Guide
June 2012

in association with

CIFAS
The UK's Fraud Prevention Service

Staff fraud and dishonesty

Managing and mitigating the risks

This guide has been produced jointly by CIFAS and the CIPD to help HR professionals understand the threat from staff fraud and dishonesty and help manage and mitigate the risks.

CIFAS – the UK's Fraud Prevention Service – is a not-for-profit membership association solely dedicated to the prevention of financial crime with more than 250 member organisations from across the public and private sectors.

The Chartered Institute of Personnel and Development (CIPD) is the professional body for those involved in the management and development of people and has 135,000 individual members.

Contents

Introduction

Most staff within any organisation are trustworthy and honest. However, businesses do realise and understand the scale of the threat posed by the small proportion of staff who act dishonestly and defraud their employer.

In an increasingly competitive marketplace, many businesses have responded by empowering staff and undertaking structural reforms. These changes aim to raise levels of customer service and enhance customer satisfaction. Paradoxically these changes, combined with the ability to undertake more financial transactions remotely, have also created more fertile conditions, scope and opportunity for dishonest action by staff.

The way in which organisations approach the issue of staff fraud is changing to respond to that increased risk. Historically, many organisations have been anxious to play down the threat from within and have been reluctant to admit to the scale of the problem or the associated financial losses. Increasingly, however, the days when HR would handle most staff fraud cases quietly with no publicity, allowing the dishonest employee either to resign discreetly or be dismissed inconspicuously, are long gone. Indeed, a number of businesses are now adopting best practice by sharing data actively with each other – under carefully controlled conditions – on incidences of staff fraud within their organisations.

The Government Fraud Review of 2006 stated that one of the strategic responses to counter fraud was to *'present a comprehensive understanding of the nature of fraud'*. Recent research by CIFAS – the UK's Fraud Prevention Service – has shown that staff fraud has continued to increase steadily, rising by 40% in the last three years. This in turn demonstrates that staff fraud continues to be a significant risk to all business sectors. The growing threat from staff fraud can be combated effectively by organisations in two ways: by co-operating and adopting a common approach that encompasses zero tolerance of all types of staff fraud and by introducing a rigorous anti-fraud internal culture that promotes honesty, openness, integrity and vigilance throughout the workforce.

The challenge lies not simply in ensuring that the correct policies are in place to facilitate such an approach and culture, but also in ensuring that such policies are consistently followed, rather than being compromised for convenience or expediency.

However, employers must tread a line between, on the one hand, ensuring that employees do not misuse business property or systems or carry out any illegal activity and, on the other, fostering a culture of mutual trust and respect.

This can be done by adopting a risk-based approach which takes into account the nature of the business, the industry sector and different job roles. If employers communicate clearly why they are adopting a particular approach, for example on staff monitoring, as well as the potential risks to the business, employees are more likely to see measures put in place as reasonable and necessary. If organisations simply impose what staff perceive as excessive supervision or controls, employees are more likely to have negative attitudes towards the organisation they work for.

In the summer 2011 *Employee Outlook* survey of employees, the CIPD identified that some staff had job fears; that their job satisfaction was low; that there was a lack of trust, with negative attitudes towards senior officers; that they felt they were under excessive pressure; and struggled to meet bills. CIFAS members also identified three major triggers which led to staff committing fraud against their employers, namely: fear of losing their job; 'revenge' against employers for grudges such as low pay or being passed over for promotion; and increasing pressure of work. It is therefore important that organisations implement controls to relieve these pressures and that they communicate properly with their staff.

The purposes of this guide are to raise awareness of the potential threat posed by staff fraud and dishonesty and to provide examples of generic best practice that can help employers manage and mitigate the related risks. Due to the diverse nature of organisations and businesses, implementing a standardised approach to staff fraud would not be feasible or practicable. However, there are a number of best practice policies and procedures that all organisations should consider following to ensure that they are at least complying with their regulatory obligations.

1 What is staff fraud?

'Staff fraud undermines the reputations of organisations and their management. Across the private sector, public sector and third sector, no organisation is immune to its impact, whether it is high-profile data theft, cash being stolen or sophisticated accounting scams. Where management is negligent by allowing unreformed fraudsters into their organisation, heads should and do roll.' **Peter Hurst MCIPD, Chief Executive, CIFAS – the UK's Fraud Prevention Service**

Defining what 'staff' means

For the purpose of this guide, the term 'staff' is defined as any individual with a contractual arrangement, whether directly or indirectly (for example through a recruitment agency), to provide their personal services to an organisation. This therefore includes, but is not restricted to, permanent staff, temporary staff on short- or fixed-term contracts and staff supplied by a recruitment agency or third party.

Defining what 'fraud' means

Before the Fraud Act was introduced in 2007, there was no legal or established definition of fraud. Indeed, there are still differing perceptions of fraud. For example, some organisations will view uncollectable debt and money laundering as fraud while others may not.

Although the Fraud Act now provides a legal definition, there are other fraud-related cases that could be reported as offences under other Acts, for example, the Theft Act offence of false accounting.

Staff identified as committing fraud who have been reported to the police are usually charged with offences relating to the following pieces of legislation:

- Theft Act 1968 (as amended)
- Forgery and Counterfeiting Act 1981
- Computer Misuse Act 1990
- Data Protection Act 1998
- Criminal Attempts Act 1981
- Copyright, Designs and Patents Act 1988.

The Fraud Act, which came into effect in 2007, broadly defines three main types of fraud:

- fraud by false representation
- fraud by wrongfully failing to disclose information
- fraud by abuse of position.

For a fraud to be committed under this new legislation there must have been an identifiable intent by the individual to make a gain or to cause a loss or to expose another to the risk of loss.

Fraud by false representation

An individual dishonestly and knowingly makes a representation that is untrue or misleading.

Fraud by wrongfully failing to disclose information

An individual wrongfully and dishonestly fails to disclose information to another person where they have a legal duty to disclose it, or where the information is of a kind that they are trusted to disclose, or they would be reasonably expected to disclose.

Fraud by abuse of position

This is where an individual who has been given a position in which they are expected to safeguard another person's financial interests, dishonestly and secretly abuses that position of trust without the other person's knowledge.

Therefore for the purpose of this guide the term 'fraud' encompasses those occurrences where a person dishonestly makes a false representation, wrongfully fails to disclose information or abuses a position of trust, with the intent to make a gain or to cause a loss or to expose another to the risk of loss.

The term 'staff fraud' in this context is also known as:

- employee fraud
- insider fraud
- internal fraud
- workplace fraud.

Types of staff fraud

Thee are numerous types of fraud that can be perpetrated by staff against their employer. Depending on the nature of the business and the products and services offered, members of staff may have many opportunities to commit fraud or pressures on them that lead them to do so. Each business and organisation will have its own particular risks and threats and there are additional ones that arise in relation to job role, responsibility and seniority. Fraudulent activity can range from compromising customer or payroll data to straightforward theft or the submission of inflated expenses. Staff fraud can have an 'opportunistic' element, that is, undertaken by an individual for personal financial gain, or can be linked to a serious and organised criminal network or terrorist financing. Staff can also feel pressured into fraudulent activity because of debt, mounting bills or gambling debts, for example. Opportunities and pressures are discussed in further detail on page 12, which looks more closely at why staff commit fraud. All organisations have vulnerabilities and all organisations have some level of risk.

The first serious attempt to create a detailed typology of staff fraud within the UK was undertaken by CIFAS. Although the intention was not to create an exhaustive list, CIFAS determined that most types of fraud perpetrated by staff could be broadly grouped into five main categories:

- employment application fraud
- unlawful obtaining or disclosure of personal data
- unlawful obtaining or disclosure of commercial data
- account fraud
- dishonest action by staff to obtain a benefit by theft or deception.

Employment application fraud	
Use of a false identity	an application either for employment or to provide services, where the applicant uses a false identity, for example a forged passport
Impersonation of an innocent party	an application either for employment or to provide services, where the applicant has impersonated an innocent party
False documents	an application either for employment or to provide services, where the applicant has provided false documents, for example a counterfeit UK passport
False immigration status	an application either for employment or to provide services, where the applicant uses a false immigration status
False qualifications	an application either for employment or to provide services, where the applicant uses false qualifications, which are considered a material falsehood*
False references	an application either for employment or to provide services, where the applicant uses false references, which are considered a material falsehood*
Concealed employment history	an application either for employment or to provide services, where the applicant conceals their employment history, which is considered a material falsehood*
Concealed employment record	an application either for employment or to provide services, where the applicant conceals their employment record, which is considered a material falsehood*
Concealed unspent criminal convictions	an application either for employment or to provide services, where the applicant conceals an unspent criminal conviction
Concealed adverse credit history	an application either for employment or to provide services, where the applicant conceals their credit history, which is considered a material falsehood*

*A material falsehood involves the commission of, or the attempt to commit, a criminal offence in relation to an application for employment or an application to provide personal services. The material falsehood should be one that would affect any decision to offer a post to an applicant, or for an existing staff member or service provider to remain in their post or move to a new post.

Unlawful obtaining or disclosure of personal data	
Contravention of IT security policy	the contravention of IT security policy for unauthorised purposes with intent to facilitate the commission of a further criminal offence, for example passing data to third parties, creating instruments/documents/payment instructions to facilitate a fraud, to view own account details (or accounts of friends/relatives), to 'surf' for likely victims/targets of fraud, to download unsuitable material from the Internet, to misuse email systems and distribute offensive material/ viruses
Contravention of systems access policy	the contravention of systems access policy for unauthorised purposes with intent to facilitate the commission of a further criminal offence, for example passing data to third parties, creating instruments/documents/payment instructions to facilitate a fraud, to view own account details (or accounts of friends/relatives), to 'surf' for likely victims/targets of fraud, to download unsuitable material from the Internet, to misuse email systems and distribute offensive material/viruses
Contravention of Internet policy	the contravention of Internet policy for unauthorised purposes with intent to facilitate the commission of a further criminal offence, for example passing data to third parties, creating instruments/documents/payment instructions to facilitate a fraud, to view own account details (or accounts of friends/relatives), to 'surf' for likely victims/targets of fraud, to download unsuitable material from the Internet, to misuse email systems and distribute offensive material/viruses
Contravention of email policy	the contravention of email policy for unauthorised purposes with intent to facilitate the commission of a further criminal offence, for example passing data to third parties, creating instruments/documents/payment instructions to facilitate a fraud, to view own account details (or accounts of friends/relatives), to 'surf' for likely victims/targets of fraud, to download unsuitable material from the Internet, to misuse email systems and distribute offensive material/viruses
Fraudulent personal use of customer/payroll data	the personal use of customer/payroll data to facilitate a fraud
Disclosure of customer/ payroll data to a third party	the disclosure of customer/payroll data to a third party to facilitate a fraud
Modification of customer payment instructions	the unauthorised modification of customer payment instructions to facilitate a fraud, for example direct debits, standing orders, and so on
Unauthorised alterations to customer data	the unauthorised alteration of customer data to facilitate a fraud, for example change of address, security details, and so on

Unlawful obtaining or disclosure of commercial data	
Contravention of IT security policy	the contravention of IT security policy for unauthorised purposes with intent to facilitate the commission of a further criminal offence, for example passing commercial data to third parties
Contravention of systems access policy	the contravention of systems access policy for unauthorised purposes with intent to facilitate the commission of a further criminal offence, for example passing commercial data to third parties
Contravention of Internet policy	the contravention of Internet policy for unauthorised purposes with intent to facilitate the commission of a further criminal offence, for example passing commercial data to third parties
Contravention of email policy	the contravention of email policy for unauthorised purposes with intent to facilitate the commission of a further criminal offence, for example passing commercial data to third parties
Theft of internal policies/ procedures/practices	the theft of internal policies/procedures/practices
Disclosure of internal policies/procedures/ practices to third parties	the disclosure of internal policies/procedures/practices to third parties
Theft of intellectual property	the theft of intellectual property
Theft of IT systems source code	the theft of IT systems source code; this may be to enable third parties to mimic internal IT architecture or introduce fraudulent payment instructions
Infringement of copyright	the theft of or unauthorised dealing with articles infringing copyright

Account fraud	
Fraudulent account transfer to employee account	the fraudulent electronic transfer of funds from a customer account to an account controlled by a member of staff
Fraudulent account transfer to third-party account	the fraudulent electronic transfer of funds from a customer account to an account controlled by a third party
Fraudulent account withdrawal	the fraudulent withdrawal of cash from a customer account without the customer's knowledge or authority

Dishonest action by staff to obtain a benefit by theft or deception	
Theft of IT equipment	the theft of IT equipment, for example monitors, PCs, keyboards, modems, printers, mice, cables, laptops
Theft of fixtures and fittings	the theft of fixtures and fittings, for example desks, chairs, cupboards, pictures, display stands, plants, and so on
Theft of office equipment	the theft of office equipment, for example stationery or electrical equipment such as kettles and microwaves
Theft of consumables and instruments	the theft of consumables and instruments, for example payment cards awaiting collection, cards recovered in ATMs, chequebooks, returned/undelivered mail, blank drafts, blank cheques and other negotiable instruments awaiting use; also includes the theft of headed paper and other internal forms for use in subsequent frauds
Theft of personal property	the theft of personal property while on employer premises, for example clothing, mobile telephones, cash and wallets belonging to other members of staff
Theft of goods or products	the theft of goods or products from warehouses, during distribution or on the shop floor
Theft of cash from employer	the theft of cash from tills, ATMs, strong rooms, safes, travellers' cheques and foreign currency awaiting collection or sale and cheques received as payment for services/fees/commission
Theft of cash from customer	the removal of personal cheques from customer chequebooks and the theft of items held within approved deposit facilities or under safe custody arrangements
False expenses/overtime/ timesheet submission	the submission of a false or inflated claim for business-related expenses/overtime or timesheet submission
Manipulation of personal account	the manipulation of internal accounting or IT systems with an intent to defraud, for example changing overdraft account limits or interest rates applied to personal accounts
Manipulation of a third-party account	the manipulation of internal accounting or IT systems with an intent to defraud, for example changing overdraft account limits or interest rates applied to third-party accounts
Removal of charges from personal account	the manipulation of internal accounting or IT systems with intent to defraud by removing or reducing the charges applied to personal accounts
Removal of charges from third-party account	the manipulation of internal accounting or IT systems with intent to defraud by removing or reducing the charges applied to third-party accounts
False/manipulated sales submission	the fraudulent submission of false or manipulated sales or performance-related measures with the intention of increasing a bonus or reward payment, for example selling products/services or falsifying accounting records to increase sales/rewards
Manipulation of bonus/ reward scheme	the fraudulent manipulation of sales or performance-related measures with the intention of increasing a bonus or reward payment, for example selling products/ services or falsifying accounting records to increase sales/rewards

Dishonest action by staff to obtain a benefit by theft or deception (continued)	
Facilitating fraudulent applications	facilitating applications with an intent to defraud
Manipulation of applications/proposals/ claims	manipulating applications/proposals/claims with an intent to defraud
Manipulation of application systems	manipulating application systems, for example ignoring anomalies in applications for products and manipulating application systems to influence scoring processes or loan amount decisions
Perpetrating fraudulent applications	making applications for products with an intent to default/defraud
Facilitating/perpetrating false insurance claims	facilitating or perpetrating false insurance claims with intent to defraud, including the submission of false statements and false supporting evidence
Procurement fraud – personal	the creation of false or inflated supplier invoices for payment and other types of procurement fraud without colluding with any third parties
Procurement fraud – collusion with third parties	the creation of false or inflated supplier invoices for payment and other types of procurement fraud through collusion with third parties, for example inappropriately awarded contracts
Facilitating transaction fraud	knowingly accepting false ID to support fraudulent transactions and the facilitation of the processing of transactions on stolen/counterfeit cards or altered instruments
Facilitating/perpetrating advance fee fraud	the use of headed notepaper and other forms/documents to facilitate/perpetrate advance fee fraud
Abuse of company time/ privilege	the excessive use of work time/email/phones for personal use with no relation to the business

2 Why is staff fraud a growing risk?

'Management remained unchecked during 2010, as fraud increased in this group by 20 per cent year-on-year, to £419 million. Being in a position of trust and authority enabled management to cause greater financial damage than employees.' **KPMG Fraud Barometer 2010**

'Employee theft continues to present one of the most important ongoing challenges for retailers.' **British Retail Consortium, Annual Retail Crime Survey, 2010**

'The threat of fraud from your own staff is much higher than you realise.' **BDO Stoy Hayward FraudTrack 8, 2011**

'In 2011 it appears that the majority of frauds were committed by employees, a statistic borne out of the increase in "internal" crimes such as accounting fraud.' **PricewaterhouseCoopers, 2011**

'An examination of the staff frauds recorded by members to the CIFAS Staff Fraud Database in 2010 reveals a 63% increase in instances of staff unlawfully obtaining or disclosing personal data with younger age groups more likely to be involved.' **CIFAS Staff Fraudscape, May 2011**

Increasing incidences of staff fraud

General intelligence and specialist research suggests that incidences of staff fraud have been growing for a number of years. Traditionally, many organisations have been reluctant to admit the scale of the problem due to potential reputational damage. It has now grown to such an extent, however, with increasingly evident links to organised crime, that specific countermeasures are required. This has raised the profile of the issue with regulators such as the Financial Services Authority (FSA), with law enforcement agencies and across the public sector.

The actual number of confirmed cases of staff fraud is rising sharply throughout the diverse membership of CIFAS. Meanwhile, research indicates that theft by store employees in the retail sector is much greater than has hitherto been supposed, although it should be remembered that the number of staff involved in fraud remains at a relatively low level. Large organisations employing more than 80,000 people can expect to dismiss in the region of 100–150 members of staff a year for fraudulent activity. This figure is likely to be an underestimation of the true scale of the problem. Research suggests that many staff fraudsters go undetected, while others resign during or prior to an internal investigation. This can often prevent their dismissal and detailed analysis or investigation of any fraudulent activity undertaken.

CIFAS research has shown that staff fraud has increased by over 40% in the last three years. In general there are more cases of staff fraud and this trend has been underpinned by the profile of the issue being raised through extra staff training and awareness, embedding an anti-fraud culture in organisations and the introduction of more robust internal controls. Some organisations have seen an increase in the number of staff fraud referrals made to the relevant fraud department.

Why are there more incidences of staff fraud?

It has been established that in recent years staff fraud has been identified as a significant threat. Broadly there are three interlinked reasons for this:

- the changing nature of business and organisational structures
- the changing nature of staff to service these new structures
- the increased targeting of business by organised criminal networks.

Although it is recognised that the most serious threat from staff fraud has been centred on relatively senior employees in management positions, it is recognised that the threat has also shifted down the organisational hierarchy to more junior members of staff. These staff have access to, and responsibility for, more confidential customer and payroll data than ever before.

The changing nature of business and organisational structures

During the 1970s and 1980s many businesses restructured their operations to focus on customers rather than being organised by products, branches or function. As a result, to provide quality customer service, increasingly organisations now need to have all their customer data co-ordinated together in one place and accessible by staff who work in a variety of locations, for example retail outlet, branch, contact centre, back office, and so on, both in the UK and overseas. This has resulted in the consolidation of diverse customer information into readily accessible customer databases. Such a process makes it much quicker and easier for staff to be provided with a comprehensive knowledge of their customer and removes the need to search more than one database for this information. The resulting explosion of contact and call centres created more opportunities for organised criminals to target members of staff who had ready access to these extensive customer databases. Since then, however, call centre operations have become wise to this, introducing more stringent controls and have – to a large extent – significantly reduced much of the fraud they were experiencing. That is not to say, however, that they do not need to remain vigilant, as any organisation with a concentrated pool of powerful customer or other personal data will always remain a target for fraudsters.

The changing nature of staff to service these new structures

The shift towards and growth in contact and call centres led to changes in the type of staff employed to service them. Those employed in call centres, and to a lesser extent branches and retail outlets, sometimes do not view their job as being part of developing a long-term career with their present employer. In addition to possessing limited loyalty, these employees also tend to be young, inexperienced and relatively low paid.

Therefore those staff members in possession of the information that would be most valuable to an organised criminal tend to be the most susceptible to an approach by an organised criminal.

Furthermore, retail outlets, call centres, centralised service units and similar functions tend to have high staff turnover rates and this puts added pressure on employee security vetting and screening procedures. Imposing restrictions on staff access to data and thorough vetting policies to mitigate the potential risk from fraud clearly need to be balanced against business and customer service requirements. As a result, it is imperative that such organisations bear in mind the need to screen rigorously all staff with access to customer data, and to protect the data by means of thorough, audited controls.

The increased targeting of business by organised criminal networks

There has been a massive rise in identity theft in recent years. The number of identity fraud cases recorded by CIFAS has grown from 16,810 cases in 1998 to 113,000 cases during 2011. This is an increase of 572% in 13 years. It is likely that organised criminals have helped fuel this rise substantially. Equally, intelligence from law enforcement agencies and the financial services industry suggests that organised criminals are also increasingly targeting financial institutions, both through infiltration and by attempting to corrupt existing members of staff.

Organised criminals are likely to be targeting staff not only because they are aware of the data they can access and their potential susceptibility to approaches, but also due to the increased volume of financial transactions that can now be conducted remotely. Telephone and Internet banking provides more opportunity for anonymous fraud by a third party should the fraudster be in possession of sufficient security information, which can be obtained by fraudulent employees. The same is true for centralised finance departments that may rely on Internet facilities to communicate with other parts of the organisation and to receive invoices, and so on, for payment.

Those employees who co-operate with criminal networks are known to assist in a number of ways. At

a basic level they can facilitate fraudulent transactions or steal cash or other items to order. However, in the financial services industry, approaching staff and persuading them to acquiesce in compromising customer or payroll data to allow third parties to perpetrate identity fraud and further frauds represents the greatest area of risk.

Many commentators have asserted that the recession has had an influence on the increased risk of staff fraud. Staff may commit fraud not only for greed but also for need. (Please refer to part 3, 'Why staff commit fraud'.) However, the perception of an increased staff fraud risk may also be attributed to businesses tightening their internal controls. This may have identified more staff fraud activity that would not otherwise have been discovered.

What level of threat does staff fraud pose?

There are four main interconnected areas of threat to consider:

- financial losses
- reputational damage
- regulatory implications
- internal impact.

Financial losses

Historically the financial threat from staff fraud has been considered insignificant compared with the financial threat from other types of fraud. However, there is now recognition that the losses resulting from staff fraud can have a considerable impact on a business's bottom line, or a public body's budget.

For example, according to research carried out by the Centre for Retail Research for their *Global Retail Theft Barometer*, UK retailers lost £1,624 billion for the 12 months ending June 2010, which constituted nearly 37% of total shrinkage from employee theft. This has increased from 2009 and represents the highest figure in Europe. The average amount stolen by dishonest employees was £1,318, which is nearly 20 times greater than the average stolen by shoplifters.

The annual *FraudTrack Report* from accountants BDO Stoy Hayward noted that reported fraud in the UK reached over £2 billion for the first time in 2009. It also showed that the amount lost by businesses and the public sector to large frauds had increased by 76% during the economic downturn. *KPMG Fraud Barometer* measures fraud cases being heard in the UK crown court system where charges are in excess of £100,000. In 2010, KPMG identified 140 cases of staff fraud, which accounted for 45% of all fraud cases. This resulted in financial losses of £548 million, which accounted for 30% of all losses to fraud. Therefore, the average staff fraud cost £4 million. To compare these figures with customers involved in fraud, only 59 cases were identified, accounting for 17% of all fraud cases. Furthermore, customers involved in fraud resulted in financial losses of £102 million, leading to only 7% of all losses. Moreover, the average customer fraud cost £1.7 million. These figures show that the loss to staff fraud outweighs those perpetrated by customers involved in fraud and that staff fraud is growing. In 2005, KPMG reported that £468 million was lost to staff fraud. Therefore, losses to businesses due to staff fraud has increased by 17% between 2005 and 2010.

Reputational damage

Staff fraud can cause unquantifiable reputational damage to the image and brand of an organisation, both at a local and national level. Any fraud that involves customer data is potentially damaging, even where the fraud is identified before any losses are incurred. There is also clear media interest in staff fraud and this can have a significant impact on the reputation of financial institutions and customer confidence in the security of financial systems. Although the financial loss to an organisation could be small, the reputational damage to the brand could be considerable. This too can impact on an organisation's bottom line.

Internal impact

Incidences of staff fraud will have a substantial internal impact on any business. For example, there will be an investigation, the involvement of managers and HR in the disciplinary process and additional costs involved in recruiting, vetting, training and employing a new member of staff. However, in addition to this, cases of staff fraud can disrupt the normal daily routines of other employees and can have a negative impact on morale and trust between co-workers. Speculation and the 'grapevine' can lead to misinformation and unsubstantiated rumours and gossip circulating within

Case study: Aon Limited

Aon Limited, a subsidiary of Aon Corporation, the risk management and insurance group, was fined £5.25 million by the FSA after it was found that they failed to take reasonable care and maintain effective systems and controls to counter the risks of bribery and corruption.

As a result of weak internal controls, between January 2005 and September 2007, Aon made two suspicious overseas payments, one of £1.26 million and another of £2.13 million, to unnamed third parties, while trying to win business abroad.

Peter Harmer, Aon's UK chief executive, said: *'We did not have appropriate systems and controls in place to identify and assess the risks involved in making payments to third parties.'* Aon admitted that they could not confirm the payments were legitimate.

Margaret Cole, Director of Enforcement at the FSA, said: *'This sends a clear message to the UK financial services industry that it is completely unacceptable for organisations to conduct business overseas without having in place appropriate anti-bribery and corruption systems and controls.'*

Source: Financial Services Authority (2009)

departments. Team spirit and morale can be harmed if staff are shocked and unsettled by co-workers being dismissed, arrested in the workplace or prosecuted. Occurrences of staff fraud can also lead to some employees becoming overzealous, or mistrustful of their co-workers. Clearly, when an employee perpetrates a fraud or acts dishonestly it can cause a disproportionate amount of distress to customers, co-workers and their employer.

As a result it is crucial that organisations ensure that their communication policy with respect to staff fraud is effective. Ideally speculation should be dispelled at the earliest possible stage. If organisations do 'name and shame' those prosecuted for fraudulent activity, this should be communicated in an appropriate forum, with appropriate support, to minimise disruption to the rest of the workforce.

Displacing the risk

Despite the clear growth in incidences of staff fraud, for many organisations the threat from within still appears to be a potential rather than a clear and present serious risk. This is likely to be due partly to difficulties in detection and partly to the fact that organised criminals no longer find it easy to obtain the data they need from the organisations they have historically targeted, for example banks. However, intelligence suggests that this is changing and that organised criminals are now targeting a more diverse set of organisations to obtain customer data and perpetrate identity fraud, encompassing numerous business sectors, the public sector and financial services firms.

In addition, the more robust controls, increased training and awareness and more stringent vetting procedures now being introduced by one business sector are likely to cause displacement to other sectors and organisations. Data thieves frequently targeted call centre operations. However, from recent CIFAS research, since call centre operations have tightened their controls, data thieves have moved to the retail environment to carry out their frauds. Furthermore, it is well known that organised crime will always target the weakest link in the information chain. Consequently it is vital that all organisations recognise the potential threat they may face and consider whether they need to change their policies or procedures.

Unfortunately many organisations will find it difficult to gain more impetus, resources or policy changes for this purpose until their organisation is affected by a significant fraud, by which time any action taken is too late.

3 Combating staff fraud

'The recession may have played its part in driving up the increase in malicious insider data loss incidences, as data becomes an increasingly valuable commodity. But the alternative is that as organisations get wiser to the tactics of hackers, then criminals may be tempting staff to pass on valuable information – hence the massive growth in the insider threat.' **KPMG Head of Information Security, Malcolm Marshall**

'When setting their financial targets, some organisations have either neglected to factor in the current economic climate or have been over optimistic about recovery from the downturn, which has resulted in increased pressure to meet these targets and, as a result, the potential for fraud.' **PricewaterhouseCoopers, *Global Economic Crime Survey* 2009**

'Fraudsters tend to show off their money rather than hide it. If an employee suddenly turns up to work in an unexpectedly expensive car, it could be time to ask some questions…' **BDO Stoy Hayward, *Fraudtrack 8*, 2011**

'There is increasing evidence that organised criminal groups are placing their own people in financial services firms so that they can increase their knowledge of firms' systems and controls and thus learn to circumvent them to commit their frauds.' **Callum McCarthy, Chairman of the FSA**

To combat staff fraud successfully, organisations need to consider the following:

- why staff commit fraud
- the profile and common characteristics shared by staff fraudsters
- the role of organised crime.

Why do staff commit fraud?

The dominant and unifying factor behind most staff fraud is greed and the desire by employees to fund the type of lifestyle that they aspire to but cannot afford. For example, where staff have been known to commit fraud to pay off debts, in many cases they will continue to undertake fraud after the arrears have been successfully cleared. This continuation of fraudulent activity would indicate that greed is the primary driver.

The British Retail Consortium has highlighted the continued threat of insider fraud in a report on retail crime. They stated that in 2009, the average value per incident of staff theft alone was £875, a rise of 271% compared with the previous year. This puts the cost per incident of employee theft at around 20 times that of a customer theft.

According to the report *CIFAS Staff Fraudscape 2011*, the most common threat was staff attempting, fraudulently, to obtain an advantage by theft or deception, for example a high street bank cashier stealing cash from a customer who was depositing their cash into their account. Furthermore, the compromise of customer or payroll data to facilitate fraudulent activity by third parties still continues to be a significant threat to the financial services industry and public bodies that hold large amounts of personal data about citizens. This will also be the case for organisations in other sectors of the economy and is due to the involvement of organised crime, the potential and current financial losses, the possible impact on customer confidence and the number of

incidences. However, all types of staff fraud have the potential to damage an organisation severely, particularly its reputation.

Although an element of greed is present in the vast majority of staff fraud cases, employees are known to commit fraud according to three variables:

- opportunity
- motivation/pressure
- integrity/rationalisation.

Opportunity

As a result of the organisational changes previously outlined, junior staff who comprise modern workforces have never had more opportunity to commit fraud and conversely more responsibility to act ethically. Furthermore, senior or long-serving employees often hold a position of trust, which can sometimes be abused.

Motivation/pressure

The increased susceptibility to targeting by organised criminals and a growth in personal debt has provided a more direct motivation and more obvious source of pressure than previously existed. Generally, staff fraudsters will typically be motivated by financial gain, which may or may not be linked to collusion with organised criminals or personal associates.

Integrity/rationalisation

There is no evidence to suggest that staff are any less ethical or lacking in integrity than before. However, the infiltration of organisations by criminals when combined with a high staff turnover, reduced loyalty, relatively low pay compared with the national average and the perception of fraud being a 'victimless' crime with little chance of being caught, means that members of staff will increasingly rationalise the crime they are committing.

The common characteristics shared by staff fraudsters

With a variety of data collected on the subject of internal fraud, there is no common profile of a staff fraudster. There is a perception that the main threat identified in respect of staff fraud related to older senior employees who abuse their position and the responsibility entrusted to them.

A 2011 report by KPMG, *Who is the typical fraudster?*, identified that the fraudster was typically:

- aged 36–45
- male
- in a senior management position
- working in the finance department
- worked at the organisation for more than five years
- motivated by greed or work pressures
- exploits weak internal controls.

A 2010 *Global Fraud Survey* carried out by the Association of Certified Fraud Examiners identified that the staff fraudster was typically:

- 31–45
- male
- in a manager position
- working in accounting
- employed at the organisation between one and five years
- degree educated
- no previous conviction or disciplinary action
- motivated by living beyond means.

CIFAS members reported that staff fraudsters are:

- male or female
- average age is 30 years old; most fraud is committed by the 21–30 age group
- working in a retail environment
- average length of service is 5.5 years (ranges from 0.4 to 8.5 years).

Donald R. Cressey, an American criminologist, devised a theory for the triggers that lead employees to commit fraud. The three aspects of pressure, opportunity and rationalisation became known as the 'Fraud Triangle'. CIFAS members have actively participated in discussions to share their expertise in how these triggers are seen in the workplace. The aim of internal controls is to minimise opportunities and remove the incentives from potential fraudsters. CIFAS members therefore focused on sharing information on pressures and opportunities (as opposed to rationalisations), as it is those factors on which improved internal controls will have most impact.

Pressure

Motivations for fraud are often rooted in the pressures and temptations in life. There are pressures to meet targets in business and to be successful, as well as personal pressures, such as financial problems or the consequences of other lifestyle choices (for example gambling habits and debts). Some people are tempted to have items that they cannot afford or aspire to a lifestyle that may be beyond their financial means otherwise. These are the factors that could push someone to commit fraud in the workplace.

Examples include:

- **Personal problems** – a common reason cited for members of staff turning to fraudulent activity. This covers a wide number of issues, such as debt, domestic and other financial costs.
- **Debts** – (particularly those which could be linked to gambling or drug addiction) may not be covered by the staff member's salary. In addition, if such debts need to be repaid within a strict timescale, this could lead the staff member to consider other ways to obtain the money required.
- **Domestic issues** – for example, pressures attributed to relationship breakdowns, divorce or child maintenance payments, or family pressure to bring in a higher income, could be crucial factors.
- **Financial** – increasingly high costs of living could also be a major influence. If employees are struggling to pay bills, they may seek to acquire the funds by another means.
- **Greed** – this is, put simply, an employee's desire to fund a lifestyle that they are not able to afford. Recent research has indicated that a higher percentage of fraud is committed as a result of greed and to fund lavish lifestyles than any other motive.
- **Fear of unemployment** – the current economic climate has led employees to fear that their jobs could be at risk and that it may be difficult to obtain further employment. In addition, increased managerial pressure on individuals to meet targets – and thereby remain employed – can lead to members of staff looking for other ways to achieve them. For example, a salesperson switches the gas and electricity supplier without the consent of the customer. This leads to the salesperson receiving a better commission. This could also lead them to achieve higher targets than other, more honest members of staff, leading to the fraudster keeping their job, whereas others with apparently lower sales lose theirs.
- **Malice/revenge** – disgruntled employees may see committing internal fraud against an employer as a way of getting 'revenge' for low pay or being passed over for promotion. Personal differences with management could also lead to staff wanting to harm or damage the employer deliberately in some way. Another factor in this could be organisational redundancies. If an employee knows, or believes, that they are being made redundant, they may set out deliberately to conduct fraudulent activity – not just to obtain a benefit, but simply to retaliate by damaging the employer.

Opportunity

For fraud to take place, the environment in which the fraudster works has to present them with the opportunity to commit it. A lack of internal controls, a blame culture and lack of a reporting structure can all (in their small ways) create the opportunity for fraud. Employees may have access to certain records, valuable documents or other information that would allow them to commit fraud, for example, and adequate controls are essential.

Examples include:

- **Weak internal controls** – this is a major factor in facilitating fraud. For example, if there is only one staff member who deals with accounts or invoicing, there is more opportunity for embezzlement. Such opportunities would be reduced by implementing dual controls, such as having a senior staff member checking and signing off transactions.
- **Lack of clear policy and procedures** – if there is no clear policy in place, there will be no fear of exposure or reprisal. If there is not a demonstrable standard of what constitutes acceptable behaviour, a staff member could rationalise that they did not believe that the activities they were undertaking were unacceptable. Clear and concise policies are vital.
- **Poor security** – lack of physical security, for example lack of CCTV surveillance or computer passwords, may lead to opportunities for staff to steal. Individuals are more likely to commit fraud if they are confident that they will not be caught.

- **Criminal infiltration** – this is when organised criminals attempt to plant a member of staff within an organisation with the deliberate intention of defrauding their new employer. With continued pressure on organisations with high staff turnover, recruitment and security screening quality has been known to suffer in order to get staff in and working as soon as possible. This allows such infiltrators to take advantage of less stringent screening that organisations adopt to achieve timely recruitment. Criminals have been known to target call centres, hospitals, bank branches and retail outlets in this way.

The role of organised crime

It is generally acknowledged that incidences of infiltration and corruption of staff members by organised criminals have increased considerably in recent years, particularly in the financial services industry. It would appear that corrupting existing staff is easier, cheaper and quicker than a sophisticated infiltration and therefore remains the favoured tactic. However, this may change as organisations target staff fraud more effectively and criminal approaches to staff become more problematic.

Improvements to security and detection through automated systems and credit controls, combined with improved consumer awareness, have made identity frauds more difficult to perpetrate. As a result organised criminals are now focusing more heavily on corrupting staff and, conversely, staff with access to the necessary personal data have never been more susceptible to criminal approaches.

Members of staff involved in fraudulent activity and linked to organised crime will usually have undertaken this activity as a result of three main situations:

- infiltration
- collusion
- coercion.

Infiltration

Some organised crime groups will attempt to plant members or associates in financial institutions, public bodies and businesses. These individuals will gain employment with the deliberate intention of defrauding their new employer. Commercial or political pressures combined with a high staff turnover are known to lead to less stringent recruitment and more expedient security screening than should be the case. This contributes to the successful infiltration of call centres, branches, centralised service centres and retail outlets. Furthermore, the reactive investigations, the informal policy of quietly dismissing staff fraudsters and the relatively short sentences for the few who are prosecuted, mean that there is no strong deterrent for determined infiltrators.

Although infiltration is not currently the main risk to businesses, increasing attempts by organised criminals to plant staff to compromise customer and other data have been identified. Often the experience and expertise of those who have infiltrated an organisation will be limited. Intelligence suggests that the criminals responsible for orchestrating the infiltration will possess extensive experience and knowledge of data controls and capture.

Many organisations have credible intelligence to suggest that infiltration is taking place, but it is difficult to detect and confirm. The speed at which some staff members begin to steal, commit fraud or resign indicates infiltration, but this cannot necessarily be proved. Members of staff who have infiltrated an organisation but leave before the data compromised has been used to perpetrate a fraud exacerbate difficulties in detection. Also, due to the lack of thorough investigations by the police into cases of staff fraud, any links to organised criminals indicating infiltration are not uncovered. Infiltration is likely to be underestimated as those who infiltrate may not use the compromised data themselves and, as indicated, detection is problematic.

Collusion

Intelligence from law enforcement agencies and organisations suggests that the greatest risk to businesses involves staff members who, in the first instance, are willing to collude with organised criminals. Organised criminals focus on targeting established junior staff that have access to customer, payroll and other personal data. These individuals usually have unblemished employment records and are not therefore identified as high risk in recruitment checks, that is, no gaps in employment, good references, no criminal records.

Approaches to staff are often made during lunchtimes or before/after work when employees are normally identifiable due to their uniforms or visible security passes. Intelligence suggests that criminals may conduct a certain amount of surveillance before approaches are made. It has been noted that direct approaches will often be made to individuals of the same ethnic background. Many staff live locally to their employer and therefore they may be approached in nightclubs/pubs or through social introductions by friends or associates. These approaches may on the surface appear opportunistic but on some occasions intelligence suggests that the conversations are well thought through and are sophisticated sales pitches. Previous employees dismissed for fraud have been known to approach former associates/co-workers in an attempt to corrupt them.

Research indicates that to persuade staff to collude, organised criminals will offer financial enticements, although details on the precise amounts are patchy. The direct approach offering cash to fund a person's lifestyle appears to be the most common and successful tactic. However, payments to reward collusion are often withdrawn once data begins to be supplied and coercion is then used to continue the criminal enterprise.

In the retail industry collusion is significant because it is normally safer than undertaking shoplifting or staff theft as separate autonomous activities. Compared with conventional staff theft, collusion ensures the employee will not be found with goods or cash on their person. The customer thief in collusive activity will have acted like a normal shopper rather than a shoplifter and will be much less likely to attract the suspicions of supervisors, managers or security staff. The main forms of collusion include refund fraud, false markdowns, 'sweethearting' ('discounts' for friends and family), theft of loyalty card points from customers and other illegitimate use of discount entitlements.

Coercion

Organised criminals are known to threaten and intimidate staff into undertaking fraudulent activity. The threats are often made in relation to harming the employee or their family/friends. Intelligence suggests that it is relatively rare for coercion to be used in the first instance. Often, after being enticed with a payment, the staff member is effectively trapped and threats can then be made for further information, usually without payment. Continuing payments may continue depending on the value of the member of staff and their personal relationship with the organised criminal. Some staff members may be threatened from the start, but generally enticements are followed by threats. Occasionally, threatening to withhold the supply of drugs on which the staff member is dependent is used as a form of coercion.

Those employees who have been identified as involved in fraudulent activity will often claim that they participated due to duress and threats. However, there is little evidence to confirm this and it is difficult to corroborate such claims. Indeed the dividing line between collusion and coercion can easily become blurred. Once a member of staff has crossed the line and begun co-operating, the criminal will have a hold over that individual and may coerce them further. Intelligence suggests that criminals rarely use coercion in the first instance; instead this will come after a period of collusion.

The most effective way to mitigate the threat from collusion and coercion is to ensure that employees are aware of the types of approaches made by organised criminals and the consequences of colluding. Also, the employer should ensure that members of staff are aware of who they should report approaches to and feel confident the matter will be dealt with in a discreet and professional manner. A true zero tolerance approach, indicating the likelihood of being caught and the consequences, is also beneficial.

The five CIFAS strategic prevention areas

CIFAS has identified five main steps that can help in combating staff fraud effectively:

- vetting and security screening
- internal corporate culture
- monitoring staff
- effective policies to respond to identified staff fraud
- analysis and deterrents.

Case study

A security manager was sentenced to jail after helping three others attempt a £229 million theft from the London offices of Sumitomo Mitsui Banking Corporation (SMBC). He helped the thieves to gain entry and install 'key logging' software to try and compromise the bank's SWIFT payment system and make electronic payments to a number of offshore accounts. The security manager had disabled CCTV cameras and tampered with electronic equipment to help the gang get into the bank.

On 1 October 2004, the gang entered the office in London and sent money transfer orders to accounts in Spain, Dubai, Israel and other locations around the world. The transactions never went through, as there were errors in the SWIFT forms, and so the gang had to enter the bank again the next night. When the break-in was found out on the Monday, the security manager was one of the first to be identified, as he had not managed to wipe the CCTV tapes completely.

Had the raid been successful, it would have been four times larger than the UK record bank robbery, the £53 million stolen from a Securitas depot in 2006. The gang received sentences in 2009 which collectively totalled 30 years' imprisonment.

Source: *Guardian Online*, 4 March 2009.

4 Vetting and security screening

'The first line of defence against fraud is to make sure you don't employ fraudsters in the first place – this is why checks at the recruitment stage are so important.' **BDO Stoy Hayward *Fraudtrack 8*, 2011**

'To be truly effective, employee screening should be applied to all staff at all levels and should be undertaken regularly in order to protect organisations over the long term…' **CIFAS *The Internal Betrayal*, 2010**

The lack of staff vetting and security screening in some organisations is central to the staff fraud problem. Recruitment checks and controls are the first line of defence in preventing infiltration and identifying staff susceptible or vulnerable to collusion or opportunistic frauds.

From CIFAS research, organisations reported that there was a 70% increase in unsuccessful employment application fraud in 2010. Moreover, according to Inventium, a business support services organisation, 28% of people have told future employers that they left a job out of choice, when the truth is they were sacked. In their report on pre-employment screening, Powerchex, a vetting specialist firm, identified that one in five job applications contained 'some kind of discrepancy'.

From 2009 to 2010, CIFAS members experienced a 1,900% increase in job applicants who concealed unspent criminal convictions in their applications for employment. Furthermore, there were increases in potential employees who concealed their employment history and their employment record, both increased by 150% and 67% respectively.

The lack of employment recruitment checks is at the centre of the staff fraud problem. Vetting and security screening is the first line of defence in not only preventing fraudsters, but also deterring fraudsters and stopping the criminals placing individuals inside an organisation.

One of the ways to vet an applicant for employment that is becoming increasingly popular for organisations is conducting Internet searches. Good practice for this method is available in the Centre for the Protection of National Infrastructure (CPNI) report *Media Screening: Use of the Internet in employment decisions – a good practice guide for employers*. Something as simple as a Google search on the applicant could reveal, for example, that the individual has allegations of fraud against them or has committed fraud in other countries. Internet searches could also be used simply to verify identity or check that the previous employer details that the applicant supplied are authentic. Where there is potential to enhance vetting using media screening of potential employees, there could also be defamation issues. Therefore, it is important to review and verify any information that is found using media screening in other ways.

CIFAS KYS (know your staff) checks

The primary purpose of pre-employment vetting should be to verify the identity of applicants, confirm their previous performance and ascertain their integrity by reference to their previous conduct.

There are numerous types of pre-employment vetting checks that can be undertaken. Employers should consider using the following CIFAS KYS checks depending on their sector, the job role and level of seniority:

- a corporate application form completed by all candidates
- identification check
- Electoral Register check
- references reviewed
- qualifications check
- Credit Reference Agency (CRA) check

- confirmation of previous employment – through either references or confirmation from HM Revenue and Customs (HMRC)
- confirmation of previous unemployment (if necessary) – through Department for Work and Pensions (DWP)
- Criminal Records Bureau (CRB) check – for FSA Approved Persons and high-risk roles
- occupational health screening
- membership of professional bodies check (if necessary)
- Companies House checks on employers and directors
- fraud prevention check – including CIFAS Staff Fraud Database check (provided that the organisation is a CIFAS member).

Many organisations will take a risk-based approach to vetting and therefore they will view some of the checks above as only necessary for those positions where the potential risk is high. However, it should be remembered that the seniority of a post does not necessarily determine the staff fraud risk associated with it; for example, it is imperative to consider the fraud risk from low-level call centre staff compromising customer data. Therefore, the vetting controls necessary should be driven by risk rather than seniority of role.

There is a legal requirement under the Immigration, Asylum and Nationality Act for employers to check if their prospective employees have the right to work in the UK. Businesses caught hiring workers who are not legally permitted to work in the UK face fines.

Other possible checks that organisations can make which are not considered mandatory for best practice purposes include:

- in-house database/products check
- financial stability check
- media/Internet search.

Organisations should also consider the local environment from which they recruit. If they are recruiting from an identified staff fraud hotspot, they should consider undertaking more thorough security checks.

They should follow a published vetting policy that incorporates the specific checks and controls outlined above at various stages of the recruitment process. These stages can be broadly divided into the following areas:

- initial applications
- verifying candidate details
- interviews/assessments
- references
- further background checks.

Initial applications

All applicants for employment should complete a generic corporate application form, rather than simply submitting a CV. If CVs are accepted this should only be in conjunction with a fully completed application form. In those cases where applicants submit both a CV and an application form, these two documents should be compared for possible discrepancies.

The application form should request that prospective employees answer specific relevant questions, providing information that is unlikely to be contained on a CV. These questions should be used to help develop a picture of all applicants, determine their suitability for the post and confirm whether they are a 'fit and proper' person to work for the organisation. Some of the relevant questions an organisation should consider including on the application form are as follows:

- a full explanation of any gaps in employment, including maternity leave, unemployment, inability to work due to injury or illness, travelling, and so on
- the reason for leaving their former employer
- confirmation of their permission to work in the UK
- involvement in any external organisations and directorships held
- details of any civil or criminal proceedings that may be pending
- details of any convictions which are not considered spent under the Rehabilitation of Offenders Act 1974
- details of any bankruptcies or county court judgments (CCJs) or defaults registered against them
- details of any disciplinary proceedings, suspensions or expulsions by any regulatory or professional body or association in relation to their business or professional activities
- details of number of days' absence due to injury or illness.

It should be made clear to candidates that they should answer the questions truthfully and that providing what they consider to be a detrimental response to the question set will not necessarily prevent them from being appointed. Instead, each case will be considered on its own merits. The application form should also request full details of qualifications and an individual's employment history, which can then be used in the later stages of the recruitment process.

It is crucial that the application form be signed and contains a declaration confirming that all the details contained on the form are correct. This declaration should also provide notification/consent that certain background checks may be carried out on the candidate. This will necessitate including on the form all of the relevant use of personal data clauses to gain permission to undertake CRA, CRB, HMRC, DWP and other fraud prevention checks. The declaration should make clear that any material falsehoods in the application may constitute sufficient misconduct to terminate any contract of employment entered into by both parties and/or facilitate the sharing of this data with fraud prevention databases.

Further information regarding background checks for people with criminal records or the recruitment of individuals working with children can be found in the following CIPD factsheets:

- Employing people with criminal records
- Employing people with criminal records: risk assessment
- Recruiting of those working with children and vulnerable adults

(cipd.co.uk/factsheets)

Verifying candidate details

It is vitally important that organisations verify the identity and address of a candidate and confirm their right to work in the UK. Organisations should consider using similar checks to those in place when complying with FSA Know Your Customer (KYC) checks.

The most effective documents for verifying the identity of an applicant are those that are most difficult to obtain illicitly or through counterfeiting. Special attention should be exercised in respect of verifying the identity of non-UK nationals. The objective of the verification process is that the evidence offered by the individual is reasonably capable of establishing the candidate's identity and that the person is who they claim to be. This means that the employer should be reasonably satisfied that the named person exists and the applicant is that person. How much identity information and evidence to ask for and what to verify is a matter of judgement for the organisation using a risk-based approach. However, for the purposes of best practice, an organisation should request at least three documents as proof of identity and address.

The lists below are not exhaustive but offer details of the most common documents used to confirm identity. Organisations should request at least one document from List A below and two from List B. All documents requested should be originals.

Alternatively, organisations can use an electronic risk-based approach to identification verification checks, which can offer higher success rates and more security against forged or counterfeit documents. There are a number of suppliers of such services.

There are separate rules and documentation required to confirm whether an individual has the legal right to work in the UK. Organisations should contact the Home Office to ascertain their obligations in this area. The Home Office website provides full details.

Any documents provided to confirm identity should be verified. Some of the reference numbers provided in the documents above can be verified electronically. For those documents that contain security features, for example passport and driving licences with holograms, UV lights should be used to confirm they are genuine. HR staff involved in reviewing such documents should be trained to ensure that they are aware of how to verify these documents effectively.

Any written references supplied should also be verified. It is important that, when recruiting, HR does not rely on 'to whom it may concern' references. Equally, reference letters, copy certificates or verbal representations should not be accepted at face value. To verify that a reference provided is from a genuine organisation, the employer

LIST A	LIST B
Request one original document from the following:	*Request two original documents from the following (they must show the candidate's name and current address and must be dated within the last three months):*
A current signed passport	Utility bill (mobile phone bills should not be accepted)
Current EEA or UK photo card driving licence	Bank/building society or credit union statement
Residence permit issued by the Home Office to EU nationals in sight of own country passport	Mortgage statement from a recognised lender
Current full UK driving licence	Local council rent card or tenancy agreement
EEA member state identity card	Council tax notification/income tax notification (valid for the current year)
If a document from List A cannot be supplied, a letter or statement from a person in a position of responsibility who knows the applicant could be provided. This letter or statement must state who they are, confirm their date of birth and permanent UK address and state their relationship to the applicant. (A person in a position of responsibility includes a solicitor, a doctor, a minister of religion, a teacher or a social worker. Contact details for this person must be supplied for verification.)	Current UK photo card driving licence (provided this has not been supplied as a document from List A)
	Benefit book or original notification from the relevant benefits agency
	Solicitor's letter confirming recent house purchase
	EEA member state identity card (provided this has not been supplied as a document from List A)

can be checked on Companies House, the ICO's Data Protection Register, Yell.com or by searching for the organisation's website. Businesses should never assume that a previous employer has carried out full and proper checks on employees.

To confirm qualifications held, only original certificates should be accepted and, if necessary, these should be checked with the issuing establishment. All individuals who claim to have a professional membership or qualification should be checked with the registered body. The rise in 'diploma mills', more commonly known in the UK as 'degree mills', is a major factor to take into account when checking qualifications. Diploma mills are often purely online entities that offer false degrees from universities that don't exist, in exchange for payment. Verifile's own database of 'unaccredited institutions and unrecognised accrediting agencies' recognised that in 2010, the UK had 271 of these entities that offered bogus degrees. When the figure for the next highest in Europe is only 30 (Netherlands), this shows that there appears to be a significant problem with diploma mills in the UK.

Interviews/assessments

Interview techniques can help to prevent employing fraudsters. All HR staff that undertake interviews should be trained and made aware of potential warning signs with respect to the susceptibility of candidates to staff fraud and possible infiltration. They should also be aware of triggers in the application which require further investigation, for example the person is applying for a job a long way from their home, the applicant is taking a pay cut, and so on. Open-ended questions can reveal more about a person's conduct.

If necessary, HR should consider referring anomalies, suspicions or identified risks in respect of a candidate to the relevant fraud department. They should also make contact with the fraud department if they are unable to validate certain information or require help in verifying the identity documents they have been provided with. If possible it is often beneficial for organisations to conduct interviews after the CRB and Credit Reference Agency check so any problems identified can be discussed and considered.

References

Employment references are increasingly vague and of comparatively little value to potential employers. Concerns over the Data Protection Act (DPA) 1998 have led many organisations to produce references that confirm only dates of employment. As a result references are useful to confirm where an applicant worked, but are less useful in respect of confirming their integrity. Many references now simply confirm that the individual was an employee, but do not provide further details in respect of their performance and conduct. HR departments are, therefore, increasingly using interviews and assessments to assess competencies rather than relying on a third party.

In response to this trend, when requesting references many organisations will now use a standard reference proforma that does not ask for a subjective view of the candidate, but instead asks specific questions that are an attempt to elicit the information wanted by the prospective employer. Indeed, employers should not ask other organisations to supply a subjective opinion as to an applicant's likely future performance as such data is unreliable and can be misleading. Instead, a standard reference proforma should be used, containing specific closed questions that focus on an applicant's honesty, integrity, reliability, competency and punctuality.

Organisations should consider requesting details of the following on their standard reference proforma:

- dates of employment
- details of the applicant's salary on leaving employment
- the reason for the applicant leaving employment
- whether the applicant was dismissed
- whether the organisation would re-employ the applicant
- whether the applicant was ever suspected of dishonesty or breach of trust
- the reliability of the applicant
- details of the applicant's time-keeping and punctuality
- details of the number of days' absence from work in the most recent 12-month period.

Many organisations will accept the standard reference proforma only if it has been completed by HR or a senior manager. When former employers fully complete a standard reference proforma this does add value to the security screening process. However, again some organisations have adopted a policy that they will only confirm the dates of employment or provide a generic reference on the individual's general performance and refuse to complete the standard reference proforma, reducing their general effectiveness.

Many of the DPA concerns that drive this policy are unnecessary and in respect of responding to requests for references all organisations should provide truthful and accurate responses. If they are sent a standard reference proforma, organisations should feel comfortable in complying with their obligations to inform another potential employer of an individual's performance and conduct.

If possible, an employee should not commence duties until references have been sought, received and verified. The level of references required will be driven by the seniority and risk associated with the post applied for. To comply with CIFAS KYS best practice, however, an organisation should confirm references covering a minimum of five years. For those roles where there are particularly high risks, organisations should verify ten years of employment history through references.

Any gaps in employment history should be investigated. There could be a number of explanations for such gaps, for example travelling, caring for a child or relative, unemployment, self-employment, and so on. HR should ensure that they examine any gaps as these may conceal part of an individual's employment history or imprisonment. If an applicant claims to have been travelling, HR can ask to see stamps in the passport, evidence of flight tickets, and so on. The DWP can be contacted, with the applicant's consent, to confirm periods of unemployment.

Organisations should have a policy in place should they be unable to confirm a reference. Ordinarily this could involve seeking an alternative reference of a more personal nature from a person in a position of responsibility. Also, HMRC can be contacted, with the applicant's consent, to confirm where an applicant was employed and the payment of tax. Alternatively, HR can request evidence of employment through bank statements, wage slips or an HMRC statement or employer tax code notification. If references are unobtainable, organisations can refer the case and undertake a risk assessment based upon all other vetting checks that have been undertaken.

If the applicant does not have an employment history due to age, references should still be requested. In respect of school-leavers/graduates, this would include a reference from the school/university and a personal character reference from a person in a position of responsibility.

Further background checks

It has been estimated that around 20% of the working population has a criminal record. Therefore, employers should encourage applicants to disclose this by ensuring that they operate fair employment practices and encourage applicant honesty by stating that applications will be considered on merit and ability. Assessing the risk of employing a person with a criminal record means comparing an applicant's skills, experience and conviction circumstances against risk criteria identified for the job.

A conviction is not 'spent' until the rehabilitation period is complete. Once it is 'spent', the rehabilitated person does not have to reveal its existence in most circumstances and can answer 'no' to the question 'do you have a criminal record?'

Given that the vast majority of staff fraud is motivated by financial gain and that analysis of previous cases has shown a high correlation between those involved in staff fraud and those with significant debts or under financial pressure, a CRA check is crucial when vetting prospective staff. Organisations in some sectors should consider having an indebtedness policy or guidelines in place for current staff and when considering applications from individuals with substantial debts, CCJs, defaults or bankruptcies. These policies should consider the level of debt that a person has, their means of payment and their ability to service the debt.

Each case should be dealt with on an individual basis. If an individual has significant financial difficulties and is being considered for a particular role where the risk potential for staff fraud or theft is considered high, businesses should consider withdrawing the offer of employment.

The electoral roll can help confirm address details. Further checks to confirm directorships held and any disqualifications as well as a media and Internet search can also be useful. Searches of in-house and external fraud prevention databases should also be undertaken if possible.

CIFAS Staff Fraud Database

The most significant response to the problem of staff fraud has been the establishment of the CIFAS Staff Fraud Database. It is well known that staff dismissed for, or strongly suspected of, fraud move from one employer to another. The deterioration in the value of references and general inadequate levels of vetting has exacerbated this problem.

As a result, CIFAS has established a database where members share data relating to those staff fraud cases that satisfy the relevant standard of proof. The database is helping to prevent staff previously dismissed for fraud being employed by another CIFAS member, without full knowledge of what has gone before.

CIFAS members have reported that 6% of staff dismissed for fraud were soon attempting to be re-employed with another CIFAS member, possibly with the intention of perpetrating further frauds.

The CIFAS membership, FSA, CBI (Confederation of British Industry), TUC (Trades Union Congress) and CIPD were consulted during the establishment of this Staff Fraud Database. The database helps organisations to vet prospective employees and acts as a useful deterrent to those employees susceptible to collusion and members of staff tempted to undertake opportunistic frauds.

Temporary and agency staff

Temporary staff recruited through agencies and subcontracted staff are rarely subjected to the same checks and controls as permanent employees and this is a major cause for concern. Due to high staff turnover rates and customer service pressures, employing temporary or agency staff is often a commercial necessity. In many cases the agencies that supply the staff are entrusted with the vetting and security screening of those individuals. However, many employers have expressed concerns about the rigorousness of the vetting undertaken.

It is good practice to vet temporary and agency staff to the same level as permanent staff. This means that organisations should consider independently requesting and verifying references and the identities of staff should be confirmed in-house. Also, a clause should be inserted in the agreement between employer and agency facilitating regular audit checks to ensure that the agency is undertaking sufficient vetting and screening of the staff supplied. Furthermore, the contract between the two parties should contain a liability clause so that, should there be any misconduct by the staff supplied, the organisation will be protected from any financial or reputational loss.

HR should keep a record of all staff supplied by third parties including their personal details, for example name, date of birth, address, national insurance number, and so on. This prevents the re-employment of the same person if their work was considered unsatisfactory or there was misconduct.

Current situation analysis

Currently most employers do not vet or security-screen employees to the level suggested as good practice by CIFAS. However, many businesses in recent years have introduced more stringent vetting with procedures becoming tighter and more robust. For example, references are now followed up more effectively. In some organisations fewer temporary agency staff are being employed and verification checks on the identification provided are undertaken more consistently.

Increasingly, organisations now outsource all or some of their vetting and security screening to outside agencies. There is nothing inherently wrong with this as long as those outsourced agencies follow best practice. Relying on a third party, whether a recruitment agency or former employer, to have undertaken satisfactory vetting is an error which should be avoided.

Despite this, due to commercial pressures, high staff turnover rates, a lack of appreciation of the threat of fraud and inadequate policies, many organisations are still employing staff before references are received, identities are verified and gaps in employment history are satisfactorily explained. Furthermore, HR require specific training to enable them to identify triggers on CVs and application forms for further investigation.

However, commercial realities are such that many organisations follow a risk-based approach that allows some staff to start work before their vetting is completed. Occasionally this will lead to that organisation having to dismiss some new joiners as the vetting process identifies material falsehoods in their applications. CIPD research finds that over the course of a year about a quarter of employers will have withdrawn a job offer or dismissed an individual because someone had lied or misrepresented their application. Although it is best practice to complete the vetting process before allowing staff to commence duties, a sensible risk-based approach can often be effective in mitigating the threat from staff fraud and allow the business to function efficiently.

Limits to the effectiveness of vetting

There are clear limits to the effectiveness of vetting as a mechanism to prevent staff fraud. 'Opportunists' or long-serving members of staff who commit fraud are likely to be identified during this process. Furthermore, as indicated, the main threat relates to the collusion of existing staff with organised criminals. Often, such staff will have few obvious indicators that they are vulnerable to criminal approaches. The main benefits of vetting are to prevent infiltration and the re-employment of offenders as well as identifying employees susceptible to fraud.

In making employment decisions, employers should make objective assessments, adopt an open mind and focus on merit and ability to do the job. Blanket exclusion policies should be avoided. Consideration should be given to extenuating circumstances, the nature and relevance of any previous misconduct, the potential risks involved in employing the individual and if/how these could be sensibly and effectively managed.

5 Organisational culture

'A code of ethics or an anti-fraud policy is not sufficient to prevent fraud. … Ethical behaviour needs to be embedded within the culture of an organisation. Commitment from senior management and "tone at the top" is key. Employees are more likely to do what they see their superiors doing than follow an ethics policy, and it is essential that management do not apply double standards.' **Chartered Institute of Management Accountants, Fraud Risk Management 2009**

Internal culture

Organisations should aim to create a rigorous anti-fraud internal culture that promotes honesty, openness, integrity and vigilance. Creating and embedding such an internal culture is not easy and there must be a strong commitment by employees at all levels. For businesses to develop a holistic response to the problem of staff fraud, it is vital that the culture of the organisation facilitates such an approach.

It is crucial that the internal culture of an organisation stresses the need for openness and trust between employees at all levels. This does not simply mean that staff are comfortable about reporting suspicions of staff fraud, but also extends to personal issues which may impact upon the performance of a staff member and increase their propensity to commit fraud. For example, if an employee is suffering financial difficulties or has another personal problem, for example gambling, they should be encouraged to disclose this and the organisation should be sympathetic and offer an employee assistance programme. This could include offering an independent helpline with qualified counsellors, the results of which can be kept confidential or fed back to HR, depending on the nature of the problem.

However, it is also vital that staff are made fully aware that, should they commit fraud, there will be absolute zero tolerance. Also, it must be made clear that if staff have concerns about co-workers, they have an obligation and duty to report this. There should be a whistleblowing policy which facilitates an independent and confidential means of reporting these concerns. Clearly employers should be careful that, while making employees aware that there is a zero tolerance policy towards staff fraud, the honest majority of the workforce does not become alienated by being made to feel that everyone is under suspicion and being monitored.

Due to the threats that exist from criminal approaches to staff from serious and organised criminals, businesses should seek to create an environment where those approached feel able to report instances and confident that the matter will be dealt with in a discreet, professional and considerate manner. Tools such as employee assistance lines offering confidential counselling and mediation services are useful in helping to create a sympathetic culture.

When seeking to create an internal culture, it is important that clear and direct policies are formulated which are always consistently and fairly followed by HR and others. Policies are the core educational and awareness requirement for all employees and should support an overall business approach to staff fraud, setting the parameters and risk exposure for the organisation. They should ensure clarity, transparency and fairness when dealing with incidences of staff fraud.

There are various policies an organisation should follow to create the desired culture. As a minimum they should have policies covering the following:

- fraud management
- staff fraud prevention
- code of conduct/business ethics
- staff assistance

- whistleblowing
- fraud specialists/HR working together
- investigations
- disciplinary matters
- fraud reporting.

The Fraud Advisory Panel has published anti-fraud policy statements and templates on its website (www.fraudadvisorypanel.org). However, a policy alone cannot ensure that the appropriate controls to prevent staff fraud are maintained. This is only achieved by action and by others seeing that action is taking place. It is this that creates the preferred behaviour the policies set out to achieve.

The anti-fraud culture needs to be endorsed and followed at all levels, meaning that, for example, managers and high-performers must follow the rules just as any other employee is expected to do.

Induction

All new entrants should receive a code of conduct/ business ethics or staff handbook clearly setting out their responsibilities and requirements for discretion and security. These documents should indicate what disciplinary procedures exist and the consequences of breaking the rules. There should also be an awareness session on staff fraud as part of the induction programme for new joiners. This should focus on links to organised crime (money laundering and terrorism) and case studies. During induction training staff should also be made aware of their responsibilities and the consequences of committing fraud. The key messages should therefore focus on actions and consequences.

Staff should be made aware that every computer transaction they undertake leaves a computer footprint for audit trails. It should also be communicated to staff that they are personally responsible for all activity undertaken using their logins and/or passwords. Staff fraudsters have been known to use unlocked computers and co-worker logins and passwords to commit frauds. Therefore it is best practice to update passwords regularly and ensure that staff are aware that they are responsible for all enquiries made using their password and that therefore they should not under any circumstances share or disclose it.

Staff training and awareness

For the internal controls to be effective, an anti-fraud working environment is vital. Regular education and awareness of fraud to all levels is key to embedding an anti-fraud culture.

Currently many organisations do not have any staff fraud awareness training, while others have it only in high-risk business areas. The threat from staff fraud is such that all staff should now receive specific awareness training, not simply during induction but on a continuing basis. Such training should be supplied both for existing staff as a refresher and for new entrants. Training should communicate to staff what early warning signs to look for in respect of staff fraud, what to do if approached by a third party, personal safety issues, the whistleblowing policy and how to report staff fraud. However, businesses should be mindful when formulating training that they do not educate the fraudster. Training staff in techniques of how fraud is committed could potentially arm employees with the skills to commit fraud.

Employees should be educated that they have a duty both to report suspicions of staff fraud by others and instances of approaches by colleagues or third parties. The messages sent to staff through training should be strong and direct, providing support as well as a deterrent. Managers and team leaders should be specifically targeted for training and case studies should be used to stress the consequences of staff fraud. It can be difficult to instil an anti-fraud culture when the punishment may be perceived as just being a light prison sentence, so explaining the impact of this on an individual's life chances is important. Other sanctions, such as being listed on the CIFAS Staff Fraud Database, withdrawal of pension and benefits to pay for losses and civil action should act as equally effective deterrents.

The code of conduct/business ethics documents should set out the standards expected of staff and it is best practice for staff to sign documents annually to confirm that they are aware of their obligations. This will prevent staff claiming during disciplinary proceedings or interviews that they were unaware of any policies they have breached. The code of conduct/ business ethics document should explicitly outline

expectations of employees in a number of areas relating to security and fraud control and indicate that employees will be monitored for adherence with the code. The code should also outline that fraud will be punished and be communicated by senior management so that it is clear that fraud is taken seriously. In a recent report on economic crime in the UK, PricewaterhouseCoopers identified that organisations were neither implementing codes of conduct properly nor communicating them regularly.

The role of HR

Analysis has shown that disaffected, demotivated and antagonistic employees are more likely to commit fraud. In addition, if staff consider themselves to be underpaid or undervalued, or are asked to undertake the duties of a more senior staff member, this can lead to rationalisation, where individuals commit fraud to 'earn' the money they believe they have 'worked' for. If remuneration policies or bonus distributions are perceived to be inequitable, this can exacerbate this problem. Furthermore, staff who feel insignificant, powerless or taken for granted are also able to rationalise any fraudulent activity they undertake. If staff can psychologically rationalise committing fraud, even if they do not actually commit it themselves, they are unlikely to be committed to combating it or being vigilant with respect to the behaviour of others. HR policies and practices for employee recognition and development should endeavour to address the cultural/developmental issues that can motivate staff to commit fraud.

Where staff are identified as involved in fraudulent activity, organisations should have strong policies in place with respect to investigations, dismissals and the involvement of law enforcement. These should balance the potentially competing demands of the internal investigation, disciplinary process and the external police investigation.

All organisations should consider implementing a staff fraud prevention policy that should be formulated with significant input from HR. This policy must take into account employment law, human rights and data protection legislation. In accordance with the Acas *Code of Practice on Disciplinary and Grievance Procedures*, fraud should be considered as gross misconduct and should warrant dismissal. This should be made clear in the disciplinary procedures.

Whistleblowing

The operation of a 'whistleblowing' facility so that staff can confidentially report any concerns about the conduct of other employees should be an important element in tackling staff fraud. A 24-hour helpline is suggested as the best whistleblowing mechanism. However, research indicates that 'whistleblowing' lines are very ineffective, partly due to staff not fully trusting the anonymous element and partly because they often feel more comfortable approaching line managers or the fraud departments direct. Organisations should give thought as to how their whistleblowing facility is promoted within their organisation to derive maximum benefit. Clearly, they should also ensure that they protect and support those who expose corruption, dishonesty or unethical behaviour.

Whistleblowing, of course, is consistently a key feature of an anti-fraud culture and is integral to an organisation's code of ethics. As highlighted in CIFAS's *Staff Fraudscape* (2011) report, however, whistleblowing is the least common way in which staff fraud is uncovered. When employees see corruption or fraud in their organisation, they do not seem to want to report it. Staff have been surveyed about whistleblowing: some are not interested and some fear being ostracised by their peers or losing their job. Media stories about whistleblowers being unfairly dismissed do nothing to help in this respect. As a result of these surveys, businesses have enhanced their whistleblowing policies (for example by having a direct phone line to the board to report unethical incidents – not just fraud or corruption) or have tried to rebrand the image of whistleblowing. Either way, whistleblowing must be an essential part of any thinking about how to tackle staff fraud, as – once again – merely having a weapon in the armoury is no use if the weapon is never used.

The profile of whistleblowing should be raised and communicated more effectively. Furthermore, those who do blow the whistle on staff fraud should be protected and supported.

6 Monitoring staff

'One of the most significant findings of this survey is the very large increase in cases involving the exploitation of weak internal controls by fraudsters – up from 49% in 2007 to 74% in 2011.' **KPMG, *Who is the typical fraudster?* 2011**

General principles

When developing their approach to monitoring employees, organisations have to strike the right balance between respecting people's privacy at work and ensuring they don't misuse business property or systems. The monitoring of email and Internet activity is helpful, although it is also recognised (albeit not academically proven) that it could affect staff morale and productivity.

The Information Commissioner's Office (ICO) Employment Practices Data Protection Code on monitoring at work sets out some clear steps to help employers achieve this balance while also meeting their obligations under the Data Protection Act.

Impact assessments

The Information Commissioner's code recommends that organisations should conduct an impact assessment to help them establish whether their data monitoring complies with the DPA. Such an assessment should identify:

- the purpose of the monitoring
- the benefits it is likely to deliver
- any likely adverse effects
- alternatives to surveillance or less intrusive methods of monitoring
- obligations that arise from monitoring
- whether monitoring is justified.

Consent

Staff consent is not needed to carry out monitoring at work. In a situation where consent was freely given, it could be withdrawn. Following an impact assessment, employers are in a stronger position to justify monitoring and, therefore, will not need the consent of members of staff.

Monitoring at work policy

Once the impact assessment has been completed, it's important for employers to write policies that spell out:

- their approach to monitoring
- what is prohibited
- what is acceptable private use of the Internet
- any unauthorised areas, for example pornographic websites
- the possible disciplinary consequences should the rules be breached.

Clearly ensuring long-term compliance is about more than having a written policy and the monitoring code makes a number of recommendations. These include:

- giving one person responsibility for making sure that policies and procedures comply with the law so that the employer's monitoring policy is kept up to date
- providing training and guidance to line managers and employees to ensure that all staff are aware of their data protection responsibilities.

The ICO's Employment Practices Data Protection Code on monitoring at work generally succeeds in helping employers to find the right line between respecting their employees' privacy and protecting their own interests. For example, on email use the code allows an organisation to check employees' accounts in their absence if they have been informed that this will happen. However, an employee's privacy must be respected if they clearly mark that an email is personal, unless the employer has a valid and defined reason to examine its content.

Video and audio monitoring

The code recommends that employers read the ICO's CCTV Code of Practice. It may be necessary to 'audio monitor' face-to-face conversations.

Covert monitoring

The code protects staff from covert monitoring, except in exceptional circumstances, such as where there are grounds for suspecting criminal malpractice. The ICO defines covert monitoring as *'monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place'*.

Organisations that ignore their monitoring responsibilities are likely to breach the DPA and risk considerable penalties. Organisations can be forced by the courts to pay compensation to their employees for distress and financial loss and a failure to comply with the DPA may ultimately be treated as a criminal offence.

The requisite level of control

Therefore, when considering what controls or countermeasures to introduce to tackle staff dishonesty, it is important to remember that only a small proportion of staff commit fraud. There is clearly a balance between monitoring staff and having effective controls in place and providing a quality customer service. A stifled and over-controlled environment can reduce innovation, demotivate staff and inconvenience customers. The level of control needs to be balanced against the potential risk and stress-tested to identify potential weaknesses.

CIPD research indicates that excessive monitoring and surveillance can have a negative effect with respect to how workforces view their employer. The Chartered Institute of Management Accountants warns that internal controls can become expensive and, if used excessively, employees may become less motivated and organisations inefficient. It is important that the objective of internal controls is not about employee entrapment but about reducing the temptation to commit staff fraud. Furthermore, it is important that employers explain policies or changes in policies to employees and provide a business reason. However, there is a balance between the need for employees to know that controls are in place and the need to know the precise nature of the control where this is judged to be counterproductive.

HR has a fundamental role in combating staff fraud in a proportionate way. A proportionate response to manage the identified risks and maintain the requisite level of control must include consideration of:

- staff training and awareness
- prevention
- deterrence
- monitoring
- detection
- investigation
- reporting
- analysis
- review
- customer awareness
- media.

Risk-based approach

To meet the demands of a competitive and fast-changing marketplace, a risk-based approach to staff fraud is inevitable. Indeed, an organisation's entire approach to the management of internal fraud should be risk-based. This should be reflected during the vetting of new entrants through to the monitoring of existing staff. Organisations must accept that there will always be some level of staff fraud. The objective of the controls is to reduce the opportunity.

However, risk can and must be minimised by taking all reasonable preventative and monitoring measures. The FSA has indicated that when dealing with the risks associated with financial crime, organisations should put a sharp focus on:

- the need for organisations to take a risk-based approach
- the need for senior-management accountability for the organisation's risk-based approach
- the need for organisations to take a holistic approach, avoiding disproportionate focus on any one tool
- the need for proportionality, with effort relating to risk, across sectors and by organisations.

In its report *Data Security in Financial Services*, the FSA provided some useful good practice on controls to prevent compromise of customer data from corrupt employees. These include:

- regularly review staff IT access rights to ensure they provide exactly the level of IT access that is required
- risk-based, proactive monitoring of staff members' access to customer data to ensure that it is being accessed and/or updated for a genuine reason
- strict controls on those who work in IT administrator roles
- consider the risk of data compromise when conducting email monitoring, for example look for strings of numbers that may appear to be credit card details
- regular sweeping for key-logging devices
- employing security guards, cleaners, and so on, directly to ensure an appropriate level of vetting and reduce risks that may arise through third-party suppliers accessing customer data.

For those organisations where staff fraud poses a significant risk and where they have suffered from numerous cases, it is likely that such organisations will want to introduce stringent controls and tough anti-fraud measures in high-risk areas. Call centre operations, for example, have introduced the following actions:

- ban on personal mobile telephones
- restricted access to email facilities
- restriction and monitoring of Internet use
- restrictions on USB sticks and other devices
- the creation of a paperless environment
- the provision of lockers for personal belongings
- regular spot checks on bags when leaving the building
- management information reporting to identify account misuse quickly
- arranging for staff suspected and investigated for fraud to be arrested at their desk in front of other employees to act as a deterrent
- 'naming and shaming' in those cases where the individual has been convicted and this is a record of public knowledge
- periodic fraud awareness training.

For those organisations where the risk from staff fraud is lower, they may want to follow a different approach, which takes into account their own corporate culture, and adjust their controls accordingly.

However, for all organisations regardless of the risk, it is best practice for staff access to systems, databases and communication channels to be restricted to what is relevant to their individual role. For example, access to email, the Internet and certain computer and database systems should be driven purely by job responsibilities and commercial necessity. Furthermore, no single individual should have access to a customer's complete set of security data. Organisations should also have a policy in place allowing them to move staff to different business areas to minimise risk where suspicions of staff fraud exist but evidence of wrongdoing cannot be confirmed.

Early warning signs

The majority of organisations rely on reactive investigations to detect and identify staff fraud. However, there are many early warning signs that exist that can assist in proactively targeting fraudulent employees or delivering awareness training to other members of staff. The Fraud Advisory Panel produced a factsheet listing behavioural, financial and procedural early warning signs (this list is not exhaustive; http://www.fraudadvisorypanel.org/new/pdf_show.php?id=170):

Behavioural

- employees who consistently work longer hours than their colleagues for no apparent reason
- employees who are reluctant to take holidays and/or time off
- employees who are excessively secretive in relation to their work
- employees known by others to be under duress for personal reasons
- employees with a sudden change of lifestyle and/or social circle
- employees under apparent stress without identifiable pressure
- employees who are aggressive or defensive when challenged and/or controlling of certain colleagues
- employees who are subject to complaints and/or tend to break the rules
- employees who delay providing information or who provide different answers to different people
- employees who ask to defer internal audits or inspections to prepare properly

- employees with new and unusual relationships with other individuals or departments within the organisation
- employees who request significant detail about proposed internal audit scopes or inspections
- excessively high or low staff turnover and/or new employees resigning quickly.

Financial

- cash-only transactions
- poorly reconciled cash expenses or customer accounts
- rising costs with no explanation or that are not commensurate with an increase in revenue
- large volume of refunds to customers
- unusually large inventories
- unusual transactions or inter-account transfers (even for small amounts)
- remuneration disproportionately linked to activities such as sales
- employees known by others to be under external financial pressure
- employees who appear to make a greater than normal number of mistakes, especially where these lead to financial loss through cash or account transactions on tills or cash desks
- employees with unexplained sources of wealth
- employees with competing or undeclared external business interests
- employees who submit inconsistent and/or unreasonable expense claims
- employees at the highest level of performance (for example sales) where there might be a concern that they are achieving this through suspect activity.

Procedural

- employees making procedural or computer-system enquiries inconsistent or not related to their normal duties
- new employees with knowledge of industry procedures but no such experience disclosed on their CV
- prospective employees who are reluctant to provide full background information or who provide inaccurate or inconsistent information
- key managers with too much hands-on control
- insufficient oversight/audit applied
- an unusual number of customer complaints
- customers or suppliers insisting on dealing with just one individual
- managers who avoid using the purchasing department
- tendering to one supplier only or to the same suppliers
- lack of transparency
- poor engagement with corporate governance philosophy
- too much delegation by senior managers without proper review procedures.

Other warning signs include:

- noticeable personality changes
- unexplained wealth or living beyond apparent means
- refusal of promotion
- reluctance to take annual leave
- choosing seats that are next to the wall or difficult to monitor
- frequent trips to the toilet or cigarette breaks
- staff in frequent communication with external parties while at work or on breaks, for example telephone conversations, text messages, emails
- key staff having too much control or authority without audit checks
- staff under stress without a high workload
- staff known to be under external pressure
- staff making computer enquiries that are unnecessary or inconsistent with their designated role
- new staff with apparent experience and knowledge of procedures without such knowledge being apparent during the recruitment process
- new staff resigning quickly after starting or sudden unexplained resignations
- cosy relationships with suppliers/contractors or customers/suppliers insisting on dealing with just one individual
- customer complaints of missing statements/ unrecognised transactions
- dormant accounts that are suddenly reactivated
- incomplete applications containing false or missing documentation
- abnormal commissions to brokers and staff
- excessive use of suspense and error accounts.

In addition to the above, intelligence suggests that staff fraudsters will sometimes appear to be 'model' employees and strong performers, partly in a bid to deflect attention and suspicion from their activities. At one major bank it was discovered that of the ten top-performing salespeople in one division, six were subsequently dismissed for fraud. In addition, those staff who are never sick or take little annual leave may be very committed or, alternatively, may not want to be away for any extended period of time for another reason. There are many examples of staff fraud that were only discovered once the individual was away from the office due to sickness or injury.

Internal monitoring systems

It is vital for monitoring staff and audit trails that organisations can identify particular enquiries or actions by individual staff members. Therefore when logging onto systems, staff should have a unique identification name or number which they must enter to gain access.

Specialist software is used by some organisations to monitor, flag up and identify suspicious activity by staff, although few organisations use such programmes proactively. This software can monitor employee actions, indicate any unauthorised access to data and create exception reports after analysing variables from employee, customer and transactional information. Many organisations do not currently use any software of this kind due to the size and complexity of their organisation, while others do not view staff fraud as offering a threat significant enough to justify the cost. However, as the problem continues to grow and the threat increases, this is likely to change.

Businesses can also use system-based approaches to internal fraud, which work primarily through control and monitoring of destination accounts and segregation of payment authority and payment approval. To avoid collateral-based fraud, parameters are system-based to prevent unusual transaction approval.

Case study: UBS

Kweku Adoboli was arrested on 15 September 2011 by the City of London Police on suspicion of committing fraud after Swiss bank UBS uncovered losses of £1.5 billion. Investigations began over a series of deals that apparently accumulated unsustainable losses after betting on currency exchange rates and share prices. Adoboli joined UBS in 2006 as a trainee investment adviser before moving on to a trade support analyst position, then later promoted to a trader, reportedly earning a six-figure salary. He had no record of any disciplinary action.

The suspected 'rogue trader' will face a charge of fraud by abuse of position, as well as a second charge of fraud and a further two counts of false accounting. Adoboli worked on the trade desk known as 'Delta One', which bets on the direction of assets and share prices. This is usually known to be a relatively safe way of trading as the bet in movement on equity is hedged with a bet the other way. However, if no hedge bet is placed and the bet goes well, returns can be very large, but likewise if the bet goes badly, losses have the potential to be huge. The Financial Services Authority will also conduct an investigation into why UBS failed to spot the alleged fraudulent trading, despite recently investing millions in risk control.

The case shares similarities with that of Jerome Kerviel, who amassed losses of £3.6 billion while working at a similar trade desk at Société Générale, one of France's biggest banks, and was subsequently sentenced to three years' imprisonment in 2010. Kerviel claimed that his superiors knew of his activities and that the practice was very common.

Sources: *Guardian Online*, 22 September 2011; *The Times*, 16 September 2011.

For those organisations that do use such software to investigate activity by staff, this is usually on a reactive basis as part of the audit trail after a problem is identified. However, organisations should give consideration to using software for proactive targeting and to prevent a potential problem from developing. If criminals perceive an organisation as having weak controls, it is likely that organisation will suffer increased targeting.

Clearly it is also best practice for sensitive or high-value accounts to have markers placed on them to flag up unusual enquiries. Staff conduct should be monitored at various levels, with spot-checks and dip-sampling to provide more unpredictability.

There are a number of internal monitoring systems that organisations can use, for example:

- exception reports
- 'same name' reports, that is, account holder has same name as staff member accessing account
- balance transfer reports, that is, where transfers have been made soon after a change of address or similar customer detail changes
- audit
- portfolio review
- reactivated accounts
- transaction pattern analysis
- behavioural pattern analysis.

7 Effective policies to respond to identified staff fraud

'It is … important to help employees and managers understand what the rules and procedures are, where they can be found and how they are to be used.' **Acas *Code of Practice 1 – Disciplinary and Grievance Procedures***

Internal investigations and HR interaction with fraud specialists

Due to the growing threat and the complexity of the problem, organisations should give serious thought to creating dedicated teams of fraud investigators and fraud detection specialists dealing specifically with staff fraud. Organisations with limited resources or small fraud teams should consider creating 'staff fraud champions', who will act as specialists for that particular organisation.

It is crucial that organisations have effective policies in place to investigate allegations or suspicions of fraud; otherwise, the investigation may fail for a number of reasons:

- Potential evidence or relevant legal processes are compromised by those lacking the necessary investigative expertise.
- Managers or others attempt to perform their own investigations without the necessary investigative expertise.
- Managers or others conceal information or evidence in case it is perceived that they have failed in their management or control of the relevant business area.
- Those qualified to undertake the investigation are deployed too late to gather the necessary evidence.
- Law enforcement is not involved early enough in the investigative process.

Close working relationships and improved communication between fraud specialists and HR departments in respect of internal fraud policies are therefore vital. The role of HR and fraud specialists should be clearly set out within an organisation's general fraud management policy or fraud specialists/HR working together policy. These policies should include the following general principles:

- All concerns or allegations of fraud and other criminal behaviour will be investigated fairly and thoroughly.
- Any staff member suspected of fraud will be presumed innocent until proven otherwise.
- The responsibility for the investigation of staff will be completely entrusted to fraud specialists as soon as it becomes evident that criminal or fraudulent activity may be involved.
- Staff identified as involved in fraudulent or dishonest activity will be dealt with consistently and fairly under the organisation's disciplinary procedures.
- If necessary, any fraudulent activity may be reported to relevant law enforcement agencies.
- Legal action may be taken against any individuals involved in fraudulent or criminal activity.
- Assistance will be provided to law enforcement, regulatory authorities and other organisations in their fight against fraud and crime.

The investigation should be used to gather enough evidence to suspend, arrest or clear an individual. HR should ensure that there are clear personal contact and communication procedures in place that are followed to make certain that any witnesses are not interfered with. Anyone involved in the investigative process should avoid protracted conversations or unnecessary confrontation.

During an investigation there are likely to be interviews conducted with the staff member suspected of fraud and possible witnesses. It is vital that organisations clearly set out who is responsible for interviews and ensure that interviews do not become entangled with any disciplinary procedures. The interviews should inform the disciplinary decision, but the disciplinary process should be kept completely separate.

Fundamentally there are two types of interviews that may be used:

- fact-finding interviews
- investigative interviews.

Fact-finding interviews

These interviews should form the first stage of the interview process and should act primarily as a means of obtaining information about staff compliance with normal business practices. The staff member should be asked questions about their role and understanding of organisational policies, procedures and standard business practices. This can include mentioning the areas of concern and requesting some comment from the interviewee.

At this stage, the interviewee is not normally afforded any forewarning of the interview. However, they should be asked if they would like to have another person present with them during the process. It is not anticipated that the interviewee will disclose any adverse information during this interview. However, during the course of the interview, should they choose to disclose any facts which may incriminate themselves, they must be informed that information disclosed in the interview may form part of either a disciplinary process or, dependent on the nature of the evidence, may be disclosed to law enforcement for prosecution purposes. Following this caution the interviewee should be asked to repeat their previous comments and whether they wish to continue with the interview or to seek advice from a colleague, line manager, HR, trade union representative, and so on. Should the interviewee wish to seek such advice, the interview should be terminated. The interviewee should be informed that a further interview may take place in due course and that the comments made will be reported to the relevant line manager.

Investigative interviews

Investigative interviews are normally conducted due to a reasonable suspicion of impropriety or dishonesty on the part of a member of staff. This interview may come after the fact-finding interview, or the fact-finding interview may not be necessary depending upon the information available to the fraud specialist.

A written invitation should be sent to the interviewee detailing their rights and the type of questions to expect. The interviewee should be given the opportunity to consult a trade union/staff association official, HR specialist, line manager or someone similar, prior to the commencement of this type of interview. The interviewee should be informed that information disclosed in the interview may form part of either a disciplinary process or, dependent on the nature of the evidence, may be disclosed to law enforcement for prosecution purposes.

The questions asked in this type of interview should explore an individual's conduct and their version of events pertaining to this. The individual should be asked to explain, in detail, their conduct, actions and decisions. Often the member of staff will be presented with evidence and asked to clarify any identified ambiguities and to give explanations and/or mitigating circumstances for their behaviour.

At the conclusion of the investigative interview, the individual should be informed of the next steps in the investigation process. Often this will involve the fraud specialists preparing a report outlining the facts uncovered in the investigation. This report should be made available to HR and possibly the relevant line manager. HR will then decide on the relevant disciplinary action if necessary.

Police involvement

Organisations should approach the police at an early stage in the investigation if there is any likelihood that the police will want to prosecute the individuals involved. This way the police can take over an investigation, undertake interviews and gather evidence. Indeed, police contributors to this guide have indicated that businesses should involve law enforcement agencies at an earlier stage in the investigation process, as often for evidential purposes they need to be involved when the fraud is happening rather than at the end of the process.

The police will bring many benefits to an investigation, including expertise and experience, power to search, seize and arrest, access to forensic techniques and asset recovery potential. For a successful investigation, police require from organisations:

- total honesty
- details of similar activity
- early notice
- commitment to the investigation
- forensic awareness
- evidential awareness.

Disciplinary procedures

When fraud is alleged or suspected, the matter should immediately be reported to the fraud specialists and no further action should be undertaken unless instructed by the fraud specialists. It is vital that disciplinary procedures do not commence and the staff member is not suspended until the appropriate HR manager in liaison with the fraud specialists sanctions this.

Primarily fraud specialists should dominate the investigative process with input from HR, while HR should dominate the disciplinary process with input from fraud specialists. However, there is no harm, and indeed in some cases it may be prudent, for HR to sit in on interviews conducted by fraud specialists and for fraud specialists to attend disciplinary meetings. The extent to which HR and fraud interact will vary depending on the size of the organisation and its internal culture. It is considered best practice for the two groups to work closely together, communicate effectively and ensure that they complement each other.

In respect of best practice vis-à-vis disciplinary procedures the CIPD endorses the Acas *Code of Practice – Disciplinary and Grievance Procedures*. The Acas guidelines stress the need for rules and disciplinary procedures and outline the key stages in handling these processes. The Code of Practice makes clear that although organisations can be flexible about how formal or extensive their procedures need to be, there is a statutory procedure they must follow as a minimum if they are contemplating dismissing an employee.

An employer should:

- establish the facts
- inform the employee of the problem
- hold a disciplinary meeting with the employee
- take action after the disciplinary
- provide the employee with the right to appeal.

According to Acas the disciplinary procedures used should:

- apply to all employees, irrespective of their length of service, seniority, and so on
- ensure that any investigatory period of suspension is with pay, unless specifically provided for in the contract of employment
- ensure the case is not pre-judged
- ensure that, where the facts are in dispute, no disciplinary penalty is imposed until the case has been thoroughly investigated and there is reasonable evidence that the employee committed the act in question.

There are several actions that fraud and HR specialists should undertake before and during a disciplinary meeting with an employee accused of fraud:

- Undertake an investigation sufficient to enable a clear view of the facts to emerge.
- Consider what explanations the employee may offer for their conduct and, if possible, check them out.
- HR should prepare for the meeting carefully, ensuring they study the fraud investigation report.
- Arrange for a second member of staff to be present wherever possible to take notes and act as a witness.
- Tell the employee in writing of the allegations against them; advise them of the disciplinary procedure and their right to be accompanied.
- Give the employee time to prepare and state their case.
- Arrange a time for the meeting, which should be held as privately as possible, where there will be no interruptions.
- Ask the employee if they have any explanation for the misconduct or if any special circumstances should be taken into account.
- Allow the employee to call witnesses or submit witness statements.
- Establish what disciplinary action was taken in similar circumstances in the past.
- Consider adjourning the meeting, if necessary, before deciding on any disciplinary penalty.

Gross misconduct

Employers should provide a clear indication to staff which offences will be considered gross misconduct and therefore involve dismissal without notice. These offences should be misconduct serious enough to destroy the contract between the employer and employee, making any further working relationship and trust impossible. The Acas guidelines provide the following list of offences, relating to fraudulent behaviour which are normally regarded as gross misconduct:

- theft, fraud, deliberate falsification of records
- unauthorised entry to computer records.

There must always be a full and fair investigation to determine the facts and to decide whether an individual has committed an act of gross misconduct. All records should be kept meticulously, as this will be vital should a case be pursued at an employment tribunal. Since the burden of proof is on the employer to show that the dismissal is not unfair or unreasonable, keeping records is vital. The types of record that should be kept by employers are minutes of meetings, attendance, notes of telephone calls, copies of correspondence, and so on.

If an individual is accused of an act of gross misconduct, they should be suspended from work on full pay. Any period of suspension should be as short as reasonably possible, allowing the allegations to be investigated thoroughly. If following the investigation the organisation is satisfied that gross misconduct has occurred, the result will normally be summary dismissal without notice or payment in lieu of notice. However, no dismissal, even if there has been gross misconduct, should be instant. The employer must still follow the statutory three-step approach.

It is essential that those implementing these procedures have the necessary training and guidance to do so, in line not just with minimum legal obligations but also with the principles of fairness and natural justice.

Internal investigation interaction with dismissal procedures

As previously mentioned it is inevitable that the internal investigation process will interact with dismissal procedures. The key is to ensure that these two processes are kept separate and do not become entangled. Therefore there are numerous stages in investigating and dismissing an individual:

1. The fraud specialist becomes aware of an allegation or suspicion of fraud.
2. The fraud specialist commences an investigation and informs HR.
3. The fraud specialist and HR consider whether to suspend the individual during the investigation because of the level of risk, evidence, and so on.
4. Interview stage – this could be a fact-finding or investigative interview; the line manager and possibly HR should attend.
5. The fraud specialist and HR again consider whether to suspend the individual based upon the evidence uncovered during the investigation.
6. The fraud specialist should complete the investigation and produce a report, which should be viewed by the line manager and HR.
7. HR should consider whether gross misconduct has occurred.
8. The fraud specialist who conducted the investigation may be required to assist with any disciplinary meetings by clarifying certain matters.

Resignations

It is well known that employees under suspicion of fraudulent activity will often resign before an investigation can commence or conclude. Ideally, an investigative team should seek to gather as much evidence as possible before suspending an individual, although there are usually risks associated with allowing a suspected member of staff to remain in post.

Although a resignation cannot be refused, organisations should advise staff members that they are still technically employees during their contractual terms of notice period and that an investigation may be conducted during that time. Organisations will usually have a notice period of four weeks to investigate the individual and undertake disciplinary proceedings if necessary. If sufficient evidence exists to dismiss employees that resign and are seeing out their notice period, employers should follow the normal disciplinary procedures. Therefore the employee should be invited to a disciplinary meeting and dismissed in their absence if they fail to attend. Resignation should not be encouraged, as potentially this may be viewed as constructive dismissal, is ineffective as a deterrent and fails to deal with the underlying issue.

8 Analysis and deterrents

'Collecting information – from open and closed sources, whether apparently innocent or incriminating – is only step one. Not until it's been analysed, evaluated, synthesised, and turned into a product that sheds light on the risks we face, does it become a practical tool which can help us make better informed judgements. And those judgements in turn reshape our understanding of risks, and help us work out what more we need to know.'
Bob Ferguson, FSA, Head of Financial Crime and Intelligence

Learning lessons

There is clearly a need for a joined-up approach to staff fraud and best practice, involving various different departments and law enforcement agencies. Some organisations try to understand the staff fraud risks they face by using profiling to establish which job roles/business areas pose the greatest threat. This profiling will indicate which roles are most susceptible to collusion or coercion. Also, geographical and business area hot spots could be analysed to produce predictive modelling, allowing subsequent preventative action to be taken. However, a recent study by BDO Stoy Hayward found that there is no typical fraudster. Staff fraudsters are as diverse as the working population. To concentrate in one area of the business as result of a profiling exercise may allow the fraudsters to defraud you or to move to another area undetected.

An incidence of staff fraud should lead to an investigation, followed by risk analysis and possible changes to policies or the code of conduct and/or business. Fraud departments should also proactively formulate a reporting system and database to record criminal approaches to staff.

A joined-up approach to intelligence- and data-sharing

Intelligence relating to staff fraud should be analysed and used to identify the scale and level of the threat posed and the nature of the problem. This should include the losses, potential impact of staff fraud and the types of staff fraud most commonly used. The analysis by fraud specialists should feed into HR-driven policies to prevent infiltration by serious and organised crime and enhance security systems to identify cases. Data and intelligence should be shared in a timely fashion for the prevention and detection of serious and organised fraud.

Contributors to this guide have indicated that there needs to be more co-operation and interaction between different businesses and between the private sector and law enforcement agencies. In some cases the organisation that employs a member of staff who is committing fraud may not be directly affected by their activities, for example where staff working in a mobile telephone call centre or a council tax direct debit unit compromise customer details, which are then in turn used to defraud a bank. Therefore a joined-up approach is vital throughout the private and public sectors.

Currently co-operation between organisations and between organisations and law enforcement agencies in this area is often based on personal relationships and trust built up over time. While these relationships are important and should be developed further, due to the complex nature of staff fraud and the cross-business sector impact it can have, organisations would benefit from a more formalised approach that is less reliant on personal contacts.

Prosecution policy

It is vital that organisations have an effective investigation and prosecution policy to ensure that staff members identified as involved in fraud are

dismissed and reported to the police. Law enforcement agencies acknowledge that they may not be able to prosecute all staff fraudsters but they have indicated that it is good practice for the purposes of intelligence to report all cases to the police. Only by organisations reporting all cases of staff fraud to the police will the scale of the problem be fully communicated, allowing police forces to allocate more resources to investigating and prosecuting those involved.

Reporting cases to the police

Currently many employers will only report to the police those cases that they feel the police will accept, investigate and ultimately prosecute. A true zero tolerance approach would report all cases where a sufficient standard of proof exists to facilitate a prosecution. As a result, in reality, many organisations actually follow a zero tolerance dismissal rather than prosecution policy.

Those organisations that rely exclusively on reactive investigations also contribute to the problem of a lack of prosecutions. For example, law enforcement agencies have indicated that simply using IT systems to track computer footprints of individuals accessing accounts is not enough evidence by itself to prove that the person accessing the account was involved in compromising the data relating to it. This evidence would justify a warrant and an interview but would not be sufficient for a conviction. Therefore, to facilitate more prosecutions, organisations need to use more proactive methods of identifying staff fraudsters.

The predominant cause of the low level of prosecutions is the low priority and resources that police forces allocate to fraud.

If fraud departments have a good relationship with the police, this often helps to facilitate more prosecutions. Developing strong and effective professional ties with the police is important. To increase the chances of the police accepting a case, organisations should approach them with a full evidential file, containing all statements and disclosure material. This makes it as easy as possible for them to put the case together for prosecution.

The police have indicated that employers are in some respects contributing to their own problems. The general under-reporting of the issue and allowing suspects to resign rather than facing alternative action leads to an underestimation of the level and scale of the problem. This, combined with concerns about reputational risk and delays in responding to police requests for production orders for access to accounts where funds have been sent to, causes delays in interviewing potential suspects and successfully combating the problem. There also remains an unnecessary reluctance among organisations to share data for fear of committing a Data Protection Act (DPA) offence. This reluctance can hinder an investigation and potentially cause a fraudulent member of staff to be recruited by another organisation.

Sentences

Typical sentences for staff fraud are mainly served in open prisons and are not that long, although the impact of the sentence on later life chances can be far longer lasting. Often the severity of the sentence is not increased due to the breach of trust and abuse of position involved in staff fraud cases. It is difficult for organisations to stress their zero tolerance policy, and for this to act as a deterrent, when sentences are so light. Typical sentences for compromising customer data are less than two years. In some instances, first offenders will receive only community service or a suspended sentence. To increase pressure for stronger sentences, businesses and law enforcement agencies need to work together to raise the profile of the issue and communicate the harm caused.

Deterrents

As the ratio of prosecutions to dismissals for staff fraud is very low (CIFAS members have successfully prosecuted just 5% of the staff fraud that they identify, a further 10% awaiting trial) and sentences are typically short, organisations need to develop alternative deterrents. There are various ways businesses can do so:

- 'name and shame' staff fraudsters
- publicise cases on internal intranet sites and/or newsletters
- publicise prosecutions by inviting staff members to court to witness sentencing
- zero tolerance policy
- civil recovery
- CIFAS Staff Fraud Database.

Those individuals who have been proven to be involved in staff fraud should be 'name and shamed' in order to act as a deterrent to others. The best forum to promote this message should be considered and should take into account the possible disruption caused and the target audience for the message. Because of the DPA, this should only involve cases where the staff member has been prosecuted and the details are in the public domain. Some organisations take this a step further by actually inviting staff members to court to witness sentencing, so that this message is then disseminated in a dramatic way.

As previously mentioned, a true zero tolerance policy, which involves dismissing all staff fraudsters and reporting all such cases to the police, should be introduced by all agencies.

Using civil recovery methods, businesses can target staff benefits, for example shares can be revoked, pensions seized and asset recovery services employed. The possibility of civil recovery should be communicated to all employees as part of a continuing training and awareness campaign to deter potential staff fraudsters, particularly those who are long-serving employees. Also, once a confiscation order has been awarded, organisations can look to receive compensation from assets and funds that are seized under Proceeds of Crime Act (PoCA) legislation.

CIFAS members can use the Staff Fraud Database to deter those staff who believe that they can simply resign or be quietly dismissed without other organisations finding out about their previous conduct during the vetting process. In order for CIFAS members to comply with the fair processing principle of the Data Protection Act, they must advise their staff on how their personal data will be used on the Staff Fraud Database. This is done by way of a fair processing notice. Fair processing notices are issued through a variety of communications, for example a global email, staff handbook, written contracts or an anti-fraud policy. As a result of these fair processing notices, CIFAS members have seen a significant deterrent effect. For example, they have reported a drop in opportunistic-driven frauds.

Conclusion

While the involvement of the fraud investigation team is to be expected, the HR function is equally crucial to combating staff fraud. With the increasing trend for organisations to outsource services (which potentially increases the staff fraud risk), HR involvement becomes even more fundamental.

Due to the diverse nature of businesses and organisations, implementing a fully standardised approach to staff fraud would not be feasible or practical. There are, however, a number of key best practice policies and procedures that all organisations should consider following:

- Organisations should establish dedicated units to specialise in proactively targeting and reactively investigating cases of staff fraud.
- Vetting and security screening is the first line of defence in preventing infiltration and identifying staff susceptible or vulnerable to collusion or opportunistic frauds. Employers should verify candidate identities, personal details and references as well as undertake further background checks on all prospective employees.
- Organisations should aim to create a rigorous anti-fraud internal culture that promotes honesty, openness, integrity and vigilance throughout the workforce. Businesses should seek to create an environment where those approached by criminals feel able to report this and confident that the matter will be dealt with in a professional and considerate manner.
- The growing threat from staff fraud is such that all staff should now receive specific awareness training. Training should communicate to staff what early warning signs exist with respect to staff fraud, what to do if approached, including personal safety issues and how to report staff fraud.
- There is a balance between monitoring staff and having effective controls and providing a quality customer service. The level of control needs to be balanced against the potential risk and stress-tested to identify potential weaknesses.
- Staff access to systems, databases and communication channels should be restricted to a level relevant to their individual role. For example, access to email, the Internet and certain computer and database systems should be driven by job responsibilities. No single individual should have access to a customer's complete set of security data.
- Those organisations or departments where staff fraud poses a huge risk and that have suffered from numerous attacks should introduce stringent controls and tough anti-staff fraud measures.
- Specialist in-house software exists and should be used to monitor, flag up and identify suspicious activity by staff and create exception reports after analysing variables from employee, customer and transactional information.
- When staff fraud is identified, an effective communication policy is essential to prevent disruption and a negative impact on morale by dispelling any speculation, misinformation, unsubstantiated rumours or gossip circulating within departments.
- Those proven to be involved in staff fraud should be 'named and shamed' as a deterrent. This should take place in an appropriate forum or using an appropriate medium to minimise disruption to the rest of the workforce, for example internal intranet, circulars, conferences, training, and so on.
- A true zero tolerance policy should be implemented where all cases of staff fraud with a sufficient burden of proof are reported to the police to facilitate a prosecution.

Promoting an anti-fraud philosophy requires collaboration between HR, fraud prevention, compliance, risk management and legal teams, together with trade unions, staff at the 'coal face' and others: collectively addressing the staff fraud risks in their organisation.

Like all crimes, staff fraud will affect you and your organisation, your competitors, your industry – in essence, your community. The best way to fight crime is to have zero tolerance throughout.

References

ADVISORY CONCILIATION AND ARBITRATION SERVICE. (2009) *Disciplinary and grievance procedures [online].* Code of practice 1. London: ACAS. Available at: http://www.acas.gov.uk/CHttpHandler.ashx?id=272&p=0 [Accessed 7 June 2012].

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS (2010) *Report to the nations on occupational fraud and abuse: 2010 global fraud study [online].* Austin, TX: Association of Certified Fraud Examiners. Available at: http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/rttn-2010.pdf [Accessed 7 June 2012].

BDO STOY HAYWARD (2011) *FraudTrack 8 : myth and misconception [online]*. London: BDO Stoy Hayward. Available at: http://www.bdo.co.uk/fraudtrack [Accessed 7 June 2012].

BOWCOTT, O. (2009) *International bank raiders foiled by form-filing [online].* London: Guardian.Online. Available at: http://www.guardian.co.uk/uk/2009/mar/04/sumitomo-fraud-attempt?INTCMP=SRCH [Accessed 7 June 12012].

BRITISH RETAIL CONSORTIUM. (2010) *Retail crime survey 2010 [online]*. London: British Retail Consortium. Available at: http://www.brc.org.uk/Downloads/2010_BRC_Retail_Crime_Survey.pdf [Accessed 7 June 2012].

BROWN, D. and GRIFFITHS, K. (2011) *UK trader Kweku Adoboli arrested over $2bn UBS loss*. The Times. 15 September.

CENTRE FOR RETAIL RESEARCH. (2011) *Global retail theft barometer 2011 [online]*. Newark: Centre for Retail Research. Available at: http://www.retailresearch.org/grtb_currentsurvey.php [Accessed 7 June 2012].

CHARTERED INSTITUTE OF MANAGEMENT ACCOUNTANTS. (2009) *Fraud risk management: a guide to good practice [online]. London: Chartered Institute of Management Accountants*. Available at: http://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf [Accessed 7 June 2012].

CIFAS. (2010) *The internal betrayal: a CIFAS report on beating the growing threat of staff fraud [online].* London: CIFAS. Available at: http://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/The_Internal_Betrayal_CIFAS_Special_Report_Aug_2010.pdf [Accessed 7 June 2012].

CIFAS. (2011) *Staff fraudscape: depicting the UK's staff fraud landscape [online].* May. London: CIFAS. Available at: https://www.cifas.org.uk/secure/contentPORT/uploads/documents/reports/2._CIFAS_Staff_Fraudscape_2011.pdf [Accessed 7 June 2012].

FINANCIAL SERVICES AUTHORITY. (2008) *Data security in financial services [online]*. London: Financial Services Authority. Available at: http://www.fsa.gov.uk/pubs/other/data_security.pdf [Accessed 7 June 2012].

FINANCIAL SERVICES AUTHORITY. (2009) *FSA fines Aon Limited £5.25m for failings in its anti-bribery and corruption systems and controls [online]*. London: Financial Services Authority. Available at: http://www.fsa.gov.uk/library/communication/pr/2009/004.shtml [Accessed 7 June 2012].

INVENTIUM. (2011) *20% of jobseekers lie in interviews [online]*. Reported at: http://www.mybusiness.co.uk/Yeh9aF5o6VWuDg.html [Accessed 7 June 2012].

JONES, S. and TREANOR, J. (2011) *Kweku Adoboli faces fourth charge [online]*. London: Guardian Online.Available at: http://www.guardian.co.uk/business/2011/sep/22/kweku-adoboli-faces-fourth charge?INTCMP=SRCH [Accessed 7 June 2012].

KPMG (2011) *KPMG forensic fraud barometer, January 2011 [online]*. London: KPMG. Available at: http://www.kpmgfightingfraud.com/15390.htm [Accessed 7 June 2012].

KPMG. (2011) *Who is the typical fraudster? [online]*. London: KPMG. Available at; http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/who-is-the-typical-fraudster.PDF [Accessed June 2012].

POWERCHEX. (2010) *The Powerchex annual pre-employment screening survey 2010*. London: Powerchex.

PRICEWATERHOUSECOOPERS. (2011) *Combating cybercrime to protect UK organisations. Global economic crime survey [online]*. London: PricewaterhouseCoopers. Available at: http://www.pwc.co.uk [registration required].

PRICEWATERHOUSECOOPERS. (2011) *Cutting costs and cutting fraud: economic crime in the public sector [online]*. London: PricewaterhouseCoopers. Available at: http://download.pwc.com/ie/pubs/2011_cutting_costs_and_cutting_fraud.pdf [Accessed 7 June 2012].

PRICEWATERHOUSECOOPERS. (2009) *Global economic crime survey – November 2009*. London: PricewaterhouseCoopers. Available at: http://www.pwc.co.uk/forensic-services/publications/global-economic-crime-survey-nov09.jhtm [Accessed 7 June 2012].

To stay up to date with the latest outputs from the Research and Practice Team at the CIPD go to **cipd.co.uk/research** and sign up to our e-newsletter at **cipd.co.uk/cipdupdate**

At the CIPD, we explore leading-edge people management and development issues through our research. Our aim is to share knowledge, increase learning and understanding, and help our members make informed decisions about improving practice in their organisations.

We produce many resources on people and management issues including guides, books, practical tools, surveys and research reports. We also organise a number of conferences, events and training courses. Please visit **cipd.co.uk** to find out more.

Chartered Institute of Personnel and Development
151 The Broadway London SW19 1JQ UK
Tel: +44 (0)20 8612 6200 Fax: +44 (0)20 8612 6201
Email: cipd@cipd.co.uk Website: cipd.co.uk

Incorporated by Royal Charter Registered charity no.1079797

Issued: June 2012 Reference: 5865