



## Dealing With The Perpetrators Of Fraud

At a recent SWFF seminar on fraud hosted in conjunction with law firm Bevan Brittan LLP, the subject for discussion was how to deal with the perpetrators of fraud. Speakers at the event, held at Bevan Brittan's offices in Bristol, included Detective Inspector Richard Budd from Avon and Somerset Police who looked at the criminal process, while Ben Daniels, a Litigation Partner from Bevan Brittan addressed the issue from the perspective of civil litigation.

The event was highly successful and was attended by a number of representatives from leading insurance and financial service companies in the South West.

Ben Daniels gave a brief overview of the civil law armoury available to the victims of fraud and looked at the circumstances in which it may be appropriate to seek civil litigation advice as part of a response to a fraud. Ben suggested that in many cases, especially straightforward cases involving employees and where the fraud is not particularly sophisticated, then the usual course of action is to conduct an investigation and if appropriate involve the Police. However, where asset recovery is important, usually because of the size of the fraud, then the civil litigation option should be considered at the earliest possible stage and certainly before arrests are made in order to prevent assets being dissipated.

Richard Budd's presentation looked at the issue of fraud from the Police Force's perspective of competing demands in relation to serious and organised crime. In describing how Forces prioritise demands he made it clear that not all

fraud cases are accepted for investigation but that the Police would always work with the victim to identify appropriate options.

Richard looked at who is most likely to commit fraud and who is most likely to uncover it.

Richard then went on to explore the current trends in fraud and in particular the rise in identity theft mainly through phishing activity to obtain personal information and credit card details. The issue of theft of company identities was also looked at, as was the growth in a wide range of scams. His presentation concluded with a number of personal preventative measures that can be undertaken to help prevent fraud.

If you were unable to attend the seminar, a copy of both presentations is available from Vanessa Taylor – Bevan Brittan, by telephoning 0870 1941654, or by emailing: [Vanessa.taylor@bevanbrittan.com](mailto:Vanessa.taylor@bevanbrittan.com)

**Bevan Brittan**

### THIS ISSUE

- 1 **Dealing with perpetrators**
- 1 **Forthcoming events**
- 2 **National Fraud Forum**
- 3 **Understanding types of fraud**
- 4 **The future of fraud**

## Forthcoming Events

### SWFF AGM

**11:30 Thursday 26 October 2006**

Exchange Conference Centre  
Bridgwater, Somerset (Junction 23, M5)

All members have been invited to attend the first South West Fraud Forum AGM to help celebrate what has been a successful year. Business commences at 11:30 with the election of the Management Committee and Steering Group members.

The AGM will be followed by lunch then a seminar to look at the problem of company theft. Speakers lined up include representatives from Jordan's, the company formation agency, Dunn and Bradstreet and Officers from the Metropolitan Police – Operation Sterling.

### Membership

If you are new to SWFF and want to participate in future events and seminars then visit the website at <http://www.southwestfraudforum.co.uk/> for details on how to subscribe.

## National Fraud Forum "The Threat From Within"

The National Fraud Forum is a bi-annual event organised by the National Working Group on Fraud. The NWGF sit as a sub-group to the Association of Chief Police Officers Economic Crime Portfolio.

Held over 3 days in October at the Latimer Conference Centre near Amersham in Buckinghamshire, 180 delegates from law enforcement, the public and private sectors met to discuss the increasing problem of the threat to companies, agencies and organisations from within.

A range of speakers from the different sectors identified the nature of the problem, whether it related to corrupt employees defrauding their employers or insiders stealing customer information to be passed onto organised crime groups.

Day 1 set the scene by examining the scale of the problem and the differing perspectives from law enforcement, the public and private sectors. Speakers included David Bowerman – Royal Bank of Scotland, Sheila Webb – NHS Counter Fraud and Robert Wardle – Director, Serious Fraud Office.

Workshops held on the second day considered a number of particular issues relevant to the problem.



Latimer Conference Centre

These included data and intelligence sharing, the importance of staff vetting, issues caused by identity theft and working covertly within organisations to detect and prevent fraud.

Several case studies from both the public and private sectors were presented to demonstrate the impact that insider fraud can have on organisations. Delegates were left with no uncertainty as to both the economic and reputational damage that can be caused by such activity.

Positive messages were the order of the third day. Eminent speakers include Lord Goldsmith – the Attorney General, Jonathan Caplan QC, Mike Bowron – Commissioner of the City of London Police and Edna Young – Financial Services Authority.

Presentations focussed on the way forward and the strategy that was being developed to ensure fraud receives a higher priority, particularly within law enforcement. The Treasury Fraud Review and the Fraud Bill, due early in 2007 were highlighted as evidence of an increasing recognition within Government to take fraud more seriously.

One of the major outcomes of the forum was the obvious need and an increasing commitment amongst Delegates to work more closely to share information across Sectors  
In a bid to combat the Problem of fraud and the Threat from within



The Attorney General – Lord Goldsmith

The Treasury Fraud Review was published and presented to Ministers in July 2006. Commencing in October 2005, a wide-ranging consultation has taken place, which has considered, the nature and scale of the problem, the appropriate response by Government and how resources can be best utilised.

A total of 42 recommendations were made and consultation on these ends 27 October 2006. The issues being addressed include, how to measure fraud, a national strategy, consistency with reporting, data sharing, prevention, investigation, more public/private collaborations and the criminal justice system with regard to more efficient trials and more effective penalties. Some of the recommendations that are likely to be realised include, a National fraud strategy, a National fraud reporting centre, a National fraud intelligence bureau, and improved arrangements for data sharing. A copy of the full report can be found at:

[http://www.lslo.gov.uk/fraud\\_review.htm](http://www.lslo.gov.uk/fraud_review.htm)

## Understanding types of fraud

Baffled by the many different problems facing a business or an individual, when it comes to fraud? In a regular feature, we will try to give you a basic understanding of the many varied and complex frauds that are currently seen throughout the country.

### COMPANY IDENTITY THEFT.

Company identity theft is similar to personal identity theft, in that it involves valuable information being obtained and compromised usually for financial gain. It is surprisingly easy to change company documentation. With little knowledge or effort on the part of the perpetrator, a company's registered address, trading address and the names of Directors can be changed. The perpetrator then effectively has control of the company and can set about placing orders for goods that can be delivered anywhere, with little hope of payment or recovery.

The documentation to achieve this is easily obtained online from the Companies House website. Companies House is a repository for information and it has to accept documentation it receives at face value.

Once the details have been changed and the fraud commences, any checks done by the supplier to validate who they are dealing with will confirm the bogus information as that currently held at Companies House. This will also affect the accuracy of any credit rating checks. If the true company was trading healthily, this rating will continue to apply to the cloned company. Hence there will be no reason not to accept the order.

The fraudsters will order goods from current or new suppliers to be delivered to the "new" trading address. The legitimate business will not see these goods and the trading address that the goods are delivered to will be a convenient drop address or an office mailbox. Mailbox addresses are used particularly where the commodity sought is relatively small but of high value. High tech and electrical goods are very popular as are leisure goods and designer clothing. If the invoice address has not been changed the legitimate company may even pick up the bill.

There are then always at least two victims of company identity theft – the company whose details have been cloned and any company that supplies goods or services to the cloned company. The companies who are impersonated tend not to be the multi-nationals or large nationals but more so mid-tier businesses. Ultimately, everyone pays for this fraud indirectly through higher product costs and insurance premiums.

As part of its economic crime strategy for London, the Metropolitan Police commenced Operation Sterling. As a crime reduction and prevention initiative, part of its remit is to work closely with Companies House to reduce opportunities for this type of fraud. One measure that has been introduced is that of WebFiling. Any changes to company's details are filed online, electronically. The company is issued with a security code and an authentication code. As an additional feature, the security code is sent by Email and the authentication code is sent by regular post to the registered office. Once these have been issued, any changes to a company's details will only be accepted through online WebFiling.

There have already been instances where Companies House customers have been telephoned by someone purporting to be from Companies House asking for verification of their security and authentication codes. You can be assured that Companies House personnel will never contact customers in this manner for this reason.

As a general rule, the following advice applies to all companies. Never throw out company documentation showing letterheads, signatures, bank account and company credit card details or invoices. Look to invest in systems that help monitor any change in details held at Companies House. Some services will send an Email alert following any request for changes. This should allow you to take immediate action in order to avoid becoming an unwitting victim of this profitable crime.

For more information about the Companies House WebFiling and other services, visit:

<http://www.companieshouse.gov.uk/>

## Shaping the Response to the Future of Fraud

### NEFF – FUTURES FOR FRAUD?

The North East Fraud Forum (NEFF) is hosting a conference on November 28 2006 at St. James Park, the home of Newcastle United football club.

Entitled “*Futures for Fraud?*” the event includes representatives from the Treasury Fraud Review Team, Association of Chief Police Officers, Financial Services Authority, Serious Fraud Office and the Fraud Advisory Panel.

In discussing the way forward in the fight against fraud, the event aims to launch a National Fraud Forum Federation. This would act as an umbrella organisation for all regional Fraud Forums. Utilising the NEFF model, it will bring all forums together to fight fraud and financial crime at a national and hopefully international level.

Fraud Forums now exist in the North East, North West, South West, Yorkshire and Humberside, East Anglia and Scotland. Others in the UK, including the Midlands and Northern Ireland will follow in 2006/2007 and plans are afoot to spread the franchise further a field to mainland Europe.

This important conference will seek to draw together a framework for developing the franchise with a view to improving the service that fraud forums currently provide.

The Attorney General – Lord Goldsmith said “*The way to fight fraud in the future is for the public and private sectors to join together. This is what that regional Fraud Forums must do and the formation of the North East Fraud Forum by Northumbria Police is an excellent example of this*”.

The event is open to members and non-members. Representatives of the South West Fraud Forum will be attending. For further information visit:

<http://www.northeastfraudforum.co.uk/>



### Calls for Complex Fraud Trials to be Replaced by Tribunals

In line with the Treasury Fraud Review recommendation the new head of the Crown Prosecution Service Specialist Fraud Unit, David Kirk calls for fraud tribunals to replace long and expensive fraud trials.

David Kirk said “*some complex fraud cases could be run faster and better by a specialist tribunal that had no jury but could impose criminal sanctions short of sending people to prison*”.

Mr. Kirk whose career as both a prosecution and defence lawyer spans 30 years says his plan could help in cases in which the alleged offences are highly technical or have been committed by executives in a clumsy attempt to stop their companies from collapsing.

Such a tribunal would have the power to impose fines and other non-custodial penalties, such as disqualification as a Director. It could provide the solution to the continuing problem of cases being too complex for juries to understand.

It would also help to avoid the embarrassing situations that can occur as seen recently in the criticism levelled at the CPS following the collapse of the Jubilee Line trial. Six men were charged with offences relating to the building of the rail line extension. The trial lasted more than two years and cost some £25 million before it collapsed without the jury being asked to consider a verdict.

Mr. Kirk stresses that the idea would be suitable only for a limited number of cases and would not be appropriate for alleged offences involving “wholesale dishonesty”. The use of tribunals would be particularly suited to cases more at the regulatory end of the spectrum or those involving corporate insolvencies where mistakes or misjudgements had been made and at some later stage greed took over.

# FRAUD FORUM NEWS AND VIEWS

## UK CARD LOSSES FALL BY £65M

The introduction of chip and pin cards has led to a reduction in overall credit card fraud in 2005. In 2002 it was projected that without the introduction of chip and pin, card losses would amount to £800m. The first annual fraud figures since the introduction has seen a 13% decrease to £439m

Credit card fraud is broken down into a number of different categories, most of which have seen a reduction. The most significant is in the mail non-receipt category where the card is intercepted before it reaches the customer. This has fallen by 45% as a direct result of chip and pin.

Other significant reductions were seen in counterfeit cards (25%) and lost/stolen cards (22%) with a combined reduction of over £60m.

Chip and pin is also impacting on domestic cash machine fraud as losses fell by 12% to £65.8m.

The only area of card fraud to rise was card not present (CNP). This includes any transaction where the card does not need to be presented, usually over the Internet or by telephone. This category rose by 21% from £150.8m in 2004 to £183.2m in 2005. However, indications are that this trend is slowing thanks to more awareness and an increased use by retailers and suppliers of verification checks on addresses and the 3 – digit security code found on the signature strip.

Cheque fraud losses continue a downward trend with a 13% decrease from £46.2m to £40.3m.

Card Identity Theft in the form of account takeover or false application is decreasing. It fell by 17% to £30.5m but continues to represent only a small fraction of total card losses at just fewer than 7%.

Organised crime gangs continue to be increasingly involved in card fraud and other forms of financial crime including on-line banking fraud. Losses here reached £23.2m in 2005, almost double the previous year's losses of £12.2m. This is the result of account holders falling for phishing scams.



## HEADING FOR A CRASH

Drivers are being advised to be on their guard against organised criminals who deliberately cause crashes in a relatively new form of fraud. The Association of British Insurers states that it has become aware of a spate of incidents in Yorkshire where criminal gangs disconnect the brake lights of their cars and “slam on their brakes at roundabouts”. When the innocent following driver goes into the back of them they are assumed to be the one at fault. The gang will then attempt to claim from their insurers.

Insurance fraud of all kinds costs the industry £1.5bn a year adding about 5% to the cost of premiums.

## PASSPORT TO SECURITY

Lukas Grunwald, a consultant with a German security company announced at a hacker's conference in Las Vegas that he has identified a security flaw in the new UK biometric passport.

He claims he has discovered a method of cloning the information held on the passport's chip and that this data could be transferred to blank chips that could be used to create new, counterfeits.

Mr. Grunwald detailed how he did this with equipment costing just over £100. If correct this could have implications for the introduction of a UK identity Card that would use similar technology

## PLANNING APPLICATION ALERT

The UK's Fraud Prevention Service – CIFAS state that local planning authorities routinely publish sufficient personal details about planning permission applicants that criminals have all that they need in order to adopt their identities, including copies of signatures. Local Authorities in addressing the problem will ensure that applicants will be aware that their applications are published on-line and will encourage them to only submit personal information they are happy will be made available on the Internet.

# FRAUD FORUM NEWS AND VIEWS

## CHARITY DONATION SCAM

Charity regulators have issued a warning about a new scam that could cheat charities out of thousands of pounds. Bogus donation cheques, some as high as £6000 have been sent to good causes across the UK, with a note asking the charity to return up to half the total donation. If the scam works and unsuspecting charities buy into the story and repay part of the donation, they find that the original cheque bounces, leaving them defrauded of vital funds.

The Immaculate Miners Inc is one fraudulent company preying on charities in this way. Deafway, a Lancashire based charity were one of their victims. Deputy Chief Executive at Deafway, John Williams said, *"When we received the cheque we were delighted – such a large sum of money could really give a boost to our work – but also somewhat suspicious. An unsolicited donation with a payback request rang alarm bells. We contacted the Police, Charity Commission and Trading Standards and were told we had fallen for a scam"*.

Charities should treat requests to return part of a donation with great caution and never release funds before the donation cheque has cleared. Bear in mind that whilst funds clear in 3 days a stolen or counterfeit cheque will take longer to be identified. Even if funds have cleared, they can be clawed back by the bank if the cheque turns out to be bogus.

## VISHING marks New Danger

Most people are familiar with the term Phising as a criminal activity to obtain personal information by Email. A new scam dubbed "vishing" makes use of net phone technology in an attempt to con people into handing over personal information. Programmed computers use automated dialling and pre-recorded messages to advise customers that their credit card accounts have been compromised. They are then asked to enter their credit card number, expiry date and 3-digit security code via the telephone handset.

It appears people are less suspicious of telephone calls particularly when the fraudster can fake the number that they are calling from. Banks are not likely to request information by these means and if they appear to be ignorant of basic details such as your name or address then you should exercise caution.

## Market Research or Scam

Four out of five people stopped in the street by a stranger posing as a market researcher gave away confidential information in return for a chance to win an Easter egg.

All those interviewed gave a name and address. 8 out of 10 gave a date of birth, while 9 out of 10 gave a telephone number. During the interview they were asked if they fed eggs to pets and 86% went on to reveal a pets name. When asked if there was a tradition of giving eggs in their family 80% revealed mother's maiden name.

You will have spotted that these are precisely the details commonly used as passwords and memorable words with financial institutions. At no time was the researcher asked for any verification of their own identification.

## TELL US WHAT YOU THINK

This is the third newsletter produced by the **South West Fraud Forum**. We would like to know what you think.

- What features would you like to see?
- Tell us about your experience of fraud
- Would you like to know more about a particular fraud or scam?
- What events or training would you like to see SWFF run?

## CONTACT DETAILS

SOUTH WEST FRAUD FORUM  
PO Box 350  
BRIDGWATER  
TA6 9AH  
Email: [info@southwestfraudforum.co.uk](mailto:info@southwestfraudforum.co.uk)

Keep up to date with the latest news on SWFF events – visit the web site at

<http://www.southwestfraudforum.co.uk/>