

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.

Case studies

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.

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. Following this caution, the interviewee should be asked to repeat their previous comments and whether they wish to continue with the interview or seek advice from a colleague, line manager, HR practitioner, union representative, and so on. If the interviewee wishes to seek such advice, the interview should be terminated. The interviewee should be informed that a further interview may take place in due course and that the comments made will be reported to the relevant line manager.

Investigative interviews

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

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.

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 shaming' 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 communication policy is essential to prevent disruption and a negative impact on morale by dispelling any speculation, misinformation, unsubstantiated rumours or gossip circulating within departments.
- Those proved to be involved in staff fraud should be 'named and shamed' as a deterrent. This should take place in an appropriate forum or using an appropriate medium to minimise disruption to the rest of the workforce, for example, an intranet, circulars, conferences, training, and so on.
- 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.



CIFAS – the UK's Fraud Prevention Service

6th Floor – Lynton House

7-12 Tavistock Square

London WC1H 9LT

Email: staff.fraud@cifas.org.uk

Website: www.cifas.org.uk

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

Chartered Institute
of Personnel and
Development

151 The Broadway London SW19 1JQ
Tel: 020 8612 6200 Fax: 020 8612 6201
Email: cipd@cipd.co.uk Website: www.cipd.co.uk
Incorporated by Royal Charter Registered charity no.1079797

