

# Future Online Security: Tackling eCrime and Fraud



# DEFINITION OF ECRIME

***The use of networked computers or internet technology to commit or facilitate the commission of crime.***

Source:ACPO (Association of Chief Police Officers)

## OVERVIEW

The growth of e-commerce and corresponding opportunities for increasing fraudulent behaviour should not be underestimated. Retailers need to be sure that as they seek to expand their businesses via e-commerce the customers they attract will be well protected. Retailers invest significant resources in protecting their customers. But too often, the current law enforcement response to eCrime and fraud is inadequate. The BRC is calling for a dedicated national unit tasked to investigate and respond to the increasing levels of eCrime.

Engagement between the private sector and law enforcement agencies should be focused on finding the most effective way to achieve a better response to eCrime and fraud. The focus must be on finding ways in which the public and private sectors can work more effectively together to reduce the level of offending and to raise consumer confidence.

The value of internet retailing in 2009 was £18.5 billion. The value for 2010 to date (January to the end of October 2010) was £17 billion. This was a 21 per cent increase when compared to the same period in 2009.

The BRC has undertaken this study to ensure that this important growth area of the economy is adequately policed and protected.



# RECOMMENDATIONS

## 1. IMPROVE LAW ENFORCEMENT COMMUNICATION

Communication between law enforcement agencies and retailers should be improved so that each is clear about the evidence that is needed to support a successful investigation. Frequently law enforcement agencies waste time and resources by unnecessarily conducting investigative work which has already been undertaken by the retailer. If there was an agreed standard for acceptance this would minimise confusion and save time and resources.

## 2. CLEARLY DEFINE LAW ENFORCEMENT RESPONSIBILITIES

There needs to be more comprehensive information about which law enforcement agencies have responsibility for eCrime and online fraud, and the extent of those responsibilities. Such information should identify overlaps and intelligence gaps. There should also be greater transparency about the case acceptance criteria for each of these agencies. If offences do not reach the acceptance criteria and therefore need to be reported locally then it is vital that local operational capacity is available to progress an investigation adequately.

## 3. MAKE EFFECTIVE USE OF INTELLIGENCE

The National Fraud Intelligence Bureau should work with third party screening companies to enable more effective use of intelligence. Members of the BRC have reported that attempted fraud is as high as a third of all transactions. There is a wealth of intelligence held by third party screening companies which could prevent offences occurring by enabling action before an offence is committed. This would reduce the number of victims and help provide reassurance to the public that they are being fully protected, which would in turn support the further development of this increasingly important retail channel.

### 4. UNDERTAKE A NATIONAL THREAT ASSESSMENT

There should be a National Threat Assessment on Online Shopping. In preparation for the introduction of locally elected commissioners, this assessment would need to identify clearly the impact that these offences have on customers and, consequently, the economy. It would also be useful to provide any available case studies linking eCrime with Serious and Organised Crimes and crime groups. This will help to identify the extent of the need for an economic crime capability as part of the new National Crime Agency.

### 5. COMMUNICATE WITH BANKS/CARD ISSUERS

There needs to be better communication and information exchanged between the bank and card issuers, and retailers. There are three key issues that retailers would like to see addressed:

1. When a card is reported as lost or stolen it is flagged by the bank to the retailer immediately. However, if the card is used fraudulently, it often takes time before the retailer is made aware. The same flagging system should, therefore, be adopted for notification of fraudulent transactions.
2. When a retailer prevents fraud, it would be beneficial if there was an effective facility in place which would enable the genuine card holder to be notified immediately. This would prevent further fraud occurring against the customer and at other merchants.
3. There needs to be greater transparency of data provided by the banks to the retailers relating to Card Not Present transactions, detailing how retailers are managing their fraud to turnover ratio. This information can then be passed on to third party screening companies to tailor their fraud screening accordingly.

### 6. IDENTIFY EFFECTIVE PRACTICE

The BRC should develop good practice guidance to enable retailers to reduce incidents of internal fraud and to increase the understanding of how to best protect consumers.



# IMPORTANCE OF ONLINE RETAILING

Online sales are now a crucial element of many retailers' commercial models. Customers are becoming increasingly accustomed to internet shopping; a recent Verdict report indicated that the total online shopping population grew by 6.7 per cent in 2009, with 28.5 million adults now shopping online. The impact of this shift is reflected in sales – online sales currently account for around 7 per cent of total retail sales. This figure is expected to grow by around 10 per cent annually. Needless to say, the commercial value of this activity is also very significant - the value of internet retailing in 2009 was £18.5 billion. The value for 2010 to date (January to the end of October 2010) was £17 billion. This was a 21 per cent increase when compared to the same period in 2009.

The outlook for the future looks similarly optimistic. If recent levels of growth continue for the remainder of the year, the value of internet retailing for 2010 could exceed £20 billion per annum. It is expected that over the next few years online spending will equate to 10 per cent of total retail sales. The value of internet retailing is, therefore, likely to reach over £30 billion at some point in the next 5 years. The potential for growth is underlined by the range of large retailers, such as Gap, Zara and H&M, that have introduced transactional websites in the last few months. Looking at the top 50 retailers in the UK, over 70 per cent of them now trade online. There are also increasing numbers of retailers who choose to trade exclusively online or via mail order.

However, as e-commerce is evolving rapidly, there is unfortunately an inevitably greater exposure to the accompanying evolving threats and risks. Online retailing is the future for many businesses and increasingly important to the economy. But to enable e-commerce to reach its full potential it is essential that consumer confidence is supported and enhanced.

Despite the significant growth in online selling, a study published by the Office of Fair Trading in 2009 highlighted that one in three internet users do not shop online. The most commonly identified reason for shoppers opting not to use the internet was a lack of trust in its security.

In January 2010, the National Fraud Authority published the first ever National Fraud Indicator. The indicator estimated that in 2008 alone, fraud had cost the UK £30 billion. Based on the direct cost of fraud within the UK combined with the indirect costs on products and services this equated to a cost of £621 to each adult in the UK. It illustrated

## Future Online Security:Tackling eCrime and Fraud

that fraud was costing the private sector £9.3 billion. Retail, Wholesale and Distribution made up £544 million of this figure. Due to under-reporting of offences and a high investment in anti-fraud protection systems by retailers this is likely to be a gross underestimate of the extent of offences against retailers and their customers.

Unfortunately the majority of offences against retailers will involve a customer who has become a victim of identity/card crime. Feedback from customers likens the trauma of identity theft to being a victim of a burglary. We are concerned that the fear of identity and online offences leads to poor consumer confidence and therefore threatens economic development and the efficient delivery of public services. A study in 2009 by Cybersource, a third party screening provider, showed that nearly a quarter of consumers (24 per cent) believed that retailers were primarily responsible for making online shopping safe.

According to the latest Annual Retail Crime Survey published by the BRC in January 2010, 76 per cent of retailers reported that fraud had increased over the past 12 months. A high percentage (64 per cent) considered that identity fraud was increasing. The survey found that the majority of such offences were attributable to customers seeking fraudulent refunds, with Card Not Present (CNP) transactions the next most important category (33.8 per cent). CNP fraud relates to transactions where neither the card nor the card holder was present at the point of sale, e.g. orders by mail, telephone, fax or internet.

Retailers invest heavily in anti-fraud systems and are continually seeking ways to safeguard themselves and their customers. One retailer who uses the services of a third party screening company reports that for every £100,000 online orders a further £30,000 of online transactions are fraudulently attempted. Another retailer estimates that up to 20 per cent of their total web sales would be fraudulent if they did not have anti-fraud systems. There is a wealth of intelligence held by third party screening companies that could be used more effectively for the prevention of crime and detection of serious and organised crime groups. By more effectively utilising this intelligence we could prevent customers and smaller businesses less capable of protecting themselves from becoming victims of increasing eCrime and fraud.

As fraudsters become more sophisticated and adapt the way that they conduct their business, retailers will need constantly to review and update their fraud prevention systems.



The cost of fraud prevention is vast, particularly when this is combined with loss of goods and damage to consumer confidence and the resulting loss of business due to fears of online fraud. Retailers have little choice but to reflect this cost in the prices of the goods they sell.

# IMPACT OF ECRIME/FRAUD ON THE RETAIL SECTOR

Retailers' significant investment in effective fraud prevention systems helps to ensure that the impact of rising eCrime is not as significant as it would be without adequate fraud protection. Nevertheless any offence involving customers, most notably card not present offences and identity offences such as account or store card hijack, can have a potentially devastating impact on retail businesses where brand reputation and retaining consumer confidence are paramount.

## COSTS OF SCREENING

Retailers use a broad range of fraud protection systems to deal with the associated challenges. These include third party screening companies, such as The 3rd Man, Cybersource and Retail Decisions. In addition external reference and verification checks are conducted by companies such as 192.com and Experian. Some retailers have reported that third party screening costs approximately 7 pence per transaction. Retailers also invest heavily in internal fraud prevention such as manual checking processes and fraud investigation teams. Some retailers have reported that without adequate screening they would potentially lose up to a third of their sales revenue to online fraud.

Of course fraud prevention systems must be employed sensitively to ensure that good customers are not turned away by over zealous fraud prevention criteria. This is inevitably a difficult balance to strike and many retailers are aware that they lose substantial 'good business' as a result. One retailer has estimated that they lose up to £2 million of sales per annum by rejecting legitimate customers.

## LOST REVENUE/GOODS

Although in the vast majority of offences customers will be protected under the banking code and, therefore, will not suffer a financial loss, the retailer is not reimbursed for the loss of goods. One retailer has reported that in 2009/2010 they lost £252,000 to fraud. This was in addition to £3.6 million of attempted fraud.

Retailers are also required to keep fraudulent transactions below one per cent of turnover to avoid sanctions from their acquiring banks. 3D Secure (e.g. Verified by Visa and MasterCard SecureCode), which prompts customers using these cards online to provide

additional password verification, has enabled retailers to protect themselves by avoiding charge backs from the banks. However, this has meant that other types of distance selling, for example telephone sales, have become particularly vulnerable as this sort of fraud protection is not available and the retailer is therefore responsible for the associated chargeback. Despite manual checks, one retailer reports that they potentially lose around £400,000 per annum as a result.

Refund frauds are also common and can lead to significant losses for retailers. These frauds can occur in a number of ways but most commonly involve fraudsters either denying receipt of the goods or returning different goods than those dispatched. These are particularly difficult for the retailer as it is not always easy to prove where in the distribution of the goods the loss has occurred. Retailers are, however, working closely together through the BRC's eCrime Working Group to identify good practice on reducing and avoiding such offences.

## IDENTITY OFFENCES – UNDERMINING CONSUMER CONFIDENCE

Impersonation attempts on store cards have reportedly increased significantly in recent years. In such cases, the fraudster has obtained very detailed information about the victim and is, therefore, able to apply for a store card using all the correct details of the individual at their current address but then manages to intercept the goods in the course of their delivery. This is usually done by changing the delivery address after the order has been placed or opting to collect the goods from in store. One retailer reports that this has cost £420,000 in a single year.

CIFAS, the UK's Fraud Prevention service, recently found that during the first nine months of 2009 the number of identity frauds increased by 33 per cent. This included both identity fraud, where criminals use a stolen identity to obtain goods or services by deception, and account takeovers, where a person hijacks an existing account. When comparing the first nine months of 2009 to 2007 account takeovers were found to have increased by 238 per cent.



CIFAS compared the first nine months of 2009 with the same period in 2008 and found that there had been a 36 per cent increase in the number of victims of impersonation. This is a trend likely to continue as more consumers are finding it increasingly difficult to access credit.

The National Fraud Authority (NFA) recently estimated that every year in the UK identity fraud costs more than £2.7 billion and affects over 1.8 million people. The first ever UK ID Crime Strategic Threat Assessment completed by the NFA and National Fraud Intelligence Bureau found that on average fraudsters gain over £1,000 from every stolen identity.

CIFAS has stated that in cases where a customer's account has been completely taken over by a fraudster, this can involve around 20-30 different organisations. It may subsequently take the victim over 200 hours and cost up to £8,000 before things return to normal. They may suffer considerable (albeit temporary) damage to their credit status, which can affect their ability to obtain finance or insurance. Indeed, even a mortgage may be temporarily compromised.

### TRIANGULATION FRAUD - CASE STUDY

Several BRC members recently reported incidents of triangulation fraud. This is where:

1. The fraudster opens a credit account online via identity theft from a creditworthy citizen.
2. The fraudster offers goods for sale on an online auction site. Photos of the product are taken from the retailer's website. The goods are advertised below the usual retail price.
3. Payment for the goods is received via PayPal.
4. The customer orders goods from an online auction site. The fraudster then places an order for the goods with the retailer and requests delivery to the customer's address.

The customer who has ordered the goods from the online auction site is unaware that a fraud has occurred. The retailer only becomes aware when the customer who has had their account hijacked complains on receiving their statement. The fraudster gains time to continue to operate the fraud.

The fraudster is able to evade fraud detection systems by ordering goods not normally associated with fraud and which retailers' have identified as a risk factor, for example household goods rather than electrical goods.

It is absolutely essential that action is taken against those who abuse the reputation of good customers and who threaten to undermine the confidence of consumers, thereby adversely affecting the growth of e-commerce.

# RETAIL CONCERNS

Retailers are concerned that the law enforcement community has failed to keep pace with the rapidly expanding threat of eCrime and fraud. Despite the emergence of the National Fraud Intelligence Bureau (NFIB) and Police Central eCrime Unit (PCeU) many retailers report a persistent lack of willingness from law enforcement agencies to pursue cases involving eCrime and fraud. This situation may be exacerbated by diminishing police resources and the introduction of locally elected police commissioners who may consider business crime a low priority.

The BRC has highlighted concern previously at the absence of consistent collaboration on cross border criminal activity. We are, therefore, reassured to see that locally elected commissioners will have a strong duty to collaborate to tackle cross border, national and international crimes. We retain concerns, however, that it will be challenging to balance the duty to respond to issues which affect the community with the demands of tackling serious and organised criminal offences such as eCrime and fraud. The lack of effective measures for these offences will make it very difficult to justify taking action against offenders who are not widely perceived to be directly impacting the local community. This will be especially relevant to eCrime offences which are extremely difficult to quantify and quite often involve several different geographic locations, for example where the retailer is based, where the goods were dispatched to and where the credit or debit card used to commit the fraud is registered.

Despite the existence of various law enforcement agencies with responsibility for eCrime and fraud, including the Serious Fraud Office, Serious and Organised Crime Agency, City of London Police (NFIB), Metropolitan Police (PCeU), there does not appear to be genuine co-ordination or oversight of the work being undertaken by these units to tackle eCrime. Consequently, it is inevitable that opportunities to share valuable intelligence are therefore being lost.

The picture is complicated by the fact that offences that retailers report frequently fall outside the criteria for action of the agencies mentioned above and retailers are therefore expected to report these offences to their local police force. At the same time, retailers are often met by an unwillingness on the part of local police to pursue these cases. There is a lack of adequate resource or expertise at the local force level to deal effectively with offences such as fraud and eCrime.



## FUTURE CHALLENGES

Many retailers are beginning to expand their businesses via e-commerce, increasing their customer base and the range of countries in which they trade. Retailers, therefore, need to ensure that they are aware of the specific threats that may arise from trading in different countries whilst also ensuring that their fraud protection systems are continually improved as fraudsters become increasingly sophisticated.

The challenge for retailers is to ensure that they are well protected and that their protection is robust enough to ensure that they do not lose legitimate customers either via too stringent security checks or by making the process too burdensome with the result that customers are put off buying goods online.

## MOBILE PAYMENTS

Research by Verdict and Ovum projected that internet shopping sales from mobile phones would more than double by 2013. Verdict estimates that, in 2009, internet shopping via mobiles ('m-commerce') was worth £122.9 million. Using Verdict's figure of £21.2 billion of sales generated via online spending, this equates to just 0.6 per cent. The research estimated that by 2013 internet sales via mobile phones will have doubled to £275 million. This will have been driven by a doubling (119 per cent rise) in the m-commerce population, improvements in technology, enhanced interoperability and greater take-up of devices enabling this technology.

IDC Retail Insights recently conducted a study which found that nearly 30 per cent of European online shoppers are using, or plan to use, mobile devices for some kind of e-commerce over the coming year (2010–2011). The survey also found that 10 per cent of consumers were already using mobile devices or smart phones for retail research, price comparison or online purchasing. Another 20 per cent planned to do so in the future.

The shift towards m-commerce will undoubtedly bring a number of challenges for the retail sector. The balance between flexibility for consumers versus protecting consumers and brands will become increasingly complex.

Some industry observers predict that mobile payments may be the next big thing, and fraudsters will certainly be looking to exploit this new channel, but until adoption increases it is too early to tell exactly where the risk lies for merchants. What is clear, however, is that retailers will have to become increasingly aware of the end-to-end process involved in m-commerce and understand exactly where the risks and liability lie for any fraud that is carried out.

### CLOUD COMPUTING

Cloud computing is internet-based computing, whereby shared resources, software and information are provided to computers and other devices on demand, in a manner that has been compared to the electricity grid. Cloud services are provided to the customer over a network on a leased basis, creating the ability to adjust the size and level of service as the customer requires. It is highly likely that developments in data storage will lead to an increase in users of cloud computing.

Cloud computing offers flexibility, accessibility, transfers responsibility for backup and upgrades to the host and is infinitely scalable. IT operations are outsourced to the cloud. However, the risk is not. Accountability for customer and business sensitive data resides with the cloud customer.

There are concerns relating to corruption of customer data when hosting data in multi-tenanted centres. The large number of third parties involved in the data cloud means that organisations and individuals are exposed to fraud through their use, directly or indirectly, of cloud storage. There is currently a lack of accepted cloud computing standards. This will make it increasingly difficult to comply with data security standards (PCI DSS). Risk assessment and assurance activities are likely to be more complex, time consuming and costly.

On a positive note, however, the use of a central storage area will enable increased connectivity between datasets enabling greater data matching and verification. This will support enhanced detection and prevention of fraud.



## ABOUT THE BRC

The British Retail Consortium (BRC) is the lead trade association for the retail sector representing the whole range of retailers, from small independent stores through to the large multiples and department stores, selling a wide selection of products through centre of town, out of town, rural and virtual stores.

Retail is at the heart of local communities, employing close to three million people across the country and providing important local goods and services to consumers. The sector is an essential contributor to economic growth and to the regeneration of areas affected by crime and disorder.

# GLOSSARY

192.com	Online Directory Service	<a href="http://www.192.com">http://www.192.com</a>
Action Fraud	The UK's National Fraud Reporting Centre (run by the NFA)	<a href="http://www.actionfraud.org.uk/">http://www.actionfraud.org.uk/</a>
ACPO (Association of Chief Police Officers)	ACPO eCrime Strategy	<a href="http://www.met.police.uk/pceu/documents/ACPOecrimestrategy.pdf">http://www.met.police.uk/pceu/documents/ACPOecrimestrategy.pdf</a>
CIFAS	UK's Fraud Prevention Service	<a href="http://www.cifas.org.uk/">http://www.cifas.org.uk/</a>
Cloud Computing	Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid	
CyberSource	e-Commerce Payment Management Company	<a href="http://www.cybersource.co.uk">http://www.cybersource.co.uk</a>  UK Online Fraud Report 2010 <a href="http://forms.cybersource.com/forms/FraudReport2010UKCYBSwww260110">http://forms.cybersource.com/forms/FraudReport2010UKCYBSwww260110</a>
eCrime	The use of networked computers or Internet technology to commit or facilitate the commission of crime	
Experian	Global information services company	<a href="http://www.experian.co.uk">http://www.experian.co.uk</a>
Fraud	An act of deception intended for personal gain or to cause a loss to another party	
Get Safe Online	Get Safe Online is a joint initiative between the Government, SOCA, public and private sector. It helps individuals and smaller businesses protect themselves against internet security risks and threats	<a href="http://www.getsafeonline.org/">http://www.getsafeonline.org/</a>
IDC Retail Insights	A worldwide advisory service and market research firm specialising in retail	
MasterCard SecureCode	Private code issued to customers to protect them when shopping online at participating retailers	<a href="http://www.mastercard.com/us/personal/en/cardholderservices/securecode/index.html">http://www.mastercard.com/us/personal/en/cardholderservices/securecode/index.html</a>
National Crime Agency	A proposed national law enforcement agency in the United Kingdom, serving as a replacement for the existing Serious Organised Crime Agency. The new agency will be launched by 2013 and will lead the fight against organised crime, protect our borders and provide services best delivered at national level	

## Future Online Security:Tackling eCrime and Fraud

National Fraud Authority (NFA)	The government agency co-ordinating the counter-fraud response in the UK	<a href="http://www.attorneygeneral.gov.uk/nfa/Pages/default.aspx">http://www.attorneygeneral.gov.uk/nfa/Pages/default.aspx</a>
National Fraud Intelligence Bureau (NFIB)	Government funded initiative run by the City of London Police. Collects and analyses reports of fraud sharing the findings with law enforcement agencies	<a href="http://www.nfib.police.uk">http://www.nfib.police.uk</a>
National Threat Assessment	Assesses the threats posed to the UK by organised criminals and considers how these threats may develop	
Ovum	Provides research and advice on the commercial impact of technology and market changes in telecoms, software and IT services	<a href="http://www.ovumkc.com">http://www.ovumkc.com</a>
PCI-DSS	Data Security Standard to enhance payment card data security	<a href="https://www.pcisecuritystandards.org/security_standards/index.php">https://www.pcisecuritystandards.org/security_standards/index.php</a>
Police Central eCrime Unit (PCeU)	Part of the Specialist Crime Directorate of the Metropolitan Police Service. National unit tasked to combat eCrime and centralise the efforts of all police forces in the UK (excluding Scotland) to fight all forms of eCrime	<a href="http://www.met.police.uk/pceu">http://www.met.police.uk/pceu</a>
Retail Decisions	Specialist in card fraud prevention and payment processing	<a href="http://www.redplc.com/red6.asp">http://www.redplc.com/red6.asp</a>
Serious Fraud Office (SFO)	Independant Government department that investigates and prosecutes serious or complex fraud, and corruption	<a href="http://www.sfo.gov.uk">http://www.sfo.gov.uk</a>
SOCA	Serious and Organised Crime Agency	<a href="http://www.soca.gov.uk/">http://www.soca.gov.uk/</a>  UK Threat Assessment 2009/10 <a href="http://www.soca.gov.uk/threats/identity-crime">http://www.soca.gov.uk/threats/identity-crime</a>
The 3rd Man	Specialist CNP (card not present) Fraud Screening Company	<a href="http://www.the3rdman.co.uk/">http://www.the3rdman.co.uk/</a>
Verified by Visa	Password-protected identity-checking service which verifies the legitimacy of both parties in an online transaction	<a href="http://www.visaeurope.com/en/businesses__retailers/retailers_and_merchants/security/handling_visa_payments/card-not-present_sales/verified_by_visa.aspx">http://www.visaeurope.com/en/businesses__retailers/retailers_and_merchants/security/handling_visa_payments/card-not-present_sales/verified_by_visa.aspx</a>
Verdict	Conducts research and analysis into retailing	<a href="http://www.verdict.co.uk/index.htm">http://www.verdict.co.uk/index.htm</a>

**BRITISH RETAIL CONSORTIUM**  
for successful and responsible retailing

A close-up photograph of a person's hands typing on a silver laptop keyboard. A blue credit card is held in the person's right hand, positioned over the keyboard. The background is a soft, out-of-focus beige color.

**www.brc.org.uk**

For further information please contact:  
Catherine Bowen  
British Retail Consortium  
21 Dartmouth Street  
Westminster  
London  
SW1H 9BP  
020 7854 8925  
catherine.bowen@brc.org.uk

Published: December 2010

[www.brc.org.uk](http://www.brc.org.uk)