Employee fraud – the internal challenge

With the economy in a double dip recession, pay freezes and non-payment of bonuses the threat of employee fraud has never been greater.

We frequently read about fraud in big companies and large scale ponzi schemes, but these frauds are often motivated by greed or pressure to out perform. But the majority of frauds committed by employees are not on this grand scale and, as Jane Fowler, Managing Director of Aquila Advisory, the boutique forensic accounting company explains, the businesses most at risk are small and medium sized companies.

The majority of businesses in the UK employs fewer than 50 employees and many don't have sufficient resources for an extensive system of controls, including the ability to affect segregation of duties. This makes them vulnerable to employee, or internal fraud.

Obviously, we all look to recruit people we like and trust and have employees whom we have known and trusted for many years. But what happens when their personal circumstances change. Maybe their partner has lost their job or they over stretch themselves with the mortgage at a time when growth was expected to continue. Their savings are all used up and they now face losing their home. Circumstances can and do change and this is often when a fraud can occur.

Fraud can be defined as obtaining a financial or personal gain through wrongful or criminal deception. It is said that there are three factors that are present in each fraud, Motive, Opportunity and Intent. There is little that a business can do to affect motive and intent - they are influenced by external forces, such as those referred to above - but opportunity is entirely in the control of the business.

Businesses, now more than ever, need to be vigilant to the risk of fraud.

Types of Employee Fraud

Employee fraud can be perpetrated by individuals working alone or in complicity with others, be they other employees or third parties. Examples of frauds committed by internal parties include:

- Direct theft of cash or realisable assets, such as laptops, stock or intellectual property, followed by continued deception to cover the theft;
- Obtaining money by deception through false expense claims;
- Payroll fraud through the diversion of payments, creating fictitious employees, making payments to ex-employees or over estimating hours worked.

As stated above, a company could also be susceptible to fraud from employees in collusion with third parties, such as:

- Receiving kickbacks or commission from suppliers;
- Intimidation from third parties to disclose confidential information, eg customer lists, price lists or being forced to process inappropriate transactions

- Related party transactions, whereby an employee or officer of the company has an undisclosed financial interest in a transaction

Signs of Employee Fraud

If we are considering how to identity fraud within a business, we need first to consider what the signs of fraud are. Here are some examples:

- Changes in employee behavior, such as:
    - Increased levels of stress which are not commensurate with an increase in workload
    - A lifestyle not commensurate with their salary
    - Reluctance to take annual leave
    - Unwilling to delegate or accept promotion
    - Works late or unusual hours
    - Increase in customer or staff complaints relating to that individual
    - High turnover of staff working with or for them.
- Changes in cashflow:
    - Poorly reconciled expenses
    - Discrepancies in level of expenses between outlets/branches
    - Cash only transactions
    - Poorly reconciled customer accounts, generally containing unreconciled items
    - Large volume of refunds to customers or credit notes issued
    - Repetitive journal entries with little or no backing papers often for round sum amounts.
- Stock shrinkage:
    - Poorly conducted stocktakes
    - Unreconciled differences between book and actual stock
    - Amounts written off as wastage
    - Lower than expected gross margins
    - Higher than expected stock turnover

Prevention of Employee Fraud

The first stage in preventing fraud within an organisation is to make it clear that instances of fraud will not be tolerated and action will be taken. The most effective way to demonstrate this to staff is to issue an Anti-Fraud Policy Statement. The Policy should make it clear that all instances of suspected fraud will be investigated and, if found to have merit, staff will be prosecuted.

Obviously, this alone will not be sufficient to protect the business. Checks and controls are necessary, even in the smallest companies. Whilst we can't all afford an Internal Audit department, there are simple controls that all businesses can implement:

- Stocktaking - the stock take should be undertaken by someone independent from those normally responsible for stock. If, in relation to your business, stock is highly desirable or of significant value, you may consider periodically engaging an external firm of stocktakers and auditors. Specialist firms exist for most industries and are reasonably inexpensive.
- Account Reconciliations - such as bank, debtor, supplier and payroll reconciliations. If possible, performance of these reconciliations should be rotated amongst accounts staff

and reviewed by an external accountant when preparing the annual accounts or VAT return, even if a full audit is not required.

- Review of management accounts - for unexpected fluctuations particularly in margins. For the review to be most effective it is necessary for the management to have an expectation of the results that they can compare to actual. So they don't just review monthly fluctuations, but look to see if the results actually demonstrate what is expected. If frauds are perpetrated over a period of time, a review of monthly fluctuations will not uncover the fraud. Any unexpected fluctuations should be noted and followed up by management.
- Monitor corporate credit card and bank statements - for unusual transactions. Ensure everyone is required to account for their expenditure, no matter how senior a position they hold. Once one party is seen as not accountable, the anti-fraud ethic is lost.
- Establish a whistleblowing policy - this can be as valuable as internal controls. Most employee frauds are spotted by other employees suspicious about how an individual can maintain a particular lifestyle, i.e. car they drive, holidays they take, their Rolex watches etc.
- Vetting of employees on recruitment - it is not just important to follow up on their previous employment history and their qualifications (approximately 80% of employees lie on their CV). If the employee is to have access to financial systems or sensitive data, it is advisable to confirm their identity, their credit worthiness and perform a fraud prevention check.
- Ongoing employee vetting - of course, as we said at the outset, circumstances can change. It is therefore advisable to perform ongoing checks on your employees, be they credit checks or fit and proper checks (required in some industries).

Responding to Employee Fraud

As we have said an essential part of any anti-fraud policy is to be prepared to respond to suspicions of fraud as they arise. A fraud response plan would set out:

- The investigation process: who, when and how. Smaller business may wish to identify an external provider for this ensuring the requisite skills are available
- Legal and ethical duties to report: shareholders, customers, bank, insurance company and/or regulators
- Reporting the matter to the police: it is important your other employees see that you take a hard line on fraud to act as a deterrent to future frauds.
- Reviewing your internal controls to tighten any loopholes: don't be afraid to learn lessons from what has happened, a good risk response should always be evolving.

Whatever your fraud response plan, you need to make sure that you are prepared to respond to any incidents of suspected fraud within your organisation swiftly and decisively.

Case Study 1

Those of you that are old enough to remember the blatant theft of monies from the NSPCC in the 1990s, will appreciate that frauds can go undetected for years and be committed by people everyone trusts.

In this particular case, a chief cashier working at the NSPCC's headquarters in London opened up a savings account at the Post Office in the name of N SPEED and paid in cheques and postal orders made out to the NSPCC. He was able to do this by altering the Payee details from NSPCC to N.SPEED by turning the C's into E's and adding a D.

When suspicions were raised about his lifestyle not being commensurate with his salary - he had bought a £200,000 luxury house in Sussex, a £200,000 villa in Spain, two cars, life insurance policies and other investments - he pleaded guilty to 19 charges of theft and 3 of forgery, committed over a 6 year period.

He had been an employee of the NSPCC for 11 years, and had therefore worked for the Charity for 5 years without incident prior to making the decision to commit the fraud.

This fraud could have been prevented by appointing two people to open the post and logging amounts received. These receipts should also have been banked and reconciled by separate members of staff. Given the importance and materiality of cash receipts in this instance, the investment in resources would have been worth it.

Case Study 2

Another case involved a sportswear manufacturer and distributor. In this instance a woman who worked for the company discovered a weakness in the credit note authorisation procedures, in that it required different authorisation levels for credit notes of different values, eg:

< £5,000	Credit Controller
>£5,001 < £10,000	Financial Controller
>£10,001 < £20,000	Finance Director
>£20,000	Two Directors

However, because the values in the computer progamme did not include a sign for equal to, i.e. ≤ ≥ instead of < and >, no authorisation was required to issue credit notes for exactly £5,000, £10,000 or £20,000.

The woman, who didn't work in the accounts department, but knew not only of the weakness in the system but also the login details (which were written down just in case anyone needed them), had her husband open a sportswear shop and order stock from the company. She was then able to access the accounts system and issue credit notes on her husband's account each month prior to statements being issued. She always left some balance to be paid so as not to draw attention to the account. Again, this fraud was not discovered until other employees became suspicious about her lifestyle: holidays, Prada handbag, dinners etc.

This particular fraud could have been detected earlier by running exception reports on the credit note system highlighting frequent credit notes issued to the same customer, credit notes for round number sums or same sum amounts.

Case Study 3

In this instance a car body repair centre, approved to carry out insurance work, pays staff based on estimated hours. This means that for each insurance job the mechanic estimates the number of hours the job will take and the mechanic is paid on the basis of this estimate, rather than actual hours worked. This is thought to incentivise the worker to work efficiently … if they complete the job quicker they effectively receive a bonus.

In order to prevent this approach being abused, all time estimates had to be authorised by the repair centre manager prior to the timesheets being entered into the payroll system.

In this case, the repair centre manager worked in collusion with a mechanic to overestimate the hours required. They then split the increased pay, something that was made easier given their affair.

Suspicions were raised by an eagle eyed Payroll Manager, when the pair became so greedy that their estimate of hours differed vastly to any other mechanic working in the repair centre and regularly exceeded the number of hours in a week.

Employee Fraud - in conclusion

Whilst many small and medium sized companies do find it difficult to find the time and resources to implement these preventative measures, every business is susceptible to internal fraud in one way or another. It is therefore essential to establish an appropriate and effective anti-fraud policy and to be prepared to respond to suspicions of fraud as they arise.

The 'do nothing' option is there, but beware! Whilst the majority of staff in any organisation are trustworthy, against a challenging background where many employees are experiencing financial hardships, internal fraud is more prevalent now than ever before. And doing nothing in the hope this situation won't arise, could end up being more costly to your business than you may realise. So be prepared. Put measures in place now to alleviate temptation and detect fraud in your business.

At Aquila Advisory, we work with businesses across all sectors, helping them and their clients to implement anti-fraud policies. We understand the impact a fraud can have on a business and, where a fraud is suspected, we undertake discreet work to investigate suspicious activity, detect fraud, collate evidence and advise on the appropriate course of action.

So contact us today for a free initial consultation and to find out how we can help you protect your business against employee fraud.

CONTACT AQUILA ADVISORY:

Jane Fowler, Managing Director

Tel: 020 7397 8318
Email: info@aquilaadvisory.co.uk
Website: www.aquilaadvisory.co.uk