Fraud without frontiers

CRIME Corporate fraud is often oversimplified, particularly when it traverses geographical territories. However, managers can avoid committing unintentional fraud and take precautions against the deliberate miscreant, says **Guy Clapperton**

Corporate fraud can be complicated. Leave aside the employee embezzling funds or putting his or her hand in the till; easily detectable theft, though thoroughly unpleasant, can be dealt with quite straightforwardly.

But take another case: although the companies involved were not named in the initial releases, just as this article was being written, the news flashed across the wires that a UK company had been taken to court because of copyright breaches originating in its US parent company's office.

The laws governing copyright in the European Union are, of course, different from those in the United States, so it is entirely possible that this breach – assuming it does not simply go away on appeal – might have been perfectly innocent in terms of intentions. Damage can still be done and, once the names emerge, the companies involved will be kicking themselves that the issue ended up in court.

This is a point made by a number of experts: a crime may have been committed internally, but police action is not necessarily the most appropriate step. John Horan, a consultant with Wolters Kluwer Financial Services (WKFS), points out that if there is a criminal act taking place then employers might be obliged to report it, but if there is a grey area it can be counterproductive.

"The police are very perpetrator-focused, whereas the client is going to be very loss-recovery focused," he says. And this is not a criticism; an ex-policeman himself, he believes the police are right in their focus but it might not serve the client or victim best. "The client will also be looking to manage their reputation," he says.

It is perhaps for that reason that so many people prefer to use a software solution when their company reaches the size at which they cannot control the problem just by talking to employees. Mr Horan comments that if someone owns a very small business, employing say five or six people, then they will not prioritise spending money on very expensive software tools to track every transaction.

TRANSACTIONS

And it is the transactions that tell you when something might be going wrong. WKFS offers software that analyses what is going on in accounts and reports immediately there is any unusual activity. There might well be good reasons for this unusual activity and not every alert leads to action being taken.

Joel Tobias, managing director of fraud specialist CY4OR (pronounced syfour), believes that monitoring bank accounts is by far the best way to detect when something is wrong. "Misappropriation of funds, purchase-order fraud, embezzlement, mortgage fraud, it all comes down to electronic transactions," he says. This is why his company offers its forensic service in which a business can hand over its computers and CY4OR checks every email, every document, for suspicious activity.

A business that thinks it is being defrauded will almost certainly co-operate with a forensics company like this. But several organisations, including some substantial concerns, are now allowing employees to buy their own computers – in the same way you get a car allowance, they offer a computer allowance – so the equipment is not the property of the business and they cannot hand it over for examination. "In the same way that lawyers can get orders for people to hand evidence over, we can apply if we have sufficient evidence," Mr Tobias says.

Many people will be more interested in how to avoid being in this sort of position than in what a forensics company does after the proverbial horse has bolted. Mr Tobias urges that rigorous IT policies should be in place, with back-ups taken diligently, so there is always an auditable trail of every event that happens on the network and why it has taken place.

INNOCENT PARTY

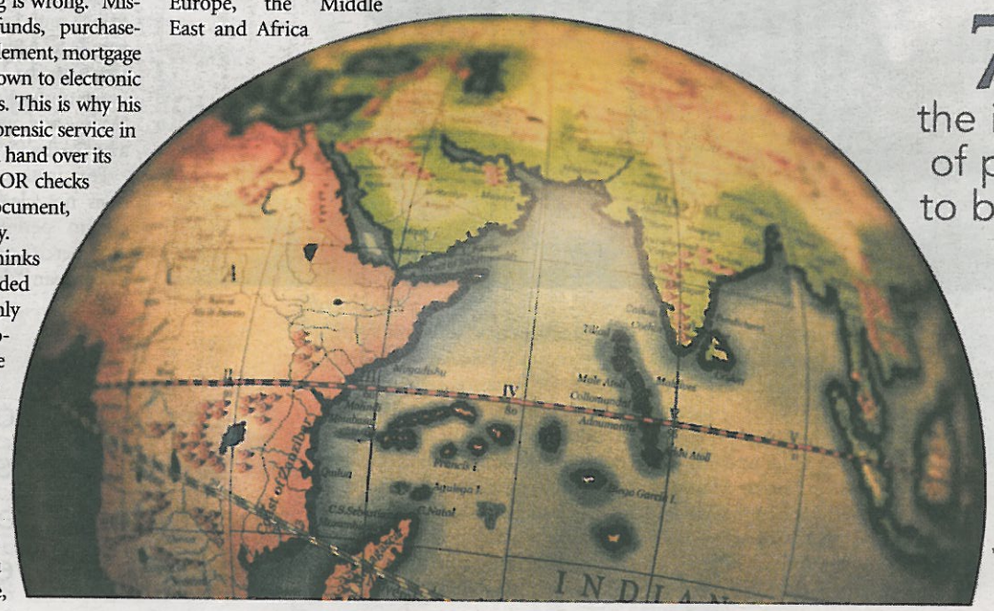
The earlier example, of the American company instructing its UK outlet to do something which turned out to be against our laws, bears no suggestion, without further information, that there was any intention of wrongdoing. Likewise, organisations can discover that they have picked up a partnership with someone who is doing something wrong and this can end up reflecting badly on the innocent party.

Suppose you owned a corporation, decided to start sourcing rivets from company X in country Y but found later that the managing director of company X was the nephew of the minister for industry in country Y. Not your fault, you might think, and maybe not technically fraudulent but certainly corrupt and unethical.

Robert Mitchell, head of enhanced due diligence at World-Check in Europe, the Middle East and Africa (EMEA), explains that his organisation works with a number of financial institutions and checks through every conceivable relationship with the directors of organisations with whom their clients are thinking of working. "We want to find out if a director of the new supplier is the trade minister's son or something," he says. "It's easy in the UK because of electronic records held at Companies House, but in other countries, even in Europe, you can be looking at a trawl through paper records."

John Evans, consultant with Logica, says that a number of legal safeguards have been put in place recently, so if someone puts £10,000 or more into an account in cash then this is reported, as a matter of course, to the UK Financial Intelligence Unit at the Serious Organised Crime Agency. Frequently there is an innocent explanation, of course. But criminals, like drug dealers for example, are aware of the laws so they have a network of people – known as smurfs – who deposit smaller amounts (withdrawing the cash is called smurfing). However, the Financial Action Task Force (FATF), an international body, is on the look-out for precisely this sort of money-laundering activity.

Corporate fraud sounds so simple. Someone understands the system, works it to their advantage and walks off with the proceeds. The point in question is when it is not deliberate, damage to reputation can still be severe. Fortunately, there are services and legislation to protect honest businesses at least from most of it.



The challenge of countering money laundering

Of anti-money laundering (AML) experts meeting in Florida last month:

91 per cent said the rise in organised financial crime was a problem

100 per cent were focused on this and the regulations surrounding it

76 per cent found tackling financial crime a challenge due to budget constraints

77 per cent said the increasing volume of payments needing to be scanned was an issue

61 per cent thought there were inefficiencies in payment-filtering operations