

# DEALING WITH FRAUD

As if those involved in running companies did not have enough to worry about in these challenging times, there is ample evidence that they are at an increased risk of loss through fraud. As companies struggle for credit and managers fear for their jobs, there is an increased risk that more managers will cook the books. As more managers lose their jobs, controls will be weakened, exposing companies to fraud.

Fraud impacts on companies both big and small. PWC's annual global economic crime survey estimates that almost half of all businesses suffer from fraud. A survey of nearly 900 international companies by the Economist Intelligence Unit for Kroll, an international security firm, found they lost an average of \$8.2 million to fraud during the past three years, with 85% reporting at least one serious incident in the period.

## SIGNS OF FRAUD

There are a number of characteristics which a fraudster may typically exhibit which, if observed, may serve at least as a flashing light for possible fraudulent conduct. These include:-

- **Tight control**  
The employee may seem unusually hard-working and refuse to take holidays. This is because he dares not leave the books and records for others to review in his absence. He will tend to keep information to himself and avoid delegating.
- **Manipulation**  
The employee is able to hoodwink his management by providing complicated responses which are not understood, or by establishing that he is not an easy person to deal with, discouraging bosses from asking searching questions.
- **Does not provide information**  
The employee will use delaying tactics, is unable to attend meetings, is evasive, does not provide the information requested.
- **Flamboyant lifestyle**  
If an employee is living a lifestyle that is lavish in comparison with his salary, this could be an indicator of fraud risk. The expenditure being incurred is sometimes passed off as the result of an inheritance or marriage to a wealthy spouse.

## THE CHARACTER OF THE FRAUDSTER

According to a survey carried out by KPMG in 2007 "Profile of a Fraudster", 89% of the fraudsters interviewed were employees, 60% were senior managers, including board members, 85% were male (although this may reflect the fact that there are fewer women in senior management) and 70% were aged between 36 and 55. In over two thirds of cases, the perpetrator acted alone. Further, the majority of fraudsters tended to be long serving employees

## COMMON TYPES OF FRAUD

Although fraud is diverse, the process involved in the fraud often falls into distinct types. A few common examples include:-

- **False Sales**  
False sales can involve the adjustment of quantities or prices with a view to increasing turnover. Dummy invoices may be issued, old invoices may be re-dated. Kickbacks may be paid to customers in return for higher prices.
- **Advance billing**  
This occurs when a sale is booked in breach of accounting rules in order to bring it into the accounts
- **Procurement fraud**  
These take many forms, including bid fixing, billing for work not performed, dealing with intermediaries and undertaking work for private purposes.
- **Stock fraud**  
Employees may claim that goods are damaged, following which they are written off and then sold on by the employees. It is not unusual for theft of stock to involve a number of employees, who regard such activities as little more than a perk of the job.

## HOW TO RESPOND IF A FRAUD IS SUSPECTED

If a company believes that a fraud has been committed, we would strongly recommend that before confronting the suspect, it should consult its legal advisers in order to plan the strategy and process for the investigation. Speed is of the essence. Matters to consider include:-

- the legal rights of the company to suspend or dismiss the suspect; can the employer prevent an employee from access to the office workplace and computer network whilst the investigation is under way?
- establishing what evidence has been obtained, and where additional evidence is likely to be kept. It is vital to secure the documentary and electronic evidence as soon as possible. We have come across examples of employees being tipped off about an investigation and then taking rapid action to delete incriminating information from computers before they are questioned. Is there evidence that relevant information is likely to have been kept on the home computer of the employee, which could be secured through an appropriate court order? Does the suspect have use of an office-supplied laptop?
- who is to conduct the investigation and the form it will take? Should the suspect be shown the evidence already obtained or should this be kept back, at least initially?
- the reporting structures for the investigation. Should a special committee of the Board be formed?
- what is believed to have happened to the proceeds of the fraud? Is this a case in which freezing injunctions will need to be sought in order to prevent dissipation?
- should the matter be reported to the Police and if so, at what stage of the investigation?
- what role should be taken (if any) by internal auditing staff and by external forensic accountants?
- issues concerning confidentiality – who within and outside the company already knows about the investigation? What, if anything, is to be said to the company at large, or to the media?

## GENERALLY

There has never been a better time for companies to review their fraud risk management strategy (or to establish this if they do not have one), despite other pressures. Anti-fraud strategy needs to be a top down commitment which is reviewed regularly by the board. This is not just another cost, but is a process which can prevent huge damage to a company and which may well identify organisational weakness, which can then be strengthened.

*For further information or assistance in relation to the above issues, please contact Justin Ede on 01306 502209 or by email: [j.ede@downslaw.co.uk](mailto:j.ede@downslaw.co.uk). Justin has advised on numerous fraud matters.*