

Fraud & Forensic Services Briefing

Keeping you up-to-date with events in your sector.

Welcome

Welcome to the third issue of our Fraud & Forensic Group Briefing. In this issue we touch on the complicated Missing Trader Intra-Community (MTIC) Fraud with an insight from our newly formed Fraud & Investigation Unit. An enormous amount of public money is being lost as a result of this criminal attack on the EU VAT system, which affects the public finances of all EU member states.

I am delighted to introduce our guest author John Burbidge-King, of Interchange Solutions and a fascinating insight into the topical area of bribery and corruption. The Joint Committee of the House of Lords and House of Commons has now completed its scrutiny of the Bribery Bill which, for many, has been viewed as both necessary and long overdue. Many other topics are also covered which we hope you find interesting and relevant.

Our Fraud & Forensic team continues to grow in experience and expertise. We look forward to working with you to meet the challenges ahead. Please address any enquiries to the author of each article or, if you have any general questions about our Fraud & Forensic Services, please contact me or the other members of our team directly.



Dr Stephen Hill
Head of the Fraud & Forensics Group
T: 020 7509 9320
E: shill@cvcdfk.com

Crime may be down but fraud is on the up How we help our clients

With the collapse of Lehman Brothers in October 2008, many at the time predicted the banking crisis would lead to an economic Armageddon that would result in an unprecedented rise in crime. Things did not turn out to be quite so bad (as predicted) for the UK economy in 2009, and the same is true of crime. Latest statistics released by the British Crime Survey (BCS) revealed that recorded crime is down 5% and confidence in the police is high. But for all this encouraging news one large threat continues to grow, fraud.

The BCS report states that e-crime and credit card fraud are becoming a more prevalent crime, with fraud in general being under-reported to the police. The findings draw on data from the UK Cards Association (which records information on plastic card fraud in the UK) and this reveals that there were 2.8 million fraudulent transactions on UK-issued cards

recorded in 2008. This represents an increase of 4% from 2007. People are now more at risk of being victims of plastic card fraud with growing concerns over identity theft.

Identify theft and data security are key issues for most organisations especially at a time when the economy is still unstable and data is seen as a lucrative asset to the disconcerting employee or is lost as a result of failed systems through poor management. Significantly, only recently a large international bank was fined £3m by the Financial Services Authority for failing to adequately protect customers' confidential details while the Office of Fair Trading (which has spent large sums urging businesses to protect themselves against scams) failed to notice a fraud until £250,000 had gone missing. This shows that now, more than ever, is the time for organisations to address the threat fraud poses to their operations.



Our Fraud & Forensics Group has evolved over the last 12 months in line with emerging threats to offer a wider range of counter fraud services in many different sectors aimed specifically at helping clients and ensuring we are always one step ahead.

Examples of the services we provide include:

Fraud prevention and detection

- IT systems review (ISO 27001, PCI DSS)
- Cybercrime and corporate fraud prevention training
- Risk management and fraud health checks
- Fraud response plans (management policy and procedure design)
- Investigations in accordance with the Police and Criminal Evidence Act (PACE)
- Surveillance under the Regulatory Investigatory Powers Act (RIPA)
- Data mining



Asset tracing & recovery of funds

- Obtaining and implementing worldwide freezing orders
- Recovery of funds in the UK and overseas jurisdictions
- Computer seizure and investigation
- Innovative use of insolvency procedures to gain control of an individual or corporation's assets
- Restraint and confiscation of assets of criminals
- Preparing reports on the provenance of assets, used in subsequent civil recovery actions
- Presenting evidence in court

Do you take Credit Card Payments – are you compliant?

The Payment Card Industry (PCI) Data Security Standard (DSS) is a compliance standard that has been developed in order to help organisations proactively reduce the risk of data compromise and the effects of fraud.

Organisations processing credit cards that failed to meet the 1 October 2009 deadline (to become compliant) face mounting pressure as failure to comply or a system compromise that causes customer card details to be used fraudulently may result in a financial penalty or termination of processing services.

At Barclaycard for example, it is their duty to report monthly to VISA and quarterly to MasterCard, letting them know the status of merchants' compliance with PCI DSS. From these reports, the card schemes then select merchants to investigate. If they find fault with a merchant's compliance, they will levy non-compliance fines.

The standard contains 12 requirements for implementing effective information and data security practices. These requirements cover technical aspects of security management, and also impact policies and procedures.

The standard is administered by the PCI Security Standards Council (PCI SSC), an organisation founded by 5 card schemes; American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. The PCI SSC is responsible for developing and enhancing the PCI DSS in order to make sure that requirements are up-to-date and in line with emerging payment security risks.

Organisations affected by the PCI DSS include all acquiring banks, all merchants that accept payment cards, and all service providers who store or transmit card or transaction data. Merchants are categorised in 4 tiers depending on the volume of transactions that they process, (tier 1

merchants process the most transactions, tier 4 process the least). The compliance process varies slightly depending on which tier a merchant belongs to.

In order to achieve compliance, organisation's must ensure their systems, and those of any third parties they work with, meet the 12 requirements of the PCI DSS. They must then conduct an audit, which is usually carried out by a Qualified Security Assessor (QSA). QSAs are certified by the PCI SSC and are responsible for validating an organisation's compliance. Compliance must be maintained on an ongoing basis.

As the evolution towards a cashless society continues to gain pace, compliance with the PCI DSS is becoming ever-more essential. Are you ready?

If you would like any further advice on PCI DSS or would like to speak to one of our experts then please contact Dr Stephen Hill or Mark Kinsella.



Dr Stephen Hill
Head of the Fraud & Forensics Group
T: 020 7509 9320
E: shill@cvsdfk.com



Mark Kinsella
Partner
T: 0118 952 4700
E: mkinsella@cvsdfk.com





John Burbidge-King
CEO Interchange Solutions
T: 0208 528 1011
E: jbk@interchange-solutions.co.uk
W: www.interchange-solutions.co.uk

“The times they are a changing”

So sang Bob Dylan years ago as is the attitude to bribery and corruption. The Serious Fraud Office (SFO) has 16 ongoing UK corporate investigations, more than 50 individual suspects, 30 new cases are under consideration and its workload has doubled in the last 12 months. Added to which, the UK Bribery Bill is inching its way into Parliament.

The mantra “it’s the way to do business in certain countries” is fast becoming passé as companies, organisations and governments, grapple with the toxic fall out of bribery and corruption; examples include the rerun of elections in Afghanistan, Siemens, AON, CBRN and Mabey & Johnson.

Mabey & Johnson is a Reading based bridge manufacturer. It approached the SFO in 2008 following an internal investigation into suspected bribery of foreign public officials, which extended into possible corruption in 6 countries, as well as breaches of the United Nations sanctions in Iraq. In September 2009, the company was fined, £3.5m for breaching UN sanctions against Iraq and bribing foreign officials. It was ordered to pay a £1.1m confiscation order, reparation to some countries including Ghana and Jamaica and costs of £350,000 to the SFO. It also had to accept and pay for, external monitoring of its anti corruption processes.

Mabey & Johnson was successfully prosecuted under the existing bribery laws. It was a landmark for the SFO as it cleared the way for the company to move on from its past. This self-referral approach is laid out in the SFO’s guide to Dealing with Overseas Corruption (www.sfo.gov.uk).

However, following the Queen’s Speech, the Bribery Bill is now going through the parliamentary process and it could become law in 2010. The old laws will be repealed and the new law would be clearer and incorporate some key changes, namely:

- In a domestic context, no distinction between bribery in the private and public sectors, nor between principal and agent
- A new separate offence for the bribery of a foreign public official
- A new offence of corporate liability; failure to prevent bribery

It is the new corporate liability offence that managers, executives and company directors need to address with some immediacy. Simply put, if a bribery investigation reveals that the bribe was in connection with the company’s business, and there was negligence by the person(s) employed to prevent it, both the company and those individuals may be prosecuted, despite their not being directly connected to the act of bribery itself. A company’s defence in court would be to prove that it had working adequate procedures in place and that the bribe was an isolated incident.

However, a company cannot avail itself of the adequate procedures defence, if the failure to prevent bribery occurred through the individual negligence of a Director.

Under the proposed new law, turning a blind eye at executive or board room (executive and non-executive) levels is no



longer an option; to the contrary, in so doing it may lead to the prosecution of those persons (fine and/or imprisonment) who had the responsibility to ensure the good governance of a company. It is therefore vital, going forward, that the board’s supervision extends to ethical and reputational risk matters to prevent prosecution for negligent board behaviour.

In future, it is possible that both the individual bribery offence(s) and the corporate offence could be tried at the same time.

The key question is therefore, what are “adequate procedures”? While there is some SFO guidance on this, the likely scenario is that the Bill will be brought into legislation and the guidance on adequate procedures will follow. This is probably too late for those companies and organisations with nothing in place at present.

Interchange gave evidence to the Parliamentary Scrutiny Committee on what might constitute Adequate Procedures, and that can be summarised as:

- A clearly articulated and communicated anti-bribery culture visibly driven by the “tone from the top” of the company
- Documented and evidenced on the board’s agenda and the risk register
- Policies to address conduct (including sanctions), ethics, hospitality and gifts, facilitation payments, oversight and disclosure mechanisms (so called whistle blowing), political and other lobbying and, conflicts of interest
- Accountability and responsibility, from employees to boardroom
- Robust processes for the appointment, due diligence and management of agents/advisers/distributors; embedded in both business strategy and measured in business process
- Education of all employees, with sign up to the anti-bribery approach from business partners including JVs and M&A, suppliers and visible to customers
- Principles and practices understood across cultures and language
- Appropriate regular oversight and audit

Unfortunately, far too many organisations are still unprepared, or inadequately equipped, against the threat of fraud.

been a legal definition of fraud in the UK, and what we consider to be fraudulent acts had to be prosecuted under a range of offences falling under a number of different pieces of legislation; not least the Theft Acts of 1968 and 1978.

The offences under this older legislation were sometimes inadequate for purpose in respect of certain forms of fraud. For example, the offence of Obtaining Property by Deception could not be applied to a situation where a fraudster used a stolen or cloned bank card to withdraw cash from an ATM machine, as the law did not recognise that a machine could be deceived. The Fraud Act 2006 removed the need to prove deception, thus allowing many more acts that are generally accepted as fraudulent to be prosecuted under anti-fraud legislation. Now such an act could be prosecuted as Fraud by Misrepresentation under the Fraud Act.

By providing for three main means by which fraud can be committed – Fraud by Misrepresentation, Fraud by Failure to Disclose Information and Fraud by Abuse of Position – as well as a number of additional offences, the Act helps to simplify and clarify the options for prosecuting the majority of means by which fraud is generally perpetrated. Not only good news for prosecutors, this is generally good news for organisations and those investigating fraud on their behalf, as the necessary points to prove under the new offences are arguably more attainable in many cases (such as in the simple ATM fraud noted above). Where more and more fraud against organisations is attempted via the internet, and/or by specifically targeting the organisations computer systems to commit and enable violations, these new legislative means of defining and prosecuting fraud look increasingly valuable.

Despite this overall improvement in the general environment in which fraud is understood and tackled in the UK,

organisations still need to be vigilant against it, perhaps to a greater degree than ever before. The rise in fraud committed via the internet, and the global business environment enabled by the same to organisations of all sizes, means that the scale and potential of the threat has never been greater (although the vast majority of frauds against organisations are still committed from within).

Some of the new agencies and approaches are untested, unproven or may raise expectations about results they are not designed to deliver: the National Fraud Reporting Centre will not, when it is launched nationally, lead to widespread investigation of cases reported, but will primarily analyse trends in the intelligence gathered, leading to the possibility of an expectation gap between the anticipation of those using the service and actual outcomes. Furthermore, the national fraud strategy has been criticised in some quarters, and while the City of London Police has been designated the national Lead Force in the fight against fraud, police priorities and budgets relating to fraud on a national basis still fall significantly below what many would expect for such a damaging crime.

Most organisations across all sectors would therefore benefit from having practical systems in place to assess and minimise the risk, procedures to deter and detect potential offences, and mechanisms and plans ready and in place to investigate incidences of fraud and corruption as soon as they come to light. Unfortunately, far too many organisations are still unprepared, or inadequately equipped, against the threat – all the more concerning as most of the risks can be minimised or avoided through having sensible systems in place before it is too late. The potential consequences for those organisations that do not can be severe. We can help.

Who to Contact

For further information or advice, please contact the author of the relevant article, your usual Chantrey Vellacott DFK partner or one of the following:

Birmingham

Suk Aulak
0121 454 4141
saulak@cvdfk.com

Croydon

Richard Willis
020 8633 9378
rwillis@cvdfk.com

Northampton

Elliot Harris
01604 639257
eharris@cvdfk.com

Watford

David James
01923 255111
djames@cvdfk.com

Brighton & Hove

Ken Touhey
01273 421200
ktouhey@cvdfk.com

Leicester

Elliot Harris
0116 247 1393
eharris@cvdfk.com

Reading

Ian Johnson
0118 952 4700
ibjohnson@cvdfk.com

Colchester

Dawn Lay-Flurrie
01206 549303
dlay-flurrie@cvdfk.com

London

Mark Lamb
020 7509 9000
mlamb@cvdfk.com

Stevenage

Mark Stevens
01438 741147
mstevens@cvdfk.com

This Briefing is a summary of recent developments. It should not be regarded as a substitute for advice in any specific situation. The opinions expressed in guest articles are those of the respective contributors and do not necessarily represent the views of Chantrey Vellacott DFK. For further information or advice, please contact the author of the relevant article or your usual Chantrey Vellacott DFK contact.

Chantrey Vellacott DFK is the trading style of Chantrey Vellacott DFK LLP, a limited liability partnership registered in England and Wales (No:OC313147) whose registered office is at Russell Square House, 10-12 Russell Square, London WC1B 5LF. The term 'partner' denotes a member of a limited liability partnership. A list of members is available at our registered office.

Chantrey Vellacott DFK LLP is registered to carry on audit work by the Institute of Chartered Accountants in England and Wales. Chantrey Vellacott DFK LLP is not authorised by the FSA but is licensed by the ICAEW to provide investment services where these are incidental to, or arise from, the professional services it is engaged to provide.

© Chantrey Vellacott DFK LLP 2009

If you do not wish to receive any further copies of this Briefing please notify us by email at info@cvdfk.com



INVESTOR IN PEOPLE

