Procurement Fraud in E-business

by Jon Hayton

Dispute Analysis & Investigations

PRICEWATERHOUSECOOPERS

Contents

Jon Hayton is a Senior Manager in the Dispute Analysis & Investigations practice of PricewaterhouseCoopers. He can be contacted on 020 7212 4210 or jon.hayton@uk.pwcglobal.com

An Old Scam in a Digital World

Procurement fraud is as old as commerce itself. 'Understandings' and 'favours for favours' remain endemic to some degree in most modern economies. Indeed the line between corporate hospitality and bribery can sometimes seem dangerously thin.

Procurement fraud can take a number of forms, from the formation of a cartel to the falsification of invoices. Most commonly, an employee responsible for procurement might receive bribes or incentives from a supplier designed to encourage them to favour that supplier.

As e-business becomes increasingly dominant in the commercial world, procurement, in common with other processes, is becoming increasingly digitised and automated. How does this development impact on the opportunities for and methodologies of procurement fraud?

In order to protect themselves against procurement fraud, companies have traditionally sought protection through controls and procedures, believing that such strong controls were difficult to breach and would discourage potential fraudsters from attacking their businesses.

Alas, this view is somewhat naïve. Sophisticated fraud revolves not around the breaching of these controls, but the circumvention of them. For example, most companies will point to their tendering procedure as an effective deterrent against procurement fraud, often pointing out how the technical and commercial evaluations are separated and controlled by different people.

But the greatest opportunity for undetected fraud remains at the initial phase of the tendering process, where the perpetrator might:

- Restrict those suppliers that are invited to tender
- Draw up a specification that suits the favoured supplier
- Ensure the other tenders receive a different specification

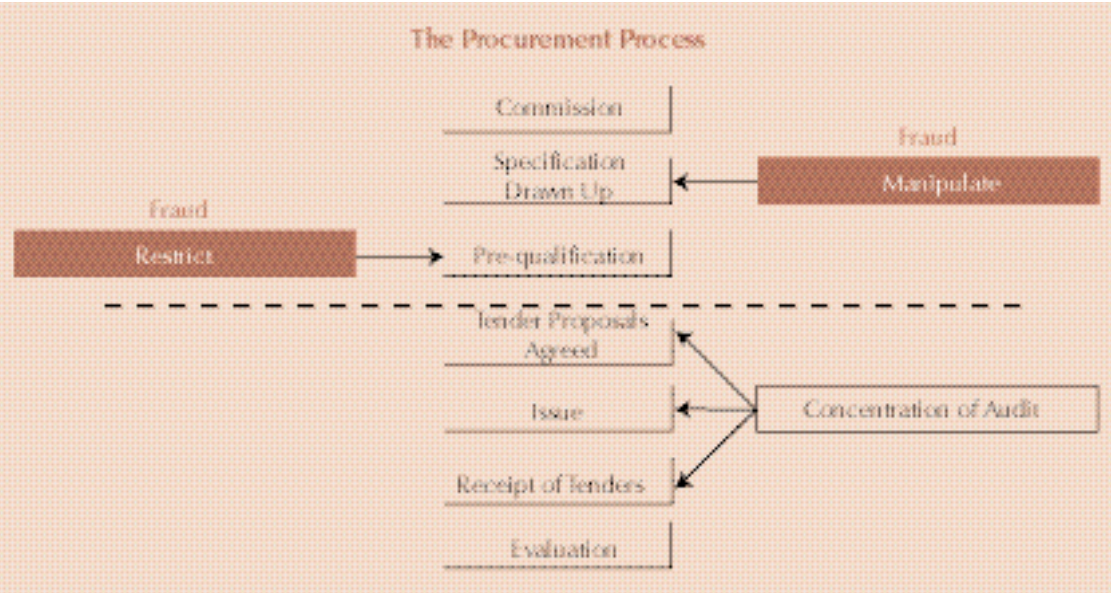

Fig. 1. Opportunities to commit procurement fraud - points at which the tender process is typically manipulated

Why do these opportunities exist?

The modern fraudster knows inside-out the procedures of the department they are defrauding. They may have worked there for years, and their deep involvement with the procurement process means that they know how that process will be audited and, in particular, where an inquisitive auditor will look.

Therefore, by tampering with the procurement process at a point where the auditor is less likely to have the technical skills to review it, the fraudster can ensure that his or her favoured supplier is awarded the contract. On the surface, meanwhile, the systems in place to warn the auditor that something is amiss appear quite undisturbed.

In today's business environment it is becoming increasingly recognised that controls can only seek to contain fraud rather than eliminate it. This is the basis upon which most controls environments are designed to limit risk. While some organisations are beginning to acknowledge that they are not equipped to detect fraud, only breakdowns in their controls, others still perceive such controls to be their only weapon against fraud.

Arguably the most fundamental problem with detecting a procurement fraud is finding the bribe and in particular how and where it manifests itself. A bribe to an employee (to secure a contract or for information about competitors, for example) will almost certainly be paid outside the workplace and may be in the shape of a service or materials, such as work on the individual's house or the provision of building supplies.

In such a case, it is virtually impossible for a routine audit or review to uncover its existence as an internal audit department does not have the power to access employee bank accounts or to visit an employee's home to assess what decorating has been carried out.

Even if access to the supplier's records can be obtained, the fraud may still be difficult to detect. A suspected employee questioned about work on his home is likely to be able to produce an invoice … and argue that he just forgot to pay it.

Bribes can take many forms: in one particular case the supplier sponsored the procurer's cricket team. It was difficult to claim the individuals received any personal benefit, but for such a small inducement, the employee involved made sure that the supplier was always awarded the company's maintenance contracts.

In another case, a British Transport Police investigation into kickbacks paid to rail employees for placing repair work with a particular supplier uncovered bribes that ranged from foreign holidays to repairs to an E-Type Jaguar. The complexity of the investigation meant it took over four and half years to complete.

In a bid to prevent this kind of corruption, companies often point to their conflicts of interest policies, or their full and detailed hospitality returns. These are all designed to prevent bribery in its embryonic stages. But even if there is evidence of potential conflict of interest it may be difficult to prove that it had a material effect on the placement of the contract. And who really believes a fraudster will honestly complete a hospitality form?

The requirements of the Turnbull Report and the need for effective monitoring of risks mean that it is no longer acceptable simply to rely on the existance of controls. Senior management must satisfy themselves that effective risk management processes are embedded in their company's day to day operations in order to ensure that the company's assets are fully protected.

The only truly effective way to reduce an organisation's exposure to procurement fraud is to go looking for it.

This in itself requires a company to examine all potential opportunities for fraud, to go looking for weaknesses and gather intelligence on potential fraudsters, rather than simply battening down the hatches and hoping the controls will do their job. It is a process of looking for opportunity and motive - in the right places.

Fraud, however, cannot be successfully detected through sampling and straightforward auditing. Random sampling might stumble across a fraud, but it requires the sort of good fortune that might be better applied to winning the National Lottery. Furthermore, the vogue for corruption-busting mathematical formulas ignores the fact that it is individuals, not machines that commit fraud; they come in many different shapes and sizes and their actions cannot be easily predicted.

So how do we go about effectively detecting fraud in the modern business environment? And, more importantly, how do we do it with minimum disruption to the business?

Sifting the Evidence - Unearthing Procurement Fraud

Increasing electronic data storage and transmission has brought more opportunities for investigators to track and retrieve that data. An e-mail message, for example, leaves a detectable 'footprint' on any server through which it passes.

In today's business environment, data mining techniques are most often employed as the solution to procurement fraud because of the increasing amount of available data that can be manipulated and examined, be it the supplier master file, invoice history file, or even access control data.

As a result, an increasing number of software packages are appearing on the market that can be adapted to interpret this data and to seek out warning signs of fraud. All these systems have their basis in tried and tested methodology but which, to date, have concentrated on such standard traditional procurement fraud profiling as looking for roundsums, sequential invoicing, and conflicts of interest.

However, by enabling investigators to identify who the procurer or buyer is within an organisation, systems such as SAP have brought a new dimension to fraud detection. This information can be used in a similar fashion to credit card data to build up profiles of individuals and their relationships with suppliers, effectively creating an account profile for each buyer. Although it remains difficult to detect a bribe, these profiles can be used to identify quickly instances where buyers may be favouring suppliers and allow an audit or a review to focus its work more effectively.

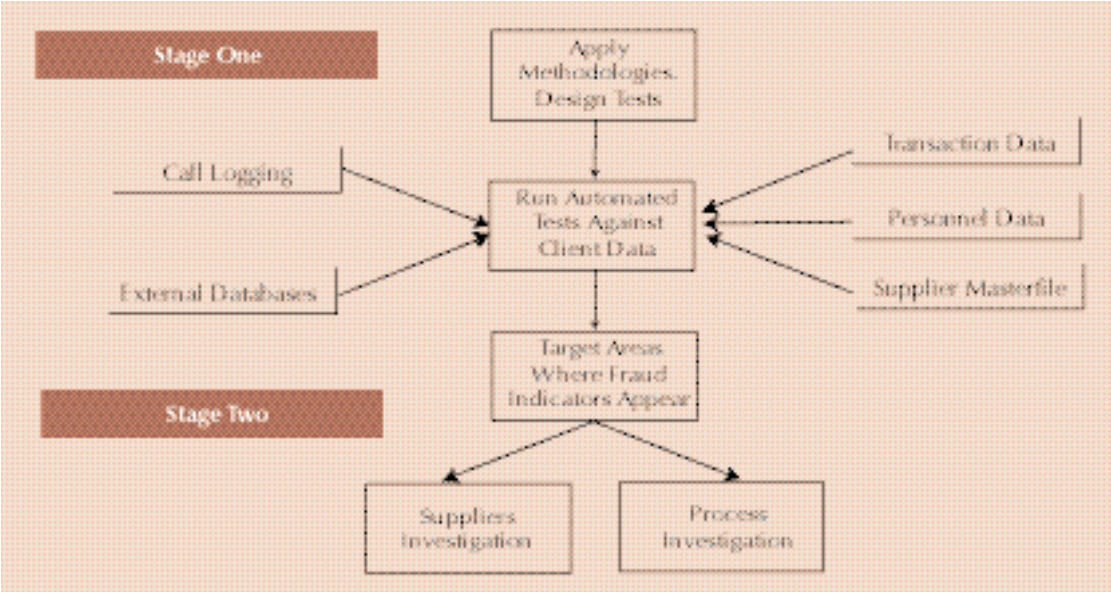

Fig. 1. Sifting the evidence - a typical fraud profiling process using company data

NB Any analysts of data relating to individuals must be carried out within the framework of the Data Protection Act 1998

Investigation and audit software such as I2 and WinIdea can then be used to process this data. By identifying links between buyers and suppliers potentially fraudulent relationships can be highlighted graphically:

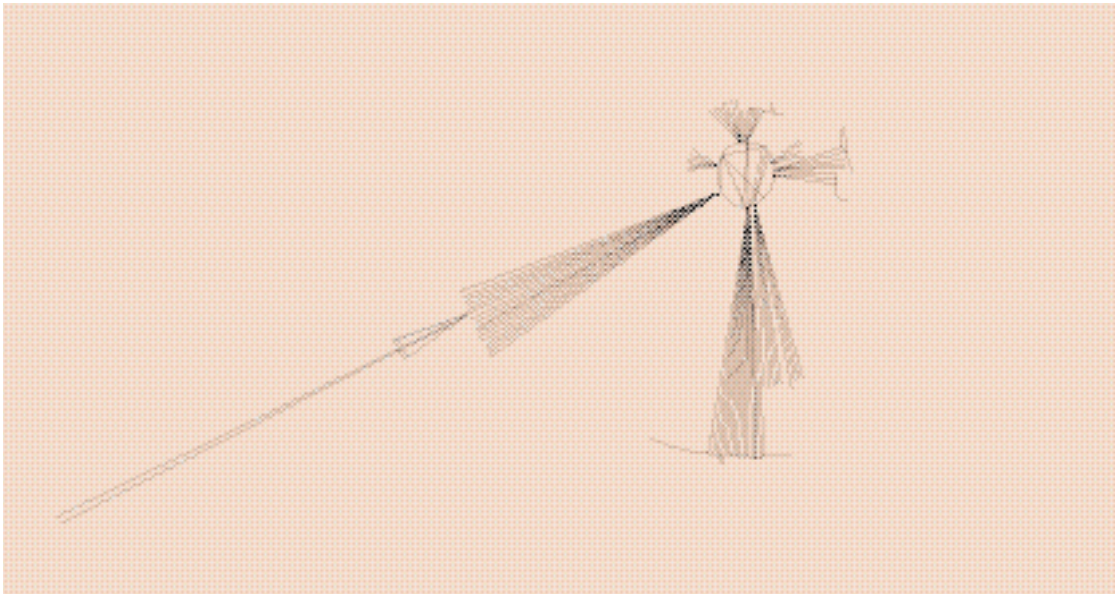

fig. 2. Company Spend Pattern showing relationships and frequency of orders

The points on the circle represent various buyers within an organisation with the spokes reflecting their relationships with suppliers. The lines within the circle represent cases where buyers are using the same suppliers and the spokes represent the number of suppliers a buyer is dealing with over a set period. Of particular interest are those buyers who deal with only two or three suppliers, where there is greater opportunity for close relationships to develop between the buyer and supplier.

In theory this is an effective approach, but companies still face the challenge of analysing the data quickly and efficiently (ie without investing thousands of man-hours and disrupting the business).

Until now, the detection process has lagged behind the procurement process as the required data has to be downloaded using existing report writing tools and then input into automated audit tool software (such as WinIdea) for analysis. There has been little real time monitoring of orders. By the time the data has been downloaded for analysis it is probable that the order has been posted, the goods received and the payment sent.

The growth of business-to-business transactions and online procurement, however, should take detection into real time as the procurement process becomes totally automated and the systems more flexible.

Network detection and intrusion systems traditionally designed to look for breaches of network security could be used to look for patterns normally associated with fraud. A number of systems can already profile users, learning their behaviour and reporting any unusual activity.

As more and more companies develop online systems, setting up company websites and switching to online procurement using either extranets, intranets or the Internet, the procurement process itself (as well as the frauds that prey upon it) is undergoing a dramatic change.

Digital Dodges – the E-business Procurement Fraudster

As we have seen, the advance of e-business and online systems within organisations offer new methods for profiling fraudulent patterns, if not actually detecting fraud itself. But what does the e-business age offer the fraudster in terms of opportunities to commit procurement fraud?

Traditionally, many procurement frauds have centred on peripheral businesses within an organisation, away from core purchases. Consultancy payments, marketing, printing, facilities management and IT are all areas where procurement fraud has commonly been uncovered, be it a bribe for the contract or an undisclosed shareholding in the printing company providing the service.

Increasingly, however, buyers in the business-to-business environment will deal with the supplier online and, as such, all their actions will be recorded electronically (e.g. which site they visited, when and with what frequency). All this helps with profiling buyers and their spend patterns, making it harder for the buyer to direct business fraudulently to his favoured supplier.

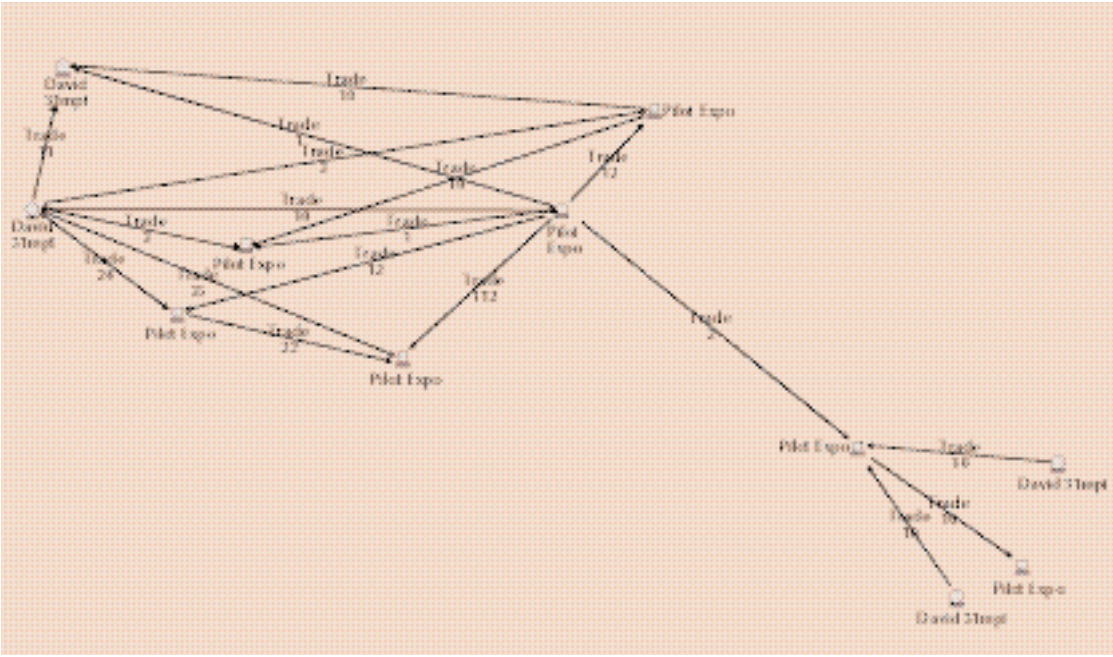

fig. 3. I2 diagram showing on-line trading between companies.

Online procurement is all about relationships between companies, the development of supply chains, leveraging corporate spend to get the right price and reducing informal purchasing. It is therefore unlikely that companies will allow buyers to continue to purchase 'on spec' from suppliers. Prices will be agreed centrally and then offered across the company's Intranet to its departments via an electronic catalogue. The buyer will have to explain why he did not use the central system. Informal purchasing, the traditional breeding ground for fraud, will almost certainly be reduced dramatically.

However, as the amount of data held electronically increases dramatically, allowing auditors and investigators to monitor patterns, it may also open up a whole new market for the hacker and information broker.

Today, most of the reported fraud on the Internet still involves simple deception rather than elaborate hacking, two of the most widely reported forms being the theft of credit card details and advanced fee fraud[1]. The typical hacker, meanwhile, is more concerned with embarrassing a government or playing around with a corporation's web site.

For example, the 'denial of service' attacks on Yahoo.com and Amazon.com (where the sites were maliciously bombarded with requests in order to deny other users access), and the share-ramping activities of unscrupulous financial websites, constitute an abuse of the medium rather than e-fraud.

Most of the current procurement-related fraud that occurs still concerns the retail sector and it is the supplier rather than the customer that is at risk. Typically, it will involve the use of stolen credit card information to obtain goods and services, the credit card details being stolen via some elaborate deception, by straightforward hacking into a company's customer files, or simply downloading them for a bulletin board.

E-business, on the other hand, is likely to offer the hacker the opportunity to move away from vandalism and into fraud. Whilst increased levels of electronic information will make fraud profiling easier, the same information will be equally useful to third parties. Internal auditors and investigators will not be the only people interested in information regarding where a buyer places his orders or what prices the supplier is providing. This information will also be of use to a competitor or potential supplier.

How much will a company be prepared to pay for the pricing and customer information of its competitors? No self-respecting hacker will bother with a single credit card number when he can steal the entire pricing structure of a major company, its customer lists and banking information - all of which can be sold for a handsome profit. In the US this type of data theft is already taking place. An online music store recently had all its customer details stolen and found itself the victim of a blackmail attempt.

The situation is further complicated by the lack of clarity over the intellectual property rights of data. If the hacker is operating in another country from where the data is held, in which country was the crime committed (if, indeed, it is a crime)? And can the company take any action to recover the data?

Firewalls and network monitoring tools will therefore become key factors in preventing procurement fraud. Although most procurement systems will operate on intranets and extranets, gateway links to the Internet may offer opportunities for third parties to access the network. Once inside they may have access to information from bank account details to pricing structures.

In this context it is vital to put in place a robust vetting process for both online customers and suppliers.

[1] **Footnote**

Advance fee frauds: The fraudsters pose as finance brokers, and purport to negotiate a large loan for a foreign company or government. The deception may be elaborate, for example, involving forged documentation, meetings in hotels. In return for the loan, a percentage fee is payable in advance; and if the loan is large, the fee itself will be substantial. Once the fee has been paid, the fraudsters disappear. Sometimes the fraudsters may succeed in obtaining collateral security for the loan, in which case they liquidate this as additional profit in the fraud. Closely related are frauds where advance fees are obtained for arranging mortgages. (Appendix F of the Roskill Report).

Business-to-business Customer and Supplier Vetting on the Internet - Ten Key Factors to Consider

1. Establish that the e-mail address and the billing and shipping address match.
2. Find out who are the customer's ISP (Internet Service Provider) and where they are located.
3. Find out whether it is a mailing address, a PO Box or an office bureau.
4. Validate the company name and incorporation.
5. Find out where the company is registered.
6. Verify the company trading address and registered office.
7. Obtain the last three years' accounts to ensure solvency and level of turnover.
8. Find out who are the directors and shareholders.
9. Carry out bankruptcy checks and county court judgment reviews on the directors.
10. Review directorships and shareholdings for potential conflicts of interest.

(It is also a good idea to check the company and its directors are in the phone book).

All these measures are straightforward company due diligence enquiries that most credit departments would undertake. In the rush to get online, however, there is a danger of them being overlooked.

As the nature of procurement changes in the modern business environment, so will the methods by which procurement fraud is perpetrated and detected. Whilst the dramatic increase in electronic traffic will make pro-active detection techniques more effective, the very same data that the auditor and investigator found invaluable will offer a greater opportunity for fraud.

It is worth bearing in mind, however, that in the midst of the e-business revolution and the accompanying maelstrom of new networks, software and methodologies, it is still human beings, and more often than not employees, who defraud organisation. Understanding where the motives lie for 'understandings' and 'favours' will remain a key priority in the fight against the fraudster in the electronic age.

Some Typical Procurement Frauds

Specification Manipulation

Often used on technical purchases where the engineer deliberately designs a specification to fit his favoured suppliers. Alternatively he might over specify what is required but tell his favoured supplier he can get away with inferior materials. The supplier says he will paint the wall three times but knows he can get away with two coats and costs the work at a lower price than his competitors. How do you check? In one case a building contractor was supposed to be fitting ventilators in kitchens, however instead of drilling through the wall he was just painting a black circle on the wall and putting a grill over it.

Final Look Arrangement

The favoured supplier is given a final look at all the other tenders to see if he can beat the price. Easily controlled through tender boxes, although it is often argued that this way the best supplier is awarded the work at the right price. Watch out for faxed tender documents, or in today's climate e-mailed documents.

Salami Tactic or Breakpoint

The old fashioned tactic of splitting orders to ensure they don't breach the authorisation limit. You will normally see a cluster of orders around the limit. If the purchase orders for the same supplier on the same project are sequential you have either set your authority levels too low or you might have a procurement fraud.

Comfort Bids and Cartels

Suppliers work together rather than bidding against each other. They either agree to keep prices high or supply notepaper to the ring leader so they can provide the company with spuriously inflated bids in order to make the winning bid look a good deal. The ringleader then divides the work up, sub-contracting it to the other suppliers. In one case the suppliers used to meet in the local pub to split up the work. The local authority they were all working for just thought building work was expensive in their area. The problem is that, given the prices quoted by the cartel members, any supplier who is not part of the cartel will appear to have under priced the work.

Back-to-Back Deal

The facilities manager sets up a company using nominees and gets the company onto the supplier masterfile. He then routes all the work through the company, sub-contracting the work to a genuine supplier firm. He adds a mark up on to the subcontractor's invoices and pockets the profit. This type of fraud is often found in periphery parts of the business such as office supplies, furniture and IT (areas traditionally ignored by management and controlled by budgets). A good fraudster will know how to stay within the budget so as not to warrant any undue attention. In one case the facilities manager had set up his own storage company and was charging his company £30,000 per year to store furniture in his garage. If his colleagues had carried out any due diligence on their suppliers they would have discovered his wife was a shareholder in the storage company.

Some Typical Bribes

Cash

Often seem as the typical bribe, but the hardest to account for in the books and records. Large cash payments will not go unnoticed. Companies will look for areas where cash income can be diverted or hidden to fund such payments. Small amounts are often recorded as petty cash expenses to pay for drinks or casual labour. In one case small payments of between £50 and £100 were being made to an employee in return for overlooking an overcharge of £70,000. Never estimate the size of the fraud by the value of bribe.

Labour and Materials

One of the more common methods and easiest to account for in that the labour and materials can be written off to other projects. The supplier can even produce an invoice - it will just never be paid. If an investigation is underway into alleged corruption within a company a trip to the planning office to see which of the suspects has had some building work done may prove productive.

Holidays

Another favourite is the two weeks in the supplier's villa in Spain, which of course was empty for those weeks. The employee can even justify it, as he has not received any payment or gift. In reality he has two weeks free accommodation, but it will be difficult to prove. Look out for postcards in the office.

Sponsorship

Most prevalent where there is no conflict of interest policy. The supplier can invest thousands in the employee's favourite hobby quite legitimately and if anyone asks he can point to the logo to demonstrate the whole thing is out in the open.

Consultancy Fees

In this case the employee or spouse has a small consultancy business which the supplier pays a fee to for some bogus advice. An easy way to account for the bribe and in some cases the supplier will include the figure in its production costs. Once again it is worth checking to see if employees or relatives hold directorships in any consultancy companies.

Credit Cards

The supplier provides the employee with one of his company credit cards and pays the bill. The employee is free to use it as he wishes and the supplier will account for the payment.

For more information about our corporate investigations team please call one of the following members of the Dispute Analysis & Investigations practice.

United Kingdom - London and the South

Rick Helsby	020 7212 2902
Bill Cleghorn	020 7804 7314
Andrew Clark	020 7804 5761
Richard Stevens	020 7804 2616
Ian Trumper	020 7212 8340
Jon Hayton	020 7212 4210
Edwin Harland	020 7804 5843
Sterl Greenhalgh	020 7804 1648
Simon Dawson	020 7212 3830

United Kingdom - Manchester and the North

Mark Stansfield	0161 247 4082

United Kingdom - Birmingham and the Midlands

Tony Parton	0121 265 5073

Czech Republic

Roger Stanley	+42 02 5115 1205

Switzerland

John Wilkinson	+41 1 630 1550

PricewaterhouseCoopers, the world's largest professional services organisation, helps its clients build value, manage risk and improve their performance.

PricewaterhouseCoopers provides a full range of business advisory services to leading global, national and local companies and to public institutions. These services include audit, accounting and tax advice; management, information technology and human resource consulting; financial advisory services including mergers & acquisitions, business recovery, project finance and litigation support; business process outsourcing services; and legal services through a global network of affiliated law firms.

PricewaterhouseCoopers is on the World Wide Web - http://www.pwcglobal.com.

 Designed by The Studio (11192 04/00).

Your worlds  Our people