of the customer on them. They will usually have the description of the goods being delivered as well as the price paid, possibly even reference to where they were served and by whom. This information in the hands of a fraudster is a licence to print money...

With a bit of simple investigative work and subterfuge it takes very little time for a fraudster to have all the

information that they need to commit crimes in the name of the innocent customer. By contacting the store, deliveries can be re-arranged or claims for goods allegedly lost in transit made. When the contact centre seeks to validate the authenticity of the request they will ask for various details – most of which of course the fraudster will have obtained from the printed delivery ticket generated by the retailer's own system!

However, the problem does not stop there. Having acquired the basic details of the customer a fraudster will then take the information acquired from one retailer and use it to open store cards, order goods and inflict losses on other retailers. So a retailer who was lax in keeping their offline information safe has actually allowed a fraudster to rob themselves as well as others on the high street.

Online/offline: an accident waiting to happen

Tony Sales, once branded Britain's greatest fraudster, now works with retailers showing them where their systems have weaknesses and helping them to fix them. "There is no question that retailers are not seeing the threat posed to their online business by acquisition of data from their offline businesses. I see it so, so often. This is true in a great many areas of crime, from refund fraud to financial services fraud. I see that there is a time-bomb ticking.

Sooner or later someone is going to get taken big time. And when the source of the fraudulently exploited data is traced back to them, it is not just the financial losses they will have to deal with but the major damage sustained by their brand. I can imagine some businesses would not be able to survive it", he comments.

What retail staff often see as unimportant materials can often be utilised by fraudsters to inflict significant loss. A folder containing 50 delivery notes is not a big deal. Or is it!?! To a fraudster that is worth probably £150,000, perhaps as much as £500,000 if the details relate to affluent customers. Because those materials are not seen as important then they are relatively unprotected and easy to get hold of as the material is not secured during trading hours or at night, when it is easier for an inside operative to take them, copy them and replace them.

Organised crime requires an organised response

So what to do? The answer is simple. Retailers need to put resources into securing their offline data to protect their profits and reputations. Attacks using offline data to defraud online systems are becoming big business. A well organised gang of fraudsters could easily inflict several million pounds worth of losses on one or two retailers over a period of a few weeks in this way.

What's more, when increased collaboration between retailers is becoming ever more important in the fight against organised crime, there also needs to be collaboration on the way in which customer detail is most effectively stored and potential abuses avoided. After all, it only takes one weak link in the retail chain to expose everybody to potential harm. **SK**

Mark Emmott

The rise and rise of ID fraud

UK fraud prevention service CIFAS was the world's first not-for-profit fraud prevention data sharing scheme, founded in 1988. It operates a data sharing service between financial institutions, with increasing participation from retail and other businesses impacted by ID fraud.

The fraudulent use of identity details (either those of an innocent victim or completely fictitious ones) is the biggest and most perturbing fraud threat, say CIFAS. 50% of all frauds identified during 2012 relate to the impersonation of an innocent victim, or the use of completely false identities.

“Fraud against retail, such as groups operating scams claiming back on high value electrical goods, frequently involves the use of compromised cards and identity details”

Furthermore, Facility (or Account) Takeover Fraud – where a fraudster gains access to and hijacks the running of an account (eg theft of security details through computer hacking, interception of post details, social engineering through popular websites) – rocketed by 53% compared with the previous year. This means that those frauds where the criminal requires identity details accounted for almost 2 in 3 (65%) of all frauds in 2012.

Sharing data on financial fraud

CIFAS is a 270 member organisation that shares confirmed fraud data and feeds this data into City of London Police's National Fraud Intelligence Bureau (NFIB). The majority of CIFAS Members are financial



institutions but, increasingly, organisations from other sectors are seeing the benefits of participating in this database.

“Fraud against retail, such as groups operating scams claiming back on high value electrical goods, frequently involves the use of compromised cards and identity details,” says Richard Hurley of CIFAS. Mobile phone providers frequently encounter forged documents and false details.

Using the data

The CIFAS database uses a system of warning flags and data is handled with care. When a member searches the CIFAS National Fraud Database they are made aware of a potential fraud by means of a flagged warning. The warning will contain details of the matched case or cases. The member, having been alerted to the risk of fraud, will then conduct an investigation. “Our data is not a blacklist, it must have the legal purpose of preventing fraud. A card cannot be refused just because it is flagged, but it does indicate the need for further investigation”.

Fraud awareness in-house

CIFAS is also increasingly working with businesses to prevent internal fraud. “It’s about driving and identifying best practice on fraud awareness and how data is treated,” Richard Hurley says. “The proliferation of online details brings an added responsibility to ensure data safety, and staff need to be upskilled to deal with it”. [SK](#)



Solving the ‘silo’ problem

Soaring retail crime figures, plus the news that only 1 in 8 shoplifting incidents are being reported*, do not paint a happy picture for retail loss prevention. Retailers complain that the police do not attend incidents, that they are slow and reluctant to help with shoplifting...

The police, in practice, must prioritise some forms of crime over others and they are working with limited resources. With a 15% cut in police budgets on the horizon, these resources are going to be even more stretched very soon.

Meanwhile, some commentators such as Professor Adrian Beck offer the controversial view that modern retailing is akin to putting the contents of your home on your front lawn and then blaming the police when it all gets stolen. Easy access to goods temptingly displayed increases the risk of crime, he believes.

The situation is made all the more poignant by the arrival of the newly elected PCCs on the scene, and the importance of retail crime being placed high on their agendas.

So how can the police do more with less - and how can retail and business help? Stolen Knowledge spoke to two senior police officers who have more than a passing interest in this question, Paul Broadbent and Richard Stones, through their roles in the National Business Crime Forum.

The National Business Crime Forum (NBCF) was launched in 2010 by the business community, including the Federation of Small Businesses (FSB) and the British Chamber of Commerce (BCC), to look at business crime in its widest context. It brings together business, the Police, Home Office, and key

business sector organisations to share intelligence and defence responses against business crime across the UK.

As the then ACPO lead on business crime, Nottinghamshire's Assistant Chief Constable Paul Broadbent worked closely with NBCF since its inception and strongly backs its role as an industry driven response to crime.

Inspector Richard Stones is one of the directors of the Forum: "As the police officer selected to be one of its directors I operate on a national basis as the staff officer to the business crime ACC, but funded via the NBCF to support police integration into their business driven crime reduction model".

Paul Broadbent





Business crime and the ‘silo’ problem

Paul Broadbent likens business crime to domestic abuse: “It is not a crime in itself but is made of different distinct crimes,” he says. It is this complexity which has meant that business crime has had no core focus nationally and made it so difficult to address.

“We have been dealing with these things in silos,” he continues. “There is a lot of intelligence in the retail community which is relevant. Banking has a network of intelligence which it could share. We need to break down these silos, share information. This is the purpose of the National Business Crime Forum”.

Richard Stones echoes this: “There is a lot going on but it is often isolated. National retailers are exposed to a cross section of local groups. In the interests of uniformity, Paul started the initiative for a common standard for Town Centre groups. There is a host of these, such as Shopwatch groups, all protective of their own positions. Furthermore, reputation issues cause many retailers to use the civil remedy which may be inconsistent for dealing with crime”.

Ethical considerations prevent police from becoming too close to retailers. So the police have greatly welcomed recent developments at the initiative of business, Broadbent says. This includes the Business Crime Intelligence Bureau, supported and funded by businesses such as Homebase and Argos, which focused specifically on intelligence and networking nationally.

The solution?

More recently, the National Business Crime Solution is an attempt to join up the private and public dots. It builds on the work of the NBCF and the

National Business Crime Intelligence Bureau (NBCIB) and indeed has just subsumed the latter. “It is a public and private collaborative model. A closed group of analysts can tease out golden nuggets of intelligence,” Paul Broadbent says. “We are very keen to stimulate and encourage intelligence sharing. If some organisations are trying to fill a space then this is great”. He highlights the role of security firm Cardinal in ‘taking a leap of faith... now others are coming on board”.

“In real terms police only hold a small amount of intelligence. We are not the sole answer to reducing crime. And we are not just the last line of defence. We are getting upstream, becoming involved in prevention, store layout, intelligence”.

There is the perception, backed by the recent British Retail Consortium survey, that smaller crimes are falling off the radar... Paul Broadbent characterises the police response: “Police should assess response based on threat and risk. If a shop assistant is being assaulted this requires an immediate response. If a fuel station reports 20 drive offs this is something where we would be expecting them to implement better checks”.

Working smarter

It seems there is no getting round the fact there has to be an acceptance that resources are limited. However, ‘working smarter’ has to be the watchword here. Nottinghamshire is seeing its lowest crime rates for 35 years. “The highest reduction has been over the last three years. Business crime is 35/40 per cent of that figure”, Paul Broadbent points out. This has been set against unprecedented budget cuts of 20 per cent and a similar reduction in officers and staff.

There is a lot of intelligence in the retail community which is relevant. Banking has a network of intelligence which it could share. We need to break down these silos, share information.

internal theft is a greater threat to retailers than external theft

The Police's job has been to protect life and property since 1929, Inspector Stones says, so they are not about to duck their responsibilities any time soon. However he acknowledges that "Some retailers' layouts lend themselves to opportunistic crime. We are developing expertise to 'design out crime'".

He also points out that internal theft is a greater problem to retailers than external theft, and highlights the TUFF database used by mobile phone companies to share information on staff who have been dismissed due to theft.

The work to collaborate with business and retail continues. 'We are working on bringing a national standard to the accreditation of guarding companies. As it stands, the Chief Constable's accreditation is only operative within local region. Silos have got to be history" says Paul Broadbent.

The biggest national threat to business

Some say that cybercrime represents the biggest danger to business nationally. It has been identified in the National Security Risk Assessment as a 'tier one' threat alongside international terrorism, an international military crisis, and a major accident or natural hazard requiring a national response.

"The biggest threat to business is the changing dynamic: it requires a change of mindset", Richard Stones points out. In response to the growing threat of cybercrime the government launched three

regional policing e-crime hubs last year, working alongside the Metropolitan Police Centre E-crime Unit.

The changing face of organised crime

At local level the face of crime is forever changing: "Stealing to eat' is an emerging trend," says Richard Stones, "Chunks of meat are being stolen to eat, rather than to sell for drugs".

Richard Stones



Paul Broadbent is now retired from the Police Force but continues the fight against crime in his new role as Chief Executive of the Gang Masters Licensing Authority. "Organised crime is a major threat", he says, "manifesting it locally with new variants", these include the theft of chewing gum (yes, chewing gum) which is taken to Eastern Europe. The theft of metal continues to be a problem although new legislation has helped. But the most esoteric must be the theft of rhino horn from museums and stately homes, which fetches £60,000, kilo for its health giving and aphrodisiac effects...

"It is organised gangs who destroy the bottom line," concludes Paul Broadbent. "Collaboration is the only way forward. We want business to conduct its business without organised crime stripping its profit margins". ^{Sk}

*BRC Retail Crime Survey 2012



Just how much information can you share?

*All retailers have sophisticated risk management mechanisms, including theft prevention. Many are now considering the benefits of sharing personal information about criminals to aid prevention and detection. What information can retailers share with each other and still comply with the law? **Annabel O'Connor**, who is an Associate at Charles Russell LLP, offers this guide.*



The Law

The Data Protection Act 1998 (DPA) governs the collection and use of personal data by organisations in the UK. Personal data is data which can identify a living individual and includes names, addresses and images.

Organisations must process personal data in accordance with the eight data protection principles (Principles) set out in the DPA:

1 Personal data shall be processed fairly and lawfully and, in particular, not processed unless certain conditions are met, these include where an organisation has a legitimate reason for processing the data.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data shall be processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subject under the Act.

7 Appropriate measures must be taken to protect the personal data.

8 Personal data shall not be transferred outside the EU.

“Processing” of personal data means obtaining, recording or holding of the information or carrying out any operations on the information. This includes sharing it with other organisations.

Sharing personal information

There is no prohibition under the DPA that completely bans the sharing of personal data, including CCTV images, but all sharing between organisations must be done in



accordance with the DPA. Sharing personal data does not take away from the duty to process personal data fairly, so when a retailer is considering sharing data they should think about how they can share the data while still complying with the DPA.

In order to comply with the Principles and process and share data fairly retailers should ensure the following:

That they have legitimate grounds for sharing the personal data. Theft prevention and loss of profit would be considered legitimate concerns for retailers, but these should be balanced with the rights of individuals. Retailers may also be able to take advantage of an exemption under the DPA relating to crime prevention and detection.

That they are transparent in their intention to share it. Retailers should make individuals aware that they intend to share personal data of people who are apprehended shoplifting in their stores and what it is then going to be used for. This could be facilitated by updating shoplifting warning signs and informing individuals when apprehended. This is in addition to other privacy notices that retailers should have in place, for example CCTV notices. These notices need to be prominently displayed, not hidden away to “tick a compliance box”.

That they don’t use the data in such a way that it has an unjustifiable negative effect on the individual (for example, an individual’s reputation).

That they don’t share excessive or irrelevant information about people. Only share the information that is necessary for the specific purpose, namely the prevention of theft.

The information they are sharing is accurate. This is particularly important when sharing images captured on CCTV. Captured images vary widely in quality and a retailer should be sure that they are identifying the correct individual.

That access is only granted to the shared personal data on a “need to know” basis. Only relevant staff at the retailers should have access to the shared information, it should not be spread to widely.

Retailers should make sure that whoever they’re sharing the data with has adequate information systems and security in place to protect the personal data once it is in their possession. A formal data sharing agreement should also be put in place which should document the reasons for sharing, the data to be shared, data quality, data security and individuals’ rights.

Could this be extended to individuals who are only suspected of wrong doing?

Retailers should be very wary about extending data sharing to individuals against whom there is no proof of actual wrong doing. If an individual was innocent the data held for them would not be accurate and therefore in breach of the Principles. There would also be no legitimate reason for the retailer to share their personal data and therefore they would be in breach of the DPA. If a retailer decided to proceed with sharing data on suspected individuals there should be mechanisms under which the individual can challenge the decision and have their data removed from any shared database.

The risks/consequences of breach

There are significant risks if a retailer shares information in breach of the DPA:

The Information Commissioner’s Office can levy substantial fines and there is the potential for criminal prosecutions.

Individuals are entitled to compensation from data controllers for damage caused by any breach of the DPA; damages are likely to be higher if a person’s reputation has been tarnished.

There are also considerations outside the DPA:

Libel: If an individual was wrongly accused by a retailer, and then had their details shared, and suffered reputational damage the retailer could also be exposed to libel claims.

Reputational damage for the retailer: Data protection cases attract a lot of media attention, as do libel claims, a retailer would have to carefully consider the balance between the risk to their reputation and the benefit they would receive from the information shared.

Final thought

Whilst there is no outright statutory bar to retailers sharing information between themselves on criminal behaviour, they should always tread with care when sharing personal information about individuals. This is particularly true where there is no evidence of wrong-doing on the part of the individual. Appropriate safeguards must be put in place to protect the rights of individuals, this in turn will help to protect the retailer against any unwanted outcomes. Tread extremely carefully or not at all! **SK**

HELLO DUBLIN..

RETAIL KNOWLEDGE LTD
**RETAIL
FRAUD**

ON THE ROAD

..IT'S SHOWTIME!

The definitive event for all aspects of physical and technological fraud prevention within the retail environment

The Shelbourne, Dublin 18th July 2013

For delegate information or to discuss exhibitor/sponsor opportunities,
call Paul Bessant on **0207 1003 999** or email paul@retail-knowledge.com

MAKE SURE TO JOIN VOLUMATIC ON THEIR STAND AT DUBLIN