TACKLING STAFF FRAUD AND DISHONESTY:
MANAGING AND MITIGATING THE RISKS
Tackling 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 financial services industry and beyond.

The CIPD is the professional body for those involved in the management and development of people and has 127,000 individual members.

Written by John Hinds, Policy and Projects Manager, CIFAS – the UK’s Fraud Prevention Service.
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Part 1 What is staff fraud?</td>
<td>6</td>
</tr>
<tr>
<td>Part 2 Why is staff fraud a growing risk?</td>
<td>12</td>
</tr>
<tr>
<td>Part 3 Combating staff fraud</td>
<td>16</td>
</tr>
<tr>
<td>Part 4 Vetting and security screening</td>
<td>21</td>
</tr>
<tr>
<td>Part 5 Internal corporate culture</td>
<td>29</td>
</tr>
<tr>
<td>Part 6 Monitoring staff</td>
<td>32</td>
</tr>
<tr>
<td>Part 7 Effective policies for responding to identified staff fraud</td>
<td>36</td>
</tr>
<tr>
<td>Part 8 Analysis and deterrents</td>
<td>40</td>
</tr>
<tr>
<td>Conclusion</td>
<td>43</td>
</tr>
</tbody>
</table>
Introduction

The vast majority of staff in any organisation are trustworthy and honest. However, businesses are now beginning to 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 market place, many businesses have responded by empowering staff and undertaking structural reforms. Undoubtedly, these changes have significantly raised the levels of customer service and enhanced 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 organisations approach the issue of staff fraud is changing in response to the increased risk. Many organisations have historically 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. However, for many organisations, 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 taking this a step further by sharing data actively with each other on incidences of staff fraud within their organisations.

Recent research by CIFAS – the UK’s Fraud Prevention Service – has confirmed that staff fraud has a reputational, financial, regulatory, internal and customer service impact on businesses. As a result, staff fraud is now emerging as the single most significant fraud risk to the financial services industry and a serious risk to all businesses. The growing threat from staff fraud can be effectively combated by organisations co-operating and adopting a common approach that includes zero tolerance of all types of staff fraud and a rigorously 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 to ensure 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 employees don’t 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 that takes into account the nature of the business, the industry sector and different job roles. If employers communicate clearly why they’re 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.

Research by the CIPD has found that organisations that seek to monitor their employees excessively are unlikely to create a work environment that encourages trust, loyalty and commitment. The CIPD research report, Pressure at Work and the Psychological Contract, reveals that employees who are closely monitored tend to have more negative attitudes towards work and are more likely to suffer from stress.

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 fully standardised approach to staff fraud wouldn’t be feasible or practicable. But there are numerous best-practice policies and procedures that all organisations should consider following in order to ensure that they’re at least complying with their regulatory obligations.

John Hinds, Policy and Projects Manager, CIFAS
Ben Willmott, Employee Relations Adviser, CIPD
Part 1 What is staff fraud?

‘Staff fraud occurs when an individual 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, while undertaking duties for an organisation with which they have a contractual arrangement to provide personal services.’ Peter Hurst MCIPD, Chief Executive, CIFAS

Defining ‘staff’
For the purposes of this guide, the term ‘staff’ is regarded as an individual with a contractual arrangement, whether directly or indirectly (for example, through a recruitment agency), to provide his or her personal services to an organisation. Therefore this includes, but isn’t restricted to, permanent staff, temporary staff on short- or fixed-term contracts, and staff supplied by a recruitment agency or third party.

Defining ‘fraud’
Within the historical legal framework, there was no formal definition of ‘fraud’.

However, the Fraud Act, which became law in January 2007, broadly defines three main types of fraud:

- **fraud by false representation** – where an individual dishonestly and knowingly makes a representation that is untrue or misleading
- **fraud by wrongfully failing to disclose information** – where an individual wrongfully and dishonestly fails to disclose information to another person when they have a legal duty to disclose it, or where the information is of a kind that they are trusted to disclose it, or they would be reasonably expected to disclose it
- **fraud by abuse of position** – 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.

For fraud to be committed under the new legislation, there will need to be an identifiable intent by the individual to make a gain or to cause a loss or to expose another to the risk of loss.

Therefore, for the purposes of this guide, the term ‘fraud’ includes situations 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 broadly includes offences commonly defined elsewhere as:

- employee fraud
- insider fraud
- internal fraud.

Types of staff fraud
There are numerous types of fraud that can be perpetrated by staff against their employer. Depending on the nature of business and the products and services offered, members of staff may have many opportunities to commit fraud. Each business and organisation will have its own particular risks and threats and there are further threats 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 in that it’s generally undertaken on an unplanned basis by an individual for the purpose of personal financial gain, or can be linked to a serious and organised criminal network or terrorist financing. All organisations are vulnerable and all organisations have some level of risk.
The first serious attempt to create a detailed typology of staff fraud in the UK financial services industry 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 (see Table 1)
- unlawful obtaining or disclosure of personal data (see Table 2)
- unlawful obtaining or disclosure of commercial data (see Table 3)
- account fraud (see Table 4)
- dishonest action by staff to obtain a benefit by theft or deception (see Table 5).

### Table 1: Employment application fraud

<table>
<thead>
<tr>
<th>Use of a false identity</th>
<th>The identification of an application, either for employment or to provide services, in which the applicant uses a false identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impersonation of an innocent party</td>
<td>The identification of an application, either for employment or to provide services, in which the applicant impersonates an innocent party</td>
</tr>
<tr>
<td>False immigration status</td>
<td>The identification of an application, either for employment or to provide services, in which the applicant uses a false immigration status</td>
</tr>
<tr>
<td>False qualifications</td>
<td>The identification of an application, either for employment or to provide services, in which the applicant uses false qualifications, which is considered a material falsehood*</td>
</tr>
<tr>
<td>False references</td>
<td>The identification of an application, either for employment or to provide services, in which the applicant uses false references, which is considered a material falsehood*</td>
</tr>
<tr>
<td>Concealed employment history</td>
<td>The identification of an application, either for employment or to provide services, in which the applicant conceals their employment history, which is considered a material falsehood*</td>
</tr>
<tr>
<td>Concealed employment record</td>
<td>The identification of an application, either for employment or to provide services, in which the applicant conceals their employment record, which is considered a material falsehood*</td>
</tr>
<tr>
<td>Concealed unspent criminal convictions</td>
<td>The identification of an application, either for employment or to provide services, in which the applicant conceals one or more unspent criminal convictions</td>
</tr>
<tr>
<td>Concealed adverse financial/credit history</td>
<td>The identification of an application, either for employment or to provide services, in which the applicant conceals their financial/credit history, which is considered a material falsehood*</td>
</tr>
</tbody>
</table>

*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.*

Tackling employee fraud
<table>
<thead>
<tr>
<th>Table 2: Unlawful obtaining or disclosure of personal data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contravention of IT security policy</strong></td>
</tr>
<tr>
<td><strong>Contravention of systems access policy</strong></td>
</tr>
<tr>
<td><strong>Contravention of Internet policy</strong></td>
</tr>
<tr>
<td><strong>Contravention of email policy</strong></td>
</tr>
<tr>
<td><strong>Fraudulent personal use of customer/payroll data</strong></td>
</tr>
<tr>
<td><strong>Disclosure of customer/payroll data to a third party</strong></td>
</tr>
<tr>
<td><strong>Modification of customer payment instructions</strong></td>
</tr>
<tr>
<td><strong>Unauthorised alterations to customer data</strong></td>
</tr>
</tbody>
</table>
### Table 3: Unlawful obtaining or disclosure of commercial data

<table>
<thead>
<tr>
<th>Contravention of IT security policy</th>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contravention of systems access policy</td>
<td>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</td>
</tr>
<tr>
<td>Contravention of Internet policy</td>
<td>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</td>
</tr>
<tr>
<td>Contravention of email policy</td>
<td>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</td>
</tr>
<tr>
<td>Theft of internal policies/procedures/practices</td>
<td>Theft of internal policies/procedures/practices</td>
</tr>
<tr>
<td>Disclosure of internal policies/procedures/practices to third parties</td>
<td>Disclosure of internal policies/procedures/practices to third parties</td>
</tr>
<tr>
<td>Theft of intellectual property</td>
<td>Theft of intellectual property</td>
</tr>
<tr>
<td>Theft of IT systems source code</td>
<td>Theft of IT systems source code. This may be to enable third parties to mimic internal IT architecture or introduce fraudulent payment instructions</td>
</tr>
<tr>
<td>Infringement of copyright</td>
<td>Theft or unauthorised dealing with articles infringing copyright</td>
</tr>
</tbody>
</table>

### Table 4: Account fraud

<table>
<thead>
<tr>
<th>Fraudulent account transfer to employee account</th>
<th>Fraudulent electronic transfer of funds from a customer account to an account controlled by a member of staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraudulent account transfer to third-party account</td>
<td>Fraudulent electronic transfer of funds from a customer account to an account controlled by a third party</td>
</tr>
<tr>
<td>Fraudulent account withdrawal</td>
<td>Fraudulent withdrawal of cash from a customer account without the customer’s knowledge or authority</td>
</tr>
<tr>
<td>Theft of IT equipment</td>
<td>Theft of IT equipment, for example, hardware, monitors, PCs, keyboards, modems, printers, mice, cables, laptops and so on</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Theft of fixtures and fittings</td>
<td>Theft of fixtures and fittings, for example, desks, chairs, cupboards, pictures, display stands, plants, and so on</td>
</tr>
<tr>
<td>Theft of office equipment</td>
<td>Theft of office equipment, for example, stationery or electrical equipment (kettles, microwaves and so on)</td>
</tr>
<tr>
<td>Theft of consumables and instruments</td>
<td>Theft of consumables and instruments, for example, payment cards awaiting collection, cards recovered in ATMs, cheque books, returned/undelivered mail, blank drafts, blank cheques and other negotiable instruments awaiting use. Also includes theft of headed paper and other internal forms for use in subsequent frauds</td>
</tr>
<tr>
<td>Theft of personal property</td>
<td>Theft of personal property while on employer premises, for example, clothing, mobile telephones, cash and wallets belonging to other members of staff</td>
</tr>
<tr>
<td>Theft of goods or products</td>
<td>Theft of goods or products from warehouses, during distribution or while on the shop floor</td>
</tr>
<tr>
<td>Theft of cash from employer</td>
<td>Theft of cash from tills, ATMs, strong rooms, safes, of travellers’ cheques and foreign currency awaiting collection or sale, and cheques received as payment for services/fees/commission</td>
</tr>
<tr>
<td>Theft of cash from customer</td>
<td>Removal of personal cheques from customer cheque books and theft of items held within approved deposit facilities or under safe custody arrangements</td>
</tr>
<tr>
<td>False expenses/overtime/timesheet submission</td>
<td>Submission of a false or inflated claim for business-related expenses/overtime or timesheet submission</td>
</tr>
<tr>
<td>Manipulation of personal account</td>
<td>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</td>
</tr>
<tr>
<td>Manipulation of a third-party account</td>
<td>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</td>
</tr>
<tr>
<td>Removal of charges from personal account</td>
<td>Manipulation of internal accounting or IT systems with intent to defraud by removing or reducing the charges applied to personal accounts</td>
</tr>
<tr>
<td>Removal of charges from third-party account</td>
<td>Manipulation of internal accounting or IT systems with intent to defraud by removing or reducing the charges applied to third-party accounts</td>
</tr>
<tr>
<td>False/manipulated sales submission</td>
<td>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</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Manipulation of bonus/reward scheme</td>
<td>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</td>
</tr>
<tr>
<td>Facilitating fraudulent applications</td>
<td>Facilitating applications with an intent to defraud</td>
</tr>
<tr>
<td>Manipulation of applications/proposals/claims</td>
<td>Manipulating applications/proposals/claims with an intent to defraud</td>
</tr>
<tr>
<td>Manipulation of application systems</td>
<td>Manipulating application systems, for example, ignoring anomalies in applications for products and manipulating application systems to influence scoring processes or loan amount decisions</td>
</tr>
<tr>
<td>Perpetrating fraudulent applications</td>
<td>Making applications for products with an intent to default/defraud</td>
</tr>
<tr>
<td>Facilitating/perpetrating false insurance claims</td>
<td>Facilitating or perpetrating false insurance claims with intent to defraud, including the submission of false statements and false supporting evidence</td>
</tr>
<tr>
<td>Procurement fraud – personal</td>
<td>Creation of false or inflated supplier invoices for payment and other types of procurement fraud without colluding with any third parties</td>
</tr>
<tr>
<td>Procurement fraud – collusion with third parties</td>
<td>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</td>
</tr>
<tr>
<td>Facilitating transaction fraud</td>
<td>Knowingly accepting false ID to support fraudulent transactions and the facilitation of the processing of transactions on stolen/counterfeit cards or altered instruments</td>
</tr>
<tr>
<td>Facilitating/perpetrating advance fee fraud</td>
<td>Use of headed notepaper and other forms/documents to facilitate/perpetrate advance fee fraud</td>
</tr>
</tbody>
</table>
Part 2 Why is staff fraud a growing risk?

‘Insider fraud within the financial services is currently the number one threat.’ Dr James Hart, Commissioner of the City of London Police, November 2005

‘The value of employee fraud has risen almost 80% in 2005 from a year earlier – and more than 200% since 2003.’ BDO Stoy Hayward, FraudTrack Report

‘Staff theft cost retailers £498 million in 2004 – up from £282 million for the previous year.’ British Retail Consortium, Annual Retail Crime Survey, 2004/05

‘British retailers are winning the battle against shoplifters but are still being hit by staff theft. The UK is one of the worst countries in Europe for stealing by employees, costing employers £1.5 billion in 2004. The UK was second behind Iceland in a study of employee theft in 25 nations.’ Centre for Retail Research Report, 2005

‘It is common knowledge most incidences of fraud go unreported. A conservative estimate is that the total cost of employee fraud to UK listed companies alone amounts to about £2 billion per annum.’ Mike Adlem, Protiviti Independent Risk Consulting

Increasing incidences of staff fraud

General intelligence and specialist research suggests that the number of incidences of staff fraud has been rising for a number of years. Many organisations have been reluctant to admit the scale of the problem due to potential reputational damage. But it has now grown to the extent that, with increasingly obvious links to organised crime, specific countermeasures are required and this has raised the profile of the issue with the Financial Services Authority (FSA) and law enforcement agencies.

In a survey conducted by Leicester University in 2003, 70% of the 2,000 people questioned admitted they would commit fraud if they knew they would get away with it. Placed in this context, it’s unsurprising that levels of staff fraud are growing. Information from law enforcement agencies suggests that the majority of operational investigations into cheque and plastic card frauds now have an identified insider element at some stage of the perpetrated fraud.

The actual number of confirmed cases of staff fraud is rising sharply throughout the financial services industry. 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 remains at a relatively low level for both sectors. Large organisations can expect to dismiss in the region of 100–150 members of staff every 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 before an internal investigation. This can often prevent their dismissal and detailed analysis or investigation of any fraudulent activity undertaken.

CIFAS research indicates that staff fraud has been a growing problem in recent years in respect of investigations, confirmed cases, referrals and unconfirmed cases. In general, there are more cases of staff fraud and this trend has been exacerbated by the profile of the issue being raised through extra staff training and awareness and the introduction of more robust internal controls. Some organisations have seen a 30% increase in the number of staff fraud referrals made to the relevant fraud department in the past year. This is viewed as being partly the result of more staff fraud being committed and increasingly aggressive targeting by organised criminals.

Why are there more incidences of staff fraud?
In recent years staff fraud has been identified as a growing threat. Broadly, there are three interlinked reasons for this:

- changes in business and organisational structures
- changes in the type of staff employed to service these new structures
- increased targeting of business by organised criminal networks.

Historically, the most serious threat from staff fraud has been centred on relatively senior employees in management positions. However, the major threat has now shifted down the organisational hierarchy to more junior members of staff, who have access to, and responsibility for, more confidential customer and payroll data than ever before.

Changes in 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 functions. As a result, to provide quality customer service, organisations now increasingly need to hold all their customer data in one place and make them accessible to staff who work in a variety of locations – 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 in readily accessible customer databases. This 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 growth in contact and call centres has created more opportunities for organised criminals to target members of staff who have access to these extensive customer databases.

Changes in the type of staff employed to service these new structures
The shift towards and growth in contact and call centres has led to changes in the type of staff employed to service the new structures established by businesses. Those employed in call centres, and to a lesser extent branches and retail outlets, sometimes don’t 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 who are now in possession of the most valuable information 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 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, the screening process for staff employed and given access to extensive customer data can sometimes be less rigorous than required, and the employment of temporary agency staff becomes a necessity.

Increased targeting of business by organised criminal networks
There has been a massive rise in identity theft in recent years. The number of victims of impersonation recorded by CIFAS has grown from 16,810 cases in 1998 to 67,400 cases during 2006. It’s 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 increasingly targeting financial institutions, both through infiltration and by attempting to corrupt existing members of staff.

Organised criminals are likely to be targeting staff, partly because they are aware of the data they can access and their potential susceptibility to approaches, and also due to the increased volume of financial transactions that can now be conducted remotely. Telephone and Internet banking provide more opportunities for anonymous fraud by a third party if the fraudster is 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 other documentation for payment.

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 compromise customer or payroll data to allow third parties to perpetrate identity and other types of fraud represents the greatest area of risk.

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.

For example, according to the British Retail Consortium (BRC), criminal activity involving staff members cost UK retailers £2.2 billion in 2005, with 20% of all retail fraud linked to credit card misuse. The BRC estimates that, on average, theft is responsible for losses equal to 2–5% of turnover. Just 1% of turnover represents 20–40% of annual profits for the organisations affected. In total, 53% of unseen losses are the result of employee theft.

The annual FraudTrack report from accountants BDO Stoy Hayward calculates that the annual value of reported fraud in the UK shot up by nearly 30% in 2005 to almost £1 billion, and has virtually tripled since 2003. The KPMG Fraud Barometer considers major fraud cases being heard in the UK Crown Court system. In the first half of 2005, it measured a sharp increase in staff fraud cases, with £38 million of identified fraud committed by management and employees. The average management fraud cost £2 million, compared with the average employee fraud of £470,000 per individual. In the first six months of 2006, major fraud cases involving £653 million came to court, up from £250 million at the same time in 2005 and £392 million for all of 2004. According to KPMG, staff fraud continued to lead the pack, with managers named as the biggest perpetrators, making up almost half, or £310 million worth, of the cases taken to court.

In addition, analysis of the stored intelligence and data on incidences of staff fraud from Operation Sterling, the Metropolitan Police Service (MPS) response to economic crime, indicated that the average staff fraud loss reported amounted to £172,000 per case during 2005.

Reputational damage
Staff fraud can cause unquantifiable reputational damage to the image and brand of an organisation, both at local and national level. Any fraud that involves customer data is always potentially damaging, even when 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.

Regulatory implications
Organisations involved in providing financial services are at risk of being fined very significant sums of money by the FSA if they fail to manage the risk of employee fraud effectively.
A subsidiary of the giant Capita group became the first firm fined by the Financial Services Authority for having poor anti-fraud controls after some of its staff helped to defraud customers. The Financial Services Authority fined Capita Financial Administrators (CFA) £300,000 when their findings were published in March 2006.

The Financial Services Authority said the frauds were ‘incredibly serious’ and their report found that:

‘CFA did not take adequate steps to ensure that it had effective controls to reduce the risk of fraud, particularly internal fraud. There was a specific failure in training to raise awareness of fraud risk and HR procedures to verify that adequate references had been received.

Although procedures were in place, these were not always completed, especially in the following up of references ... This resulted in a material risk that new staff were not competent or lacked integrity.’

Case study: Capita

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 the additional costs involved in recruiting, vetting, training and employing a new member of staff. However, in addition, cases of staff fraud can disrupt the normal daily routines of other employees and can have a negative impact with respect to morale and trust between co-workers. Speculation and the ‘grapevine’ can lead to misinformation and unsubstantiated rumours and gossip circulating within 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 create a culture of mistrust and suspicion.

As a result, it’s crucial that organisations ensure their communication policy with respect to staff fraud is effective. Ideally, speculation should be dispelled at the earliest possible stage. If organisations ‘name and shame’ those prosecuted for fraudulent activity, this should be communicated in an appropriate forum 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 an obvious and present serious risk. This is likely to be partly due to difficulties in detection and partly due to the fact that organised criminals, until now, have found it relatively easy to obtain the data they need from the organisations they’ve historically targeted – banks. However, intelligence suggests that this is changing and that organised criminals are now targeting a more diverse set of organisations encompassing numerous business sectors and financial services firms in order to obtain customer data and perpetrate identity fraud.

In addition, the more robust controls, increased training and awareness and more stringent vetting procedures now being introduced by the banking sector are likely to cause displacement to other sectors and organisations. It’s well known that organised crime will always target the weakest link in the information chain. So it’s 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 manpower, resources or make policy changes until their organisation is affected by a significant fraud, by which time any such action taken is likely to be too late.
Part 3 Combating staff fraud

‘Nearly two-thirds of staff frauds where a motive was reported have been as a result of greed and the desire to lead a lavish lifestyle. A further 11 per cent were linked to gambling and 10 per cent were to pay existing debts.’ BDO Stoy Hayward, FraudTrack Report

‘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.’
Sir Callum McCarthy, Chairman of the Financial Services Authority

To combat staff fraud successfully, organisations need to consider:

- 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 employee’s desire to fund the type of lifestyle they aspire to but can’t afford. For example, in many cases where staff have committed fraud in order to pay off debts, they will continue to undertake fraud after the arrears have been successfully cleared. The continuation of fraudulent activity would indicate that greed is the primary driver. Indeed, research by BDO Stoy Hayward has indicated that over 60% of fraud is committed as a result of greed and to fund a lavish lifestyle.

A report by the Centre for Retail Research concluded that theft was the main criminal threat to the retail industry, with staff-related crime responsible for over 50% of total store theft.

According to the 2006 CIFAS Staff Fraud Risk Assessment, the compromise of customer or payroll data to facilitate fraudulent activity by third parties is assessed to be the greatest overall fraud-related threat to the financial services industry, and this will also be the case for businesses in other sectors of the economy. The magnitude of this threat 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 often 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 some may abuse.

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 existed previously. 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 in the past. However, the infiltration of organisations by criminals, combined with a high staff turnover, reduced loyalty, relatively low pay compared to 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’re committing.

**The profile and common characteristics shared by staff fraudsters**

Traditionally, the main threat identified in respect of staff fraud relates to older senior employees who abuse their position and the responsibility entrusted to them. These employees are primarily ‘opportunists’ who commit fraud for personal gain and have no links to organised criminals. Although any employee at any level has the opportunity to commit fraud, certain types of fraud can only be committed by senior members of staff who possess the necessary authority to carry out certain actions.

For those long-serving employees who pose a significant risk, research indicates the typical profile is of a person who is:

- middle aged (over 40 years old)
- male
- in their current employment for more than 10 years
- in middle management
- disgruntled or disaffected.

These employees are long-serving and, as a result of their seniority and perceived loyalty, they are able to abuse their position of trust. A 2004 report by KPMG Forensic, *Profile of a Fraudster*, found that, in the case of large-scale financial frauds, long-serving male executives were the most likely to be involved, with around 40% of fraud cases involving employees from the finance department. The *Fighting Retail Crime* report produced by the Centre for Retail Research found that more experienced employees may continue to steal for many years. Over 40% of the organisations interviewed reported that 25% or more of their total staff apprehensions were management grade, supervisors, senior administrators and security officers – the very people entrusted with guarding the company’s assets. They usually had unsupervised access to most parts of the building at unsocial hours and were able to steal, often in conjunction with associates, over many months or years.

‘Opportunist’ staff fraudsters who commit fraud for personal gain will usually have one dominant motivating factor, typically one of the following:

- greed to fund lifestyle
- personal problems, for example, gambling addiction or a drug habit
- being disaffected/disgruntled
- divorce
- depression
- pressure from family/friends.

However, research suggests that the main staff fraud threat now relates to theft and the compromising of customer data. This also applies to payroll and other data in all companies that can be used to perpetrate further frauds.

The *Fighting Retail Crime* report also found that the ‘typical’ staff thief was usually someone who had been employed for less than 12 months and was frequently a part-timer. Detailed interviews found that most staff fraudsters usually admitted to starting to steal in the first few weeks of their new job (sometimes after being taught to steal by a co-worker).

Contributors to CIFAS research have indicated that the typical profile of a staff fraudster involved in compromising data is of a person who is:

- young (under 25 years old)
- male
- employed full-time
- in their current employment for less than a year
- in a junior non-management role
- low paid
- possibly in financial difficulties.
Indeed, analysis of the data from MPS Operation Sterling fully supports this profile, except that it indicates a fairly equal split between male and female fraudsters. The 2005 BDO Stoy Hayward FraudTrack report found that fraud continues to be a male-dominated domain, with women accounting for only 18% of those convicted for fraud. For the first time since the analysis was started in 2003, however, women under the age of 20 have been convicted for involvement in fraud.

Those individuals who share similar characteristics with the profile above often aspire to a lavish lifestyle they’re unable to achieve due to their relatively low pay. Furthermore, these individuals have often recently been students and may be tempted to collude due to debts and financial difficulties.

It has been identified that staff fraudsters who compromise customer or payroll data will do so for one or a combination of these reasons:

- greed to fund lifestyle
- lack of loyalty and integrity due to length of service
- taking the view that fraud is a victimless crime as the customer is refunded
- not believing they’ll be detected and regarding internal controls as lax
- being unaware of the ramifications and possible consequences
- to alleviate financial problems and pay off debts
- coercion/threats against the employee or their family.

The role of organised crime
It’s generally acknowledged that incidences of infiltration and corruption of staff members by organised criminals has 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 staff with access to the necessary 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 criminal groups will attempt to plant members or associates in financial institutions and businesses. These individuals will gain employment with the deliberate intention of defrauding their new employer. Commercial pressures combined with 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 derisory 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 numbers of attempts by organised criminals to plant staff in order 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 can’t 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 who have access to customer, payroll and other data. These individuals usually have unblemished employment records and are not therefore identified as high risk in recruitment checks, for example, they have good references, no gaps in employment and no criminal record.

Approaches to staff are often made at lunchtimes or before/after work when many employees are 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 as the criminal. Many staff live locally to their employer and can therefore 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 in fact 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 of precise amounts are patchy. The direct approach offering cash to fund a person's lifestyle appears to be the most common and successful tactic to gain collusion. However, payments to reward collusion are often withdrawn once data begins to be supplied, and coercion is then used in order to continue the criminal enterprise.

In the retail industry, collusion is significant because it's normally safer than shoplifting or staff theft as separate autonomous activities. Compared with conventional staff theft, collusion ensures that the employee isn’t found in possession of the goods or cash. 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 to undertake fraudulent activity. The threats are often made in terms of harming the employee or their family/friends. Intelligence suggests that it's 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. Ongoing 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.

Employees who’ve been identified as being involved in fraudulent activity will often claim that they participated under duress or due to threats. Analysis of MPS intelligence relating to Operation Sterling indicates that 45% of the staff linked to internal bank fraud claimed to have been coerced, while 15% admitted to having been paid for supplying customer data. However, there is little evidence to confirm this and it’s 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 criminal approaches made by organised criminals and the consequences of colluding. For example, staff need to understand that collusion often leads to coercion as organised criminals withhold payments for data supplied and use blackmail and threats to force them to continue with their activities. Also, as an employer, you should ensure that members of staff are aware who to report approaches to and that they feel confident the matter will be treated with discretion and professionalism. A true zero-tolerance approach that indicates the likelihood and the consequences of being caught is also beneficial.

The five CIFAS strategic prevention areas
CIFAS has identified five steps that can help in effectively combating staff fraud:
1. Vetting and security screening (Part 4)
2. Internal corporate culture (Part 5)
3. Monitoring staff (Part 6)
4. Effective policies to respond to identified staff fraud (Part 7)
5. Analysis and deterrents (Part 8)

Case studies

In September 2005, a cashier at a high-street bank branch in Cosham, Portsmouth, was sentenced to two years for helping fraudsters steal almost £500,000 from customers’ accounts. She served customers at the branch and then trawled through their accounts to check whether they had made any large deposits in the past. She then passed on their details to a criminal gang. Equipped with information such as balances, last transactions and direct debits on the accounts, gang members walked into branches in London and Cardiff and asked to change address details and set up online banking facilities. They then used the Internet to transfer funds to accounts they controlled.

In 2004, fraudsters siphoned off £280,000 from the bank account of TV comic Harry Hill as part of a scam targeting wealthy people which netted an estimated £500,000. A court heard that an unnamed pair of criminals allegedly used threats to obtain answers to confidential security questions needed to control the bank accounts of prospective victims. These details allowed fraudsters to set up bogus bank accounts in their victims’ names and transfer money to the fraudulent accounts, where large sums of money were subsequently extracted. A customer adviser admitted passing on customer details, but claimed to have been coerced.
Part 4 Vetting and security screening

‘In a world of constantly changing threats, background screening is a first line of defence. Successfully implemented screening reduces the risk to a company from potentially fraudulent employees.’ Control Risks Screening

‘The lack of employee recruitment checks and controls in some organisations lies at the heart of the employee fraud problem. They are the first line of defence in stopping the criminals placing individuals inside your organisation.’ CIFAS research, Employee Fraud: The enemy within

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 opportunist frauds.

According to research carried out for the Risk Advisory Group in August 2005, candidates applying for jobs at finance firms are increasingly likely to lie in their job applications. Around 25% of CVs examined contained incorrect or false information, usually involving academic qualifications, previous jobs, gaps in employment and directorships. The report found that CVs had an average of three pieces of misleading information on them. Furthermore, a Mori poll found that 30% of applicants admitted to lying on their CV, while 18% thought it necessary to exaggerate. It’s therefore clear that businesses need to undertake stringent recruitment checks to combat this extensive problem, particularly when considering the additional threats from infiltration and employees’ susceptibility to collusion.

Indeed, the recruitment process should attempt to ascertain the honesty, reliability and integrity of a candidate, as well as their ability, skills and experience. A Mori poll also indicated that 34% of managers don’t check the background of most applicants because it’s too time-consuming. In addition, research by the CIPD found that only 77% of organisations always take up candidate references. This potentially represents a huge risk because the recruitment process is vital as a mechanism to mitigate the risk of staff fraud.

CIFAS ‘know your staff’ (KYS) 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.
Currently, in some organisations, the ‘know your customer’ (KYC) checks carried out to comply with Financial Services Authority requirements for opening new customer accounts are sometimes more rigorous than those in place for employing new staff. Organisations urgently need to reverse this situation and there’s a great deal of evidence to support the value of using the same types of checks for both processes.

Typical checks on customers are now risk-based but could include taking copies of up to three proofs of identity and address to satisfy the Financial Services Authority money-laundering requirements. This is usually supplemented by an electoral-roll check, a credit reference agency (CRA) check, telephone or face-to-face contact with the customer and anti-fraud database checks. Typical checks on new permanent staff, due to commercial pressures, are often less stringent.

Further information regarding KYC checks can be obtained from the Joint Money-Laundering Steering Group: www.jmlsg.org.uk

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

- completion of a corporate application form by all candidates
- identification checks
- electoral register checks
- references reviewed
- qualification checks
- Credit Reference Agency checks
- Criminal Records Bureau (CRB) checks for Financial Services Authority-Approved Persons and high-risk roles
- occupational health screening
- membership of professional bodies checks (if applicable)
- Companies House checks on employers and directors
- fraud prevention checks, including CIFAS Staff Fraud Database checks (if a CIFAS member).

Many organisations will take a risk-based approach to vetting and will view some of the checks listed above as only being necessary for positions where the potential risk is high. However, the seniority of a post doesn’t necessarily determine the staff fraud risk associated with it, for example, the growing risk from low-level call centre staff compromising customer data. Therefore the necessary vetting controls should be driven by risk rather than seniority of role.

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

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

Businesses should also consider the local environment they’re recruiting from. If it’s an identified staff fraud hotspot, it could be important to consider undertaking more thorough security checks.

Organisations 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:

- 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. When applicants submit both a CV and an
application form, the two documents should be
compared for possible discrepancies.

The application form should include specific relevant
questions so that prospective employees have to
provide information that’s unlikely to be contained on
their CV. These questions should be used to help
develop a comprehensive picture of all applicants, to
determine their suitability for the post and to confirm
their suitability as an employee of the organisation.
The information employers should consider specifically
requesting on their application forms includes:

• a full account of any gaps in employment, including
  maternity leave, unemployment, inability to work
due to injury or illness, time taken off for travelling,
  and so on
• the candidate’s reason for leaving their previous
  employment
• confirmation, if relevant, of the candidate’s
  permission to work in the UK
• any involvement in external businesses and details
  of directorships held
• details of any civil or criminal proceedings that may
  be pending
• details of any convictions that are not considered
  spent under the Rehabilitation of Offenders Act 1974
• details of any bankruptcies or county court
  judgments (CCJs) or defaults registered against the
  candidate
• details of any disciplinary proceedings, suspensions
  or expulsions by any regulatory or professional body
  or association in relation to the candidate’s business
  or professional activities
• the number of days’ absence due to injury or
  illness in the individual’s most recent 12 months
  in employment.

The form should make it clear to the candidate that
they must answer the questions truthfully; that
providing what they consider to be a detrimental
response to the question set won’t necessarily prevent
them from being appointed; and that each case is
considered on its own merits.

The application form should also request full details of
the candidate’s qualifications and employment history –
these details can be used later in the recruitment process.

It’s crucial that the application form is signed by the
candidate and includes a declaration confirming that all
the details given on the form are correct. The
declaration should also include notification of and
candidate consent to any background checks that will
be carried out, for example, the use of personal data to
undertake CRA, CRB and other fraud prevention
checks. In addition, the declaration should confirm the
candidate’s understanding that any material falsehoods
in the application may constitute misconduct and could
result in the termination of any contract of employment
entered into following this application and/or could
mean that this data is consequently shared with fraud
prevention databases.

Further information regarding background checks for
people with criminal records or on the recruitment of
individuals working with children can be found in the
following CIPD factsheets (www.cipd.co.uk/factsheets):

• Employing People with Criminal Records
• Employing People with Criminal Records: Risk
  assessment
• Recruitment of those Working with Children and
Vulnerable Adults.

Verifying candidate details
It’s 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 checks similar to the KYC checks used by
financial institutions to comply with the FSA
anti-money-laundering requirements.

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 paid to 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 that 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 in Table 6 are not exhaustive but offer details of the documents most commonly used to confirm identity. Organisations should request at least one document from List A and two from List B. The candidate should provide originals of all documents.

<table>
<thead>
<tr>
<th>LIST A</th>
<th>LIST B</th>
</tr>
</thead>
<tbody>
<tr>
<td>(If a document from List A can’t be supplied, a letter or statement can be provided from a person in a position of responsibility who knows the applicant. This letter or statement must state who the issuer is, 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 and a social worker. Contact details for this person must be supplied for verification.)</td>
<td>(These documents must show the candidate’s name and current address and must be dated within the last three months.)</td>
</tr>
<tr>
<td>• A current signed passport</td>
<td>• Utility bill (mobile phone bills should not be accepted)</td>
</tr>
<tr>
<td>• Current EEA or UK photocard driving licence</td>
<td>• Bank/building society or credit union statement</td>
</tr>
<tr>
<td>• Residence permit issued by the Home Office to EU nationals on sight of own-country passport</td>
<td>• Mortgage statement from a recognised lender</td>
</tr>
<tr>
<td>• Current full UK driving licence</td>
<td>• Local council rent card or tenancy agreement</td>
</tr>
<tr>
<td>• EEA member state identity card</td>
<td>• Council tax notification/income tax notification (valid for the current year)</td>
</tr>
</tbody>
</table>

| | |
| | • Current UK photocard 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) |
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.

Separate rules and documentation are required for confirmation of whether an individual has the legal right to work in the UK. Organisations should contact the Home Office to check their understanding of 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 listed in Table 6 can be verified electronically. For documents that contain security features, for example, passports 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 they’re aware of how to verify these documents correctly.

Written references supplied by the candidate should also be verified. It’s important that HR doesn’t rely on references that are addressed ‘to whom it may concern’. Equally, reference letters, copy certificates or verbal representations should not be accepted at face value. To verify that a reference is from a genuine company, the employer can be checked on Companies House, Yell.com or by searching for the company website. Businesses should never assume that a previous employer has carried out full and proper checks on their employees.

To confirm qualifications held, only original certificates should be accepted and, if necessary, these should be checked with the issuing establishment. Candidates claiming to have a professional membership or qualification should be checked with the registered body.

**Interviews/assessments**

Staff who undertake interviews should be trained and made aware of potential warning signs with respect to possible infiltration and the susceptibility of candidates to staff fraud. They should also be aware of aspects of the application that trigger the need for further investigation, for example, if the person is applying for a job a long way from their home, or they’re taking a pay cut, and so on.

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’re unable to validate certain information or require help in verifying the identity documents they’ve been provided with. In many organisations, which don’t have a dedicated fraud department, it will be the HR department which has responsibility for identifying potential warning signs, as well as for ensuring the validity of any information and verifying documents provided. If possible, it’s often beneficial for organisations to conduct interviews after the CRB and CRA checks so that any problems identified can be discussed and considered.

Although they remain a central element of the vetting and security screening process, many organisations now indicate that references are increasingly becoming a certificate of service rather than a reliable mechanism to confirm the integrity or performance of a candidate. As a result, HR departments now often use interviews and assessments to assess these competencies rather than relying on a third party.

**References**

Employment references are increasingly vague and of comparatively little value to businesses. 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 and when an applicant worked but are less useful with regard to the candidate’s integrity, conduct and performance.

In response to this trend, when requesting references, many organisations now use a standard reference proforma that doesn’t ask for a subjective view of the candidate and their likely future performance (this sort of information is, in any case, unreliable and can be misleading), but instead asks specific questions in an attempt to elicit the information wanted by the prospective employer. The standard reference proforma should therefore contain closed questions that focus on an applicant’s honesty, integrity, reliability, competency and punctuality. For example, it could be helpful to cover:
• dates of employment
• details of the applicant’s salary on leaving employment
• the reason the applicant left/is 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
• the number of days’ absence from work in the most recent 12-month period.

Many prospective employers will only accept the standard reference proforma if it has been completed by HR or a senior manager. When former employers complete a standard reference proforma fully, it definitely adds value to the security screening process. But some businesses have now adopted a company policy that allows them to confirm only the dates of employment or to provide a generic reference on the individual’s general performance and will refuse to complete the standard reference proforma, which of course reduces its effectiveness.

Many of the DPA concerns that drive this type of 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 complying with their obligations to inform another potential employer of an individual’s performance and conduct.

If possible, an employee shouldn’t start their new job until references have been requested, received and verified. The level of references required will be driven by the seniority and risk associated with the post applied for. However, to comply with CIFAS KYS best practice, an organisation should obtain references covering a minimum of five years. For roles that carry 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, time off for 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.

Organisations should have a policy in place in case they’re unable to obtain/verify a reference. Ordinarily, this could involve seeking an alternative reference of a more personal nature from a person in a position of responsibility. Alternatively, HR can request evidence of employment through bank statements, wage slips or an HMRC statement. If references are unobtainable, organisations can refer the case and undertake a risk assessment based on all other vetting checks that have been undertaken.

If the applicant doesn’t have an employment history, perhaps due to their age, references should still be requested. In respect of school leavers/graduates, this would include a reference from their school/university and a personal character reference from someone in a position of responsibility.

Further background checks
It has been estimated that a fifth of the working population has a criminal record. Employers should therefore encourage applicants to disclose this information through their use of fair employment practices and by stating that applications are 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 isn’t ‘spent’ until the rehabilitation period is complete. Once it is ‘spent’, the rehabilitated person doesn’t have to reveal its existence in most circumstances and can legitimately answer ‘no’ to the question ‘do you have a criminal record?’

Given that the motivation for the vast majority of staff fraud is 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. Such policies should consider the level of debt 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 a person is found to have significant financial difficulties and is being considered for a particular role in which the risk potential for staff fraud or theft is considered high, businesses should consider withdrawing the offer of employment if it has already been made.

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.

**Temporary and agency staff**

Temporary staff recruited via 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.

If possible, it’s 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 determine 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, if there is 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, their 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 if there was misconduct.

---

**CIFAS Staff Fraud Database**

The most significant response by the financial services industry to the problem of staff fraud has been the establishment of the CIFAS Staff Fraud Database. It’s well known that staff dismissed for, or strongly suspected of, fraud move from one employer to another. Deterioration in the value of references (see above) and generally inadequate levels of vetting has exacerbated this problem. Analysis of a relatively small sample of individuals linked to Operation Sterling, the Metropolitan Police Service response to economic crime, indicates that around 10% of individuals dismissed for fraud soon found employment again with another employer in the same sector, possibly with the intention of perpetrating further frauds.

As a result, CIFAS has established a database where members share data relating to staff fraud cases that satisfy the relevant burden of proof. The database is helping to prevent staff who have previously been dismissed for fraud being employed by another CIFAS member if that member considers this appropriate. The CIFAS membership, the Financial Services Authority, the Confederation of British Industry (CBI), the Trades Union Congress (TUC) and CIPD have all welcomed the establishment of this Staff Fraud Database to help organisations vet prospective employees and to act as a useful deterrent to those employees susceptible to collusion and long-serving members of staff tempted to undertake opportunistic frauds.

* The database is being made available by CIFAS to any employer that is willing to become a CIFAS member.
Current situation analysis

Currently, most employers don’t vet or security screen employees to the level recommended 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 is 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 the outsourced agencies follow best practice. Relying on a third party, whether it’s a recruitment agency or a former employer, to have undertaken satisfactory vetting is an error that should be avoided.

In spite of 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 verified and gaps in employment history satisfactorily filled. Furthermore, HR staff require specific training to enable them to identify information on CVs and application forms that trigger the need 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 the organisation having to dismiss some new joiners as the vetting process identifies material falsehoods in their applications. CIPD research found that, over the course of a year, about a quarter of employers withdrew a job offer or dismissed an individual because the person had lied or misrepresented information on their application. Although it’s best practice to complete the vetting process before allowing staff to start the new job, a sensible risk-based approach can often be effective in mitigating the threat from staff fraud and allowing the business to function efficiently.

Limits in the effectiveness of vetting

There are clear limits in the effectiveness of vetting as a mechanism to prevent staff fraud. Few ‘opportunist’ or long-serving members of staff who commit fraud are likely to be identified during this process. And, as indicated above, the main threat relates to the collusion of existing staff with organised criminals. Often, such staff will demonstrate few obvious indicators that they’re 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.
Part 5 Internal corporate culture

‘The senior management should promote an organisation culture which establishes through both actions and words the expectations of integrity for all employees in conducting business.’ Section 11, Basel Committee on Banking Supervision, July 2002

‘Companies are focusing their spending on securing systems from external attack via sources such as the internet and are not sufficiently aware of the threat posed by people with internal access.’ Rob Cotton, Chief Executive, NCC Group

**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 isn’t 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’s vital that the culture of the organisation facilitates such an approach.

It’s crucial that the internal culture of an organisation stresses the need for openness and trust between staff and managers. This doesn’t simply mean that staff are comfortable about reporting suspicions of staff fraud, it also extends to personal issues that may impact on 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. Staff should feel that their employer cares about their welfare. Employer actions could include offering an independent helpline with qualified counsellors.

However, it’s also vital that staff are fully aware that, if they committed fraud, there would be absolute zero tolerance. It should also be clear that if staff have concerns about co-workers, they have an obligation and a duty to report this. The organisation should have a whistleblowing policy that facilitates an independent and confidential means of reporting such concerns.

Employers should provide incentives for complying with the rules and deterrents for breaking them. Clearly, though, while making employees aware that there is a zero-tolerance policy towards staff fraud, care should be taken to ensure that the honest vast majority of the workforce don’t 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/organised criminals, businesses should seek to create an environment in which anyone who is approached feels comfortable enough to report this and confident that the matter will be dealt with in an effective, professional and considerate way. As suggested above, employee helplines offering confidential counselling and mediation services are useful in creating a sympathetic culture.

When seeking to create an internal culture, it’s important that clear and direct policies are formulated and 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 that help to create the desired culture. As a minimum, an organisation should have a:

- fraud management policy
- staff fraud prevention policy
- code of conduct/business ethics
- staff assistance policy
- whistleblowing policy
- fraud specialists/HR ‘working together’ policy
- investigations policy
- disciplinary policy
- fraud reporting policy.

However, policies alone can’t 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. This is what creates the preferred behaviours the policies set out to achieve.

It’s also important that the employer doesn’t condone low-level fraud, such as inflated or false expenses or timesheets. 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.

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. It’s therefore best practice to update passwords regularly and ensure that staff are aware that they are responsible for all transactions and enquiries made using their password and that they should not under any circumstances share or disclose it.

Staff training and awareness

Research by BDO Stoy Hayward has revealed that, when it comes to stopping fraudsters, businesses are failing to make use of their main ally – the honest majority of workers. When questioned, most employees said they would want to report dishonest colleagues, but many would be prevented from doing so because they don’t know the correct procedure or through fear of recrimination.

Currently, many organisations don’t have any staff fraud awareness training, while others have it only in high-risk business areas. The growing 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 how to recognise early-warning signs 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 don’t educate the fraudster.

Employees should understand that they have a duty to report both 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 being 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.

The code of conduct/business ethics documents should set out the standards expected of staff, and it’s best practice for staff to sign documents annually to confirm that they’re aware of their obligations. This will prevent staff claiming during disciplinary proceedings or interviews that they were unaware of any policies they’ve breached. The code of conduct/business ethics documents should explicitly outline expectations of
employees in a number of areas relating to security and fraud control and indicate that employees will be monitored against adherence to the code.

The role of HR
Analysis has shown that disaffected, demotivated and antagonistic employees are more likely to commit fraud. In addition, if members of staff feel underpaid, undervalued or are asked to undertake the duties of a more senior staff member, this can lead to rationalisation, where staff commit fraud to ‘earn’ the money they believe they have ‘worked’ for. Inequitable remuneration policies and bonus distribution 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 rationalise committing fraud, even if they don’t commit it themselves, they won’t 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 being 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 guidelines issued by the Advisory, Conciliation and Arbitration Service (ACAS) on disciplinary and grievance procedures, fraud should be considered gross misconduct and should warrant dismissal. This should be made clear in the organisation’s disciplinary procedures.

Whistleblowing
The operation of a whistleblowing facility so that staff can confidentially report any concerns about the conduct of other employees is an important element in tackling staff fraud. Research indicates that whistleblowing helplines are very ineffective, partly due to staff not fully trusting that they can remain anonymous and partly because they often feel more comfortable approaching line managers or their fraud department direct. Organisations should give thought 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.
Part 6 Monitoring staff

‘Fraud may be systematically under-reported, as doing so can result in reputational damage and indicate that a firm’s controls are inadequate. Survey evidence suggests many firms are misleading themselves as to the strength and effectiveness of their controls.’

Financial Services Authority, Financial Risk Outlook, 2004

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 Information Commissioner’s code on monitoring sets out some clear steps to help employers achieve this balance while also meeting their obligations under the DPA.

Risk 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 Data Protection Act. Such an assessment should identify:

- the purpose of the monitoring
- the benefits it’s likely to deliver
- any likely adverse effects.

The assessment should also consider alternatives to surveillance or less-intrusive methods of monitoring.

Monitoring at work policy
Once the risk assessment has been completed, it’s important for employers to write policies that spell out:

- their approach to monitoring
- what is prohibited
- any unauthorised areas, for example, pornographic websites
- the possible disciplinary consequences if rules are breached.

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

- giving one person responsibility for making sure 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 all staff are aware of their data protection responsibilities.

The Information Commissioner’s monitoring code generally succeeds in helping employers find the right balance between respecting their employees’ privacy and protecting their own interests. For example, on email use, the code allows an organisation to check an employee’s account in their absence if the employee has been informed that this will happen. However, an employee’s privacy must be respected if an email is clearly marked ‘personal’, unless the employer has a valid and defined reason to examine its content.

Covert monitoring
The code also protects staff from covert monitoring, except in exceptional circumstances such as when there are grounds for suspecting criminal malpractice.

Organisations that ignore their monitoring responsibilities are likely to breach the Data Protection Act 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's 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 on how workforces view their employers. Furthermore, it's important that employers explain and provide employees with a business reason for policies’ existence or changes in policies.

HR has a fundamental role in combating staff fraud in a proportionate way. A balanced approach to managing the identified risks and maintaining 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 market place, 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 in the vetting procedures applied to new entrants through to the monitoring of existing staff. Organisations must accept that there will always be a certain amount of staff fraud. The objective of the controls is to reduce the level of opportunity.

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

- a risk-based approach
- senior management accountability for the firm’s risk-based approach
- a holistic approach, avoiding disproportionate focus on any one aspect
- proportionality, with effort relating to risk, across sectors and by firms.

Those organisations where staff fraud poses a significant threat are likely to consider introducing stringent controls and tough anti-staff-fraud measures in high-risk areas. For example, in call centres, which are considered by some UK banks to be the area of greatest risk, some banks have introduced:

- bans on personal mobile telephones
- restricted access to email facilities
- paperless environments
- lockers for personal belongings
- regular spot checks on bags when staff leave the building
- the arrest of staff at their desk and in front of other employees when suspected and investigated for fraud
- ‘naming and shaming’ in cases where the individual has been convicted and this is a record of public knowledge.

Organisations where the risk from staff fraud is lower could follow a different approach that takes into account their own corporate culture, adjusting their controls accordingly.

However, for all organisations, regardless of the risk, best practice is to restrict staff access to systems, databases and communication channels to what’s 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. Businesses should also have a policy that allows them to move staff to different business areas to minimise risk in cases where staff fraud is suspected but evidence of wrongdoing isn’t readily available.

**Early-warning signs**
The vast majority of businesses rely on reactive investigations to detect and identify staff fraud. However, there are many early-warning signs that can help in proactively targeting fraudulent employees or delivering awareness training to staff, for example:

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

In addition, 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. In one major bank, of the ten top-performing sales people in one division, six were subsequently dismissed for fraud. Also, staff who are never sick or take little annual leave may be very committed or, alternatively, they might not want to be away for any extended period of time for another reason. There are many examples of staff fraud that are only discovered once the individual is away from the office due to sickness or injury.

**Internal monitoring systems**
It’s vital when monitoring staff and audit trails that organisations can identify particular enquiries or actions by individual staff members. So, when logging on to 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. Few organisations currently use any software of this kind due to the size and complexity of their organisation, while others don’t 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.
In the 1990s, Nick Leeson was appointed manager of a new operation in futures markets on the Singapore Monetary Exchange (SIMEX) for Barings Bank. By the end of 1993, he had made the company more than £10 million – about 10% of total profit that year. His bosses back in London were delighted with his performance and the large profits meant Leeson was trusted to remain chief trader while also being responsible for settling his trades, a job that's usually split. This made it much simpler for him to hide his losses when the Japanese market fell. Barings were unaware that they were responsible for the account where Leeson hid his losses. Leeson effectively bankrupted Barings Bank, creating $1.3 billion of liabilities, wiping out investors' savings and causing 1,200 employees to lose their jobs. In December 1995, a court in Singapore sentenced him to six and a half years in prison.

In April 2004, Joyti De-Laurey was convicted of plundering millions of pounds from her bosses at Goldman Sachs. Within months of starting work as a personal assistant, De-Laurey was proving indispensable in both the business and personal arenas. She made out cheques for her bosses to sign and paid their many bills, made personal shopping appointments and arranged holidays. Added to her undoubted efficiency was the sympathy she got from claiming she had cancer. However, De-Laurey abused her position of trust to plunder £4.3 million from her boss's personal accounts to fund a lavish lifestyle which included luxury cars, villas and designer gems.

In June 2006, Donald Mackenzie was jailed for ten years at the High Court in Edinburgh for embezzling £21 million from the Royal Bank of Scotland (RBS). He was caught after RBS introduced a new loan-guard computer system. He accessed the money through the bank's loan system by setting up false accounts in the names of fictitious customers at a branch in Edinburgh. Mackenzie had been named Manager of the Year for three consecutive years from 2002.

Case studies

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 prevent collateral-based fraud, parameters are system-based to stop unusual transaction approval.

Organisations that do use such software to investigate activity by staff usually do this on a reactive basis as part of the audit trail once a problem has been identified. However, organisations should give consideration to using software for proactive targeting and to prevent a potential problem developing. If criminals perceive that an organisation has weak controls, it's likely the organisation will undergo increased targeting.

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

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

- exception reports
- ‘same name’ reports to highlight cases where the account holder has the same name as a staff member accessing the account
- balance transfer reports to highlight transfers that are made soon after a change of address or other similar customer detail changes
- audit
- portfolio review
- reactivated accounts
- transaction pattern analysis
- behavioural pattern analysis.
Part 7 Effective policies for responding to identified staff fraud

‘Organisations should set standards of performance and conduct reinforced by company rules.’ ACAS Advisory Handbook: Discipline and Grievances at Work

Internal investigations and HR interaction
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’s crucial that businesses have effective policies in place to investigate allegations or suspicions of fraud. Otherwise, investigations can 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 they’re perceived as having 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 agencies are 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 in an organisation’s general fraud management policy or fraud specialists/HR ‘working together’ policy. In organisations that don’t have dedicated fraud specialists it may well be the HR department that has the primary responsibility for developing and implementing a fraud management 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 internal investigators* as soon as it becomes evident that criminal or fraudulent activity may be involved.
- Staff identified as being 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 witnesses are not interfered with. Anyone involved in the investigative process should avoid protracted conversations or unnecessary confrontation.

* The term ‘internal investigator’ is generic and simply describes the person or persons who has/have been assigned to carry out the investigation into the alleged fraud. The internal investigators may be members of the HR team, the finance department or from another business function.
During an investigation, there are likely to be interviews conducted with the staff member suspected of fraud and with possible witnesses. It’s vital that organisations clearly set out who is responsible for interviews and ensure that interviews don’t 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 isn’t 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’s not anticipated that the interviewee will disclose any adverse information during this interview. However, during the course of the interview, if they choose to disclose any facts that may incriminate them, they must be informed that information disclosed in the interview may form part of either a disciplinary process or, depending on the nature of the evidence, may be disclosed to law enforcement agencies for prosecution purposes.

At the conclusion of the fact-finding 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 appropriate disciplinary action if necessary.

**Police involvement**

Organisations should approach the police at an early stage in the investigation if they feel that potentially the police will want to prosecute the individuals involved. Then the police can take over an investigation, undertake interviews and gather evidence if appropriate. Indeed, police contributors to this guide indicated that businesses should involve law enforcement agencies at the earliest possible stage in the investigation process as, often for evidential purposes, they need to be involved when the fraud is happening rather than later in the process.

**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 on the information available to the internal investigator.

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

The questions asked in this type of interview should explore an individual’s conduct and their version of events. The individual should be asked to explain their conduct, actions and decisions in detail. 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 appropriate disciplinary action if necessary.
The police will bring many benefits to an investigation, including expertise and experience; the power to search, seize and arrest; access to forensic techniques; and asset-recovery potential. For an investigation to be successful, 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 HR and no further action should be undertaken unless instructed by whoever is tasked to carry out the investigation. It’s essential that disciplinary procedures aren’t invoked and that the staff member isn’t suspended until the appropriate HR manager, in liaison with the internal investigators, sanctions this.

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

For best practice regarding disciplinary procedures, the CIPD endorses the approach set out in the ACAS Code of Practice: Discipline and Grievances at Work. These ACAS guidelines stress the need for rules and disciplinary procedures and outline the key stages in handling these processes. The code of practice makes it clear that, although organisations can be flexible in how formal or extensive their procedures are, there is a statutory procedure they must follow as a minimum if they are contemplating disciplining or dismissing an employee. This is outlined in Schedule 2 of the Employment Act 2002.

The statutory procedure involves the following three steps:

- a statement in writing detailing what the employee is alleged to have done
- a meeting to discuss the allegations
- the right of 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, in cases 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 things that internal investigators and HR specialists should do 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.
- Prepare for the meeting carefully, ensuring they (HR) 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, and 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, with 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 are considered gross misconduct and therefore incur dismissal without notice. These offences should be misconduct that’s 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 that are normally regarded as gross misconduct:

- theft, fraud, deliberate falsification of records
- fighting, assault on another person
- deliberate damage to organisational property
- serious incapacity through alcohol or illegal drugs
- serious negligence that causes unacceptable loss, damage or injury
- serious act of insubordination
- 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 important if a case is 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 of utmost importance. The types of records that should be kept by employers are minutes of meetings, attendance records, 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 is 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 (see above).

It's 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 mentioned above, the internal investigation process will inevitably interact with disciplinary procedures. The key is to ensure that these two processes are kept separate and don’t become entangled. Therefore there are numerous stages in investigating and dismissing an individual:

1. The internal investigator (see note on page 36) becomes aware of an allegation or suspicion of fraud.
2. The internal investigator commences an investigation and informs HR.
3. The internal investigator and HR consider whether to suspend the individual during the investigation because of the level of risk, evidence, and so on.
4. The interview – this could be a fact-finding or investigative interview, with the line manager and possibly HR attending.
5. The internal investigator and HR again consider whether to suspend the individual based on the evidence uncovered during the investigation.
6. The internal investigator completes the investigation and produces a report, which should be viewed by the line manager and HR.
7. HR considers whether gross misconduct has occurred. If so, they should follow the three-step statutory procedure.
8. The person who conducted the investigation may be required to assist with any disciplinary meetings, clarifying certain matters.

Resignations
It’s well known that employees under suspicion of fraudulent activity will often resign before an investigation can be started or concluded. 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 can’t be refused, organisations should advise staff members that they are still technically employees during their contractual 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 who have resigned and are seeing out their notice period, such employees should be subject to the normal disciplinary procedures. They should therefore be invited to a disciplinary meeting and dismissed in their absence if they fail to attend. Resignation should not be encouraged as this can potentially be viewed as constructive dismissal. It’s also ineffective as a deterrent and fails to deal with the underlying issue.
Part 8 Analysis and deterrents

‘While the larger firms have been forced to wake up to fraud, those that have so far remained outside the fraudsters’ radar are not as developed. Fraud threats are dynamic and fraudsters constantly devise new techniques to exploit the easiest target. Firms need to continue to invest in systems and controls and manage their responses to fraud in order to avoid being targeted as the weakest link.’ Philip Robinson, Financial Crime Sector Leader, Financial Services Authority

Learning lessons
There is clearly a need for a joined-up approach to staff fraud and best practice involving various departments and law enforcement agencies. To understand fully the risks they face, organisations should use 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 should be analysed to produce predictive modelling, allowing subsequent preventive action to be taken. 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. Organisations should also set up 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, the potential impact of staff fraud and the types of staff fraud most commonly perpetrated. The analysis by fraud specialists and/or HR practitioners 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 indicated that there needs to be much 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 fraudulent member of staff 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 used to defraud a bank. Therefore a joined-up approach is imperative 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’s less reliant on personal relationships.

Prosecution policy
It’s very important that organisations have an effective investigation and prosecution policy to ensure that staff members identified as being 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’s 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 businesses only report to the police the cases that they feel the police will accept, investigate and ultimately prosecute. A true zero-tolerance approach would mean reporting all cases where a sufficient burden of proof exists to facilitate a prosecution. As a result, in reality, many organisations actually follow a zero-tolerance dismissal policy rather than attempting to prosecute in all cases.

Those organisations, which 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 isn’t 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 enough 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. The police are more likely to pursue a case where a confession exists, but they have even been known to turn down such cases. Contributors to this guide indicated that it’s difficult to get the police involved. Often they appear uninterested in incidences of staff fraud. Furthermore, local police often lack knowledge with respect to staff fraud and which law the member of staff has breached. For example, on occasion, the police have argued that an employee hasn’t followed correct procedures rather than committing a criminal offence.

If fraud departments have a good relationship with the police, this often helps facilitate more prosecutions. Developing strong and effective professional ties with the police is important. The police are only likely to accept cases where overwhelming evidence of guilt exists, and this is often not the case in staff fraud. 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, due to untimely submission by the organisation defrauded, reject some cases.

The police have indicated that businesses 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 under-estimation 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 that 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 DPA offence. This reluctance can hinder an investigation and can potentially cause a fraudulent member of staff to be recruited by another organisation.

Sentences
Typical sentences for staff fraud are derisory and mainly served in open prisons. Often the severity of the sentence isn’t increased due to the breach of trust and abuse of position involved in staff fraud cases. It’s difficult for organisations to stress their zero-tolerance policy and for this to act as a deterrent when sentences are so light. Typical custodial sentences for compromising customer data are for less than two years. In some instances, first offenders receive only community service or a suspended sentence. In 2005, the typical prison sentence for a fraudster taking £1 million was under four years. To increase pressure for stronger custodial 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 (research indicates that less than 5% of those individuals dismissed for staff fraud are actually prosecuted) and sentences are derisory, organisations need to develop alternative deterrents. For example:

- ‘naming and shameing’ staff fraudsters
- publicising prosecutions by inviting staff members to court to witness sentencing
- adopting a zero-tolerance policy
• using civil recovery methods
• using the CIFAS Staff Fraud Database.

Individuals who have proven involvement in staff fraud should be ‘named and shamed’ so that this can act as a deterrent to others. The best forum to promote this message, the possible disruption caused and the target audience for the message should all be considered. Because of the DPA, this should only be applied to 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 the message is disseminated in a dramatic way.

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

Using civil recovery methods, businesses can target staff benefits – for example, shares can be revoked, pensions seized and asset-recovery companies 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 the Proceeds of Crime Act (PoCA).

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 businesses finding out about their previous conduct during the vetting process.
Conclusion

Due to the diverse nature of businesses and organisations, implementing a fully standardised approach to staff fraud would not be feasible or practicable. 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 undertaking 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 comfortable reporting this and feel 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, personal safety issues and how to report staff fraud.
- There is a balance between monitoring staff, 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 appropriate 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.
- Organisations or departments where staff fraud poses a huge risk and which 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 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 comfortable reporting this and feel confident that the matter will be dealt with in a professional and considerate manner.
- There is a balance between monitoring staff, 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.
- A true zero-tolerance policy should be implemented in which all cases of staff fraud with sufficient burden of proof are reported to the police to facilitate a prosecution.
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 management and development issues including guides, books, practical tools, surveys and research reports. We also organise a number of conferences, events and training courses. To find out more please visit www.cipd.co.uk