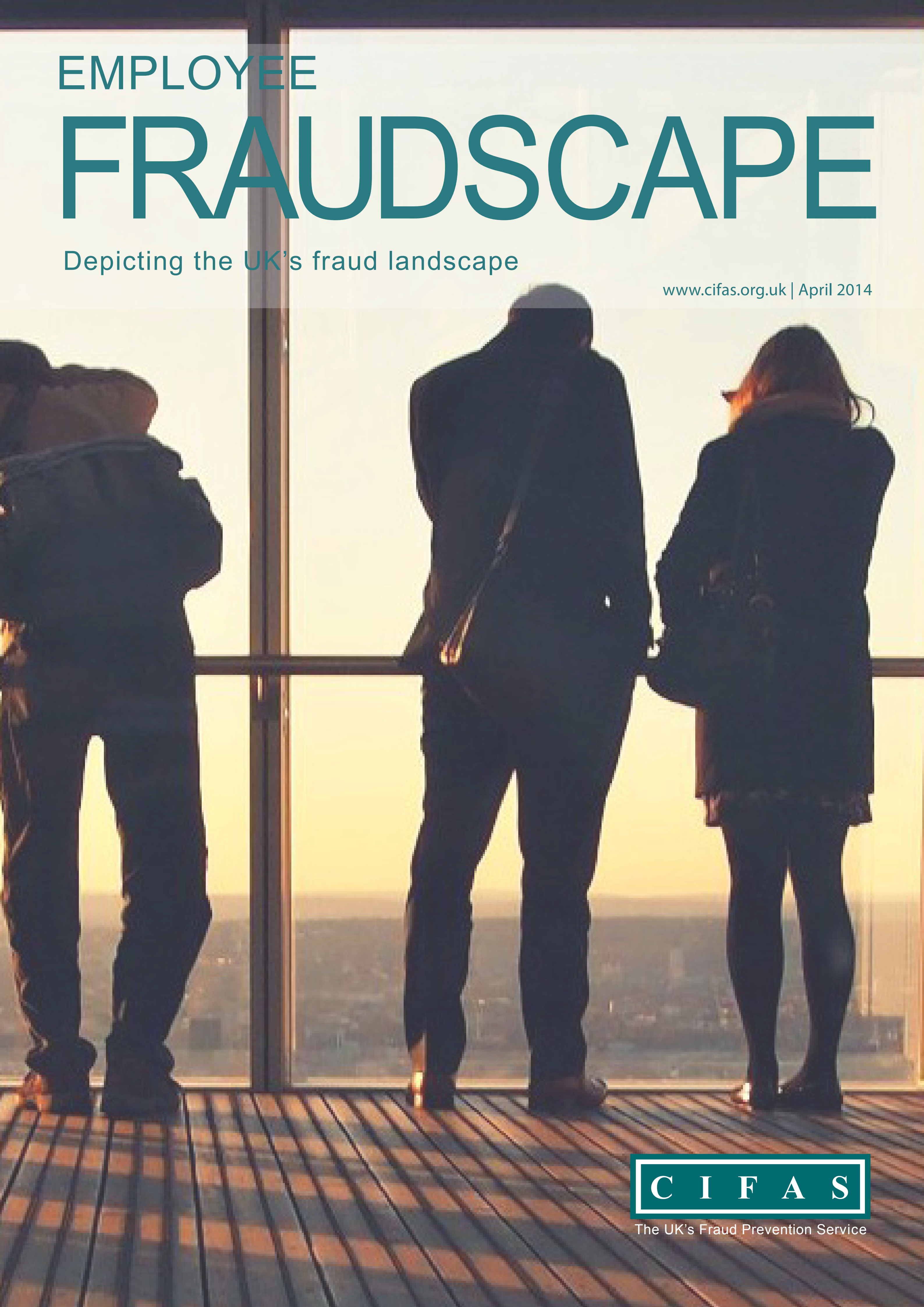
EMPLOYEE

FRAUDSCAPE

Depicting the UK's fraud landscape

www.cifas.org.uk | April 2014



CIFAS

The UK's Fraud Prevention Service

In this Report . . .

CIFAS is a not-for-profit organisation, concerned solely with the prevention of fraud and funded by subscription. CIFAS Members are drawn primarily from the UK financial services industry, but also from telecommunications, insurance, other business sectors and from the public sector.

Website: www.cifas.org.uk www.identityfraud.org.uk

CIFAS - A company limited by Guarantee. Registered in England and Wales No.2584687 at
6th Floor, Lynton House, 7-12 Tavistock Square, London WC1H 9LT

CIFAS

Introduction

By Simon Dukes, CIFAS Chief Executive

As the UK's Fraud Prevention Service, CIFAS is responsible for the largest and most comprehensive fraud sharing databases of their kind in the UK. We are a not-for-profit company and our mission is simple: to protect those Member organisations that work with us, and their customers and clients, from the effects of fraud.

Over 300 organisations share fraud information through two CIFAS databases – the Internal Fraud Database and the National Fraud Database – and the organisations represent a wide cross-section of the public and private sectors including banking, grant giving, credit card, asset finance, retail credit, online retail, savings, telecommunications, factoring, share dealing, vetting agencies and insurance.

The CIFAS Internal Fraud Database was launched in 2006 and, by the end of 2013, over 260 organisations were participating in it. These organisations share confirmed data on frauds and theft committed inside an organisation by the people it should be able to trust the most: its employees. This information is shared for the purpose of preventing further fraud in other organisations. We insist on a high standard of proof before a fraud can be recorded to the CIFAS databases and it is this data integrity which sets us apart from other data sharing schemes and makes CIFAS such an effective fraud prevention service. Intelligent data sharing allows CIFAS Members to detect, target and prevent fraud and the data which emerges from this activity, once analysed, provides a robust and reliable set of figures for the fraud landscape regarding employees in the UK in 2013.

Fraudsters are imaginative, creative and resourceful. And this is particularly true when the fraudster is an insider, because they are perfectly placed to spot and exploit any weaknesses: whether in processes and internal controls or simply because they assume that such rules do not apply to them.

The motivations and triggers to commit internal fraud, the role of organised crime, the steps that have or have not been taken to counter fraud dangers – and the ramifications for those organisations that fall victim – are constant themes in this report. We examine what has happened and what needs to happen in order to prevent an organisation's counter fraud strategy crumbling from the inside.

With the average cost of each internal fraud being as much as four times the sum initially lost*, organisations simply cannot afford to ignore it. Countering internal fraud and consumer fraud successfully demands that both fraud types are treated as seriously as each other and form the cornerstones of every organisation's risk strategy. By analysing fraud in the ways presented in this report, organisations are able to learn and apply intelligence in a way that will enable them to combat whatever happens next.

* *The True Cost of Insider Fraud* www.cifas.org.uk/research_and_reports

1. Executive Summary

An organisation's vulnerability to fraud committed by external parties is something that tends to be accepted as an inevitable risk of doing business. Figures from the CIFAS Internal Fraud Database demonstrate clearly that fraud committed inside an organisation must now be seen in parallel and should be just as integral to an organisation's risk strategy.

There were 638 confirmed cases of fraud committed by insiders or an organisation's employees and filed to the CIFAS Internal Fraud Database in 2013; an increase of 18% compared with 2012. This increase was not driven by the rise in the number of organisations sharing data through CIFAS, however. Organisations have become more adept at identifying frauds taking place on the inside and have recognised that the same data sharing and preventative steps taken to combat consumer fraud must now be taken to stop other fraud types.

'Know Your Employee' as vital as 'Know Your Customer'

Employment Application Frauds were the most commonly recorded type of internal fraud in 2013 – accounting for over 50% of all the internal frauds. This is significant as it is the first time since the founding of the Internal Fraud Database that such fraudulent attempts to gain employment accounted for the majority of insider frauds. These figures underline the particular vulnerability that organisations face during a period when the first signs of economic recovery make themselves known. As competition for jobs remains fierce, organisations need to be sure that any new recruits are precisely who they claim to be.

In some ways, this is not so very different from a customer lying to an organisation: the prospective employee/customer makes an application containing several material falsehoods and declarations (or, equally, withholds information) that is vital to the organisation's decision. This underlines the precise reason why internal threats must be seen in the same terms as external threats.

Dishonest actions still as potent as ever

Dishonest Actions to Obtain a Benefit by Theft or Deception – traditionally the most prevalent form of internal fraud – was not the most commonly recorded in 2013, but still remained a very toxic and prevalent form of fraud. Common examples included the submitting of false expenses, or stealing cash from a customer. 254 cases were recorded to CIFAS in 2013 – accounting for almost 40% of all records. This underlines the continued necessity for organisations to review their processes and controls. These are crucial not only to prevent these frauds but also to create an equal and fair culture of accountability inside the organisation: one that has a zero tolerance to fraud and that applies the same processes and principles to all levels of seniority.

Where one fraud can lead to thousands more

The Unlawful Obtaining or Disclosure of Commercial/Personal Data remains one of the less common frauds, but one whose impact and severity is immense. While numerically low (a total of 52 cases recorded in 2013), this still represented an increase on the previous year. Given that each incidence can involve the records of thousands of customers, then it becomes easier to see why over 60% of frauds reported to CIFAS' National Fraud Database are data driven identity crimes: one type of fraud links directly to another. With organised crime behind many of the thefts of data, and with this type of fraud most likely to be committed by younger members of the workforce, the battle lines of the future look set to be dominated by the use and abuse of data in all its forms.

Ownership of the problem

Understanding the trends in this report provides organisations with insight to help them counteract the insider fraud threat. Variations in those trends – combined with demographic insight such as 7.2 years being the average length of service for fraudsters recorded for Dishonest Action to Obtain a Benefit by Theft or Deception – underline that employee fraud is not committed solely by those who entered an organisation with the intention of committing fraud. There are triggers and motivations that will make some turn from committed, honest, employees into fraudsters. By recognising the motivations and triggers, organisations can go a long way to address the issues that lie behind them. Whether it is through the provision of staff support services (from employee engagement monitoring through to counselling services) or addressing issues in the culture of an organisation (i.e. making sure that the workplace is seen as fair and equitable; a place where the same standards of ethical behaviour are demanded from senior management as those expected from junior staff), organisations can be seen to take ownership of the problem of insider fraud by not shying away from the lessons it may teach them.

This sense of ‘owning’ the problem extends to organisations combating the insider fraud threat publicly. While the fear of damaging reputation is understandable, organisations are increasingly recognising that attempting to ‘hide away’ is counterproductive for two reasons. First, the inevitability that the fraud will come to the public’s attention and that this will only result in greater damage being done to the organisation if there has been an attempt at concealment. Second, by brushing cases of fraud under the carpet, the wrong signal is sent out. Organisations have made great strides in recent years in being seen to take a strong stand in cases of fraud committed by consumers. It is to be commended that the same approach is already beginning to prevail in those less frequent instances where fraud is committed by someone inside the organisation.

The damage done

Internal fraud – like consumer fraud – will have a financial cost associated with it. But, traditionally, many organisations have been willing to see it only in terms of an amount of money lost to the fraudster. As research published in 2013 by CIFAS and the University of Portsmouth attested*, the cost of internal fraud can be many times greater than the initial amount lost. Total costs will include those that are measurable (e.g. cost of investigation, disciplinary, recruitment for replacements, etc.) and those that are unquantifiable – such as the impact on reputation, lost productivity due to the impact upon staff morale, and potential loss of custom as a result. This – understandably – makes organisations nervous about ‘going public’, but should underline that the damage of fraud by an employee can be immense: therefore, being seen to take a stand by treating the fraud threat at least as seriously as it would a consumer fraud is essential.

Consistency

Tackling fraud means being as aware of the internal risks as the external risks. An organisation cannot successfully promote safe practice to its customers if its own house is not in order. Simply put – fraud is fraud: no matter who commits it, the risk is there. Counter fraud measures that are accepted when it comes to consumer fraud (such as the use of intelligence, checking, data sharing, etc.) must now start to be used by organisations with reference to the dangers and vulnerabilities that exist inside the organisation. If organisations understand that they need to verify customer information then the same steps need to be taken with reference to potential employees. If organisations want their customers to practise good online safety, then they must also demand the same of their employees. And if organisations treat all types of consumer fraud seriously then they cannot differentiate between frauds committed inside the organisation: no matter whether it is committed by a branch staff member or a senior manager. The organisation that sees its own internal practices as being a key component of its fraud and risk strategy stands a much better chance of being a safer, more stable and successful organisation. ●

* *The True Cost of Insider Fraud* www.cifas.org.uk/research_and_reports

2. CIFAS Internal Fraud Database

2.1 Overview

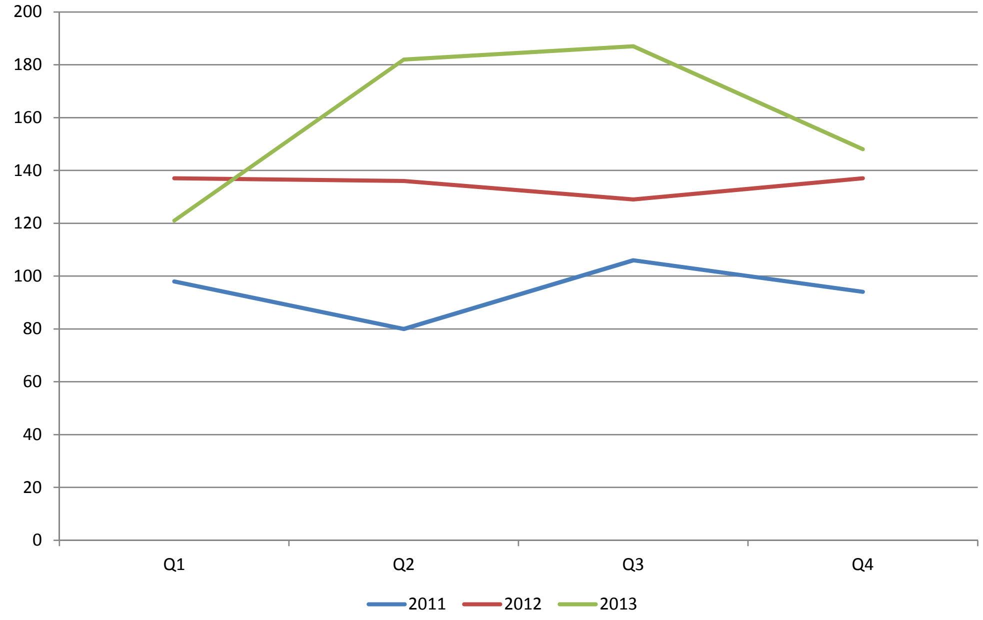
638 frauds were recorded to the CIFAS Internal Fraud Database in 2013; an increase of 18% compared with 2012. *Figure 2.1.1* shows the internal frauds recorded by participating organisations during the past three years.

Apart from the first quarter, the figures in 2013 were higher than the number recorded in 2011 and 2012, resulting in a substantial growth in the size of the database. Each year, more organisations join the Internal Fraud Database and it might be expected that this would be responsible for the overall increase in cases recorded. This isn't, however, the reason for the uplift: as fewer than 2% of the recorded cases in 2013 came from the new organisations. While this might lead to the question 'well, why have these organisations joined the Internal Fraud Database?' it is important to remember that the database forms part of their counter fraud strategy and represents a window of opportunity being closed to fraudsters that otherwise might be exploited by them.

The quarterly pattern for 2013 shows peaks in quarters two and three, with the lowest figure of the year recorded in the first quarter. No set pattern occurs annually, and the levels tend to be unpredictable for a number of reasons. The point at which a fraud takes place isn't always when the fraud is recorded to the database due to the lag between when the fraud is committed and when it is discovered. In addition, a strict standard of proof requirement means that the frauds recorded have to be ones where a clear, criminal offence was committed and with enough evidence to enable the organisation to press legal charges if it decides to do so. This carefully regulated process can take some time, as an organisation's fraud team examines the evidence and amasses the proof required. Finally, while many organisations recruit all year round, others will have designated recruitment periods and this can also affect the quarterly figures. ●

Total Internal Fraud cases recorded to the Internal Fraud Database 2011-2013

Figure 2.1.1



2.2 Internal Fraud by Fraud Type

Internal Fraud cases recorded by Fraud Type in 2012-2013

Table 2.2.1

Fraud Type	2013	2012	% Change
Account Fraud	46	55	-16.4%
Dishonest Action by Staff to Obtain a Benefit by Theft or Deception	254	268	-5.1%
Employment Application Fraud (Successful)	31	34	-8.8%
Employment Application Fraud (Unsuccessful)	293	171	+71.3%
Unlawful Obtaining or Disclosure of Commercial Data	4	2	+100.0%
Unlawful Obtaining or Disclosure of Personal Data	48	46	+4.3%

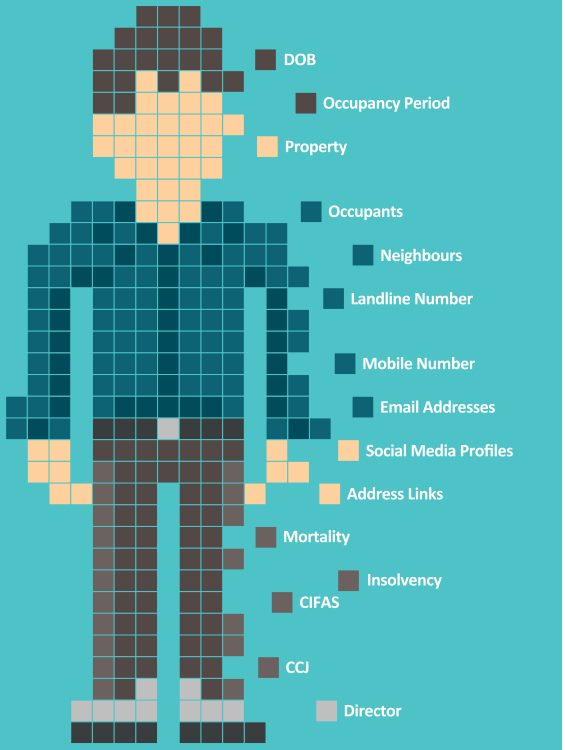
It is not just the overall numbers that tell the most interesting story. In 2013, there were many notable changes in the types of fraud recorded to the database compared with previous years. *Table 2.2.1* shows the number of internal frauds recorded during 2013 (compared with 2012) broken down by each fraud type.

Perhaps the most noticeable change was that of the Employment Application Frauds. The number of unsuccessful Employment Application Frauds increased by over 70% compared with 2012. Such frauds were ones where the individual supplied serious material falsehoods on or with their application, such as the failure to disclose adverse credit history (when a clean credit history was a requirement of the position) or claiming and providing details of professional qualifications that they did not hold. The 'unsuccessful' element means that the falsehood was identified prior to the position being offered and the application was rejected as a result of the findings. What is unclear, however, is whether the increase was the result of an increase in the number of people committing these frauds, or whether an improvement in the measures implemented by organisations to counter this threat was responsible for the rise in the detection. The number of successful Employment Application Frauds (those that were spotted only after the individual had started working for the organisation) remained relatively stable, dropping by 8.8% in 2013 compared with 2012. This highlights (if nothing else) that the checks that organisations now increasingly carry out (in order to identify falsehoods before the individual has the opportunity to commence employment) have remained robust and have enabled the vast majority of frauds to be weeded out in advance.

The number of internal frauds involving the Unlawful Obtaining or Disclosure of either Personal or Commercial Data increased slightly in 2013 compared with the previous year (up 8.3%). Organisations are understandably most concerned about both the financial and reputational damage which will arise from this internal fraud. An increase in this type of crime (as reported by CIFAS Members) confirms that the problem has not gone away. This trend is certainly one for employers to keep a close eye on. Given that each theft can involve many thousands of pieces of consumer data being stolen (and that over 60% of frauds recorded to CIFAS' National Fraud Database related to the abuse of personal data in 2013) then the potential ramifications of the problem become clear.

For many organisations, an overall increase in internal fraud is of particular concern because of the corresponding financial and reputational damage that can result. Both reputational losses and financial losses are understandably at the forefront of an organisation's mind, but the majority are unaware as to precisely how much they actually lose on a case by case basis. Collaborative research between CIFAS and the University of Portsmouth has calculated the full cost of an internal fraud being valued at several times the original fraud loss. This is because the overall, net, loss exceeds simply a financial amount lost to the fraud, but takes in many other aspects such as the costs of investigations, dismissals and subsequent recruitment*.

Furthermore, the research identifies several 'costs' that cannot be accurately calculated such as: reputational damage; the impact on remaining staff, and lost productivity. With some organisations still not undertaking adequate internal fraud prevention measures, these figures emphasise that it is now more vital than ever for employers to introduce measures to minimise the opportunities and motivations for employees to commit fraud. ●



* *The True Cost of Insider Fraud* www.cifas.org.uk/research_and_reports

2.3 Internal Fraud by Business Sector

Internal Fraud cases recorded by Business Sector in 2012-2013

Table 2.3.1

Sector	2013	2012	% Change
Banking Services	537	415	+29.4%
Plastic Cards	24	13	+84.6%
Call Centres	29	34	-14.7%
Insurance Services	22	33	-33.3%
Other Financial Services	15	10	+50.0%
Other	11	34	-67.6%

Table 2.3.1 outlines the number of frauds suffered by organisations in each business sector. Some organisations carry out business covering more than one of the following sectors so, where this occurs, their main line of business has been used. The ‘Other’ sector covers those organisations such as recruitment or IT companies that don’t fit into any of the specified categories.

It is perhaps not surprising that the business sectors suffering the majority of the reported fraud in 2013 were collectively the banking, plastic card and other financial services sectors. 61% of organisations using the Internal Fraud Database are from these three sectors, as this is traditionally where fraudsters are most likely to concentrate their criminal efforts for financial gain. With an increase of almost 30% in the number of internal frauds having been carried out in the banking sector in 2013, not only are the fraudsters recognising the opportunities for committing fraud in this sector, but the organisations themselves are aware that they are a target for criminals. This recognition drives organisations in the financial sector to implement improved preventative measures, which in turn enables them to identify and record more fraud than other sectors.

Representation within the CIFAS membership of some of the other sectors, such as call centres, is relatively small in comparison to the banking sector and they are therefore less likely to be reporting fraud in such high volumes. This doesn’t mean that the frauds carried out in call centres are any less serious. Some call centre staff have access to just as much personal information as those working in a customer facing role in a store or branch, but possibly with a level of anonymity that can enable them to conceal their actions more effectively. The call centres using the Internal Fraud Database are, however, the organisations within this sector which take fraud prevention seriously. It is not clear just how many other call centres fail to employ adequate fraud prevention measures nor, indeed, the breadth of the problem faced by them. ●

3. What Causes a Member of Staff to Commit Fraud?

As with any form of fraud, it is impossible to give one simple answer to this question. As with frauds recorded to the CIFAS National Fraud Database, it is important to remember that some frauds will have been committed by those for whom fraud is effectively a business practice. These are often the frauds with links to organised criminal activity or those used as a means to raise money for other criminal actions.

However, there will also be frauds recorded which are legally fraud but were committed by individuals for whom fraud was not a predetermined choice. The perpetrators, for instance, may commit fraud because of circumstances (e.g. partner's loss of income or job) even though the individual may never have considered committing or attempting fraud otherwise. The difference between these two overarching types of motivation are frequently described as 'fraud for need versus fraud for greed', and this description can also be used to classify frauds that are committed by someone inside an organisation.

It is – of course – important to note that the vast majority of staff would never consider committing fraud inside the organisation that employs them. The potential for loss of position and income is too great a risk even to contemplate. However, for those that do commit internal fraud, there are several motivating factors that help us to understand why these frauds take place.

1 – Greed

Fraud for greed will account for many frauds, whether committed by someone whose actions are planned and criminally motivated (typically those linked with other organised criminals) or by those who may have no other links to criminal activity. These will include a range of frauds such as:

- Someone who submits an application for employment with knowingly fraudulent declarations; made specifically for the purpose of gaining employment inside a specific organisation.
- An individual who steals customer data specifically for the purpose of selling it to outsiders (frequently, in the case of the theft of data, the recipients will be organised criminals).
- An employee who steals cash or submits fraudulent expenses claims for the sole purpose of getting extra money to fund a lifestyle that he or she – otherwise – cannot afford.

In all of these cases, the fraud is committed simply out of greed. The fraudster wants something extra and will knowingly commit fraud in order to get it.

2 – Need

Fraud for need will encompass a much wider range of motivations and circumstances. While, frequently, they will be committed by individuals who are not linked to organised criminality, there are cases where the individual has been targeted by criminals outside the organisation and coerced or pressurised into committing fraud.

The most common reasons of fraud for need are:

a) Debts (self inflicted)
b) Debts (true necessity)
c) Work targets/Deficit/Concealment of Error
d) Coercion/Threat/Blackmail
e) Addiction: alcohol, drugs, sex, gambling.

Examples of frauds that fall into this group will include:

- An individual whose partner is in financial difficulty or has become unemployed. Due to the resultant problems that they are facing the individual steals cash from the branch or store that they are employed within.

- An individual who is struggling to meet living costs. Due to this, they start to make fraudulent withdrawals from customer accounts.
- An employee who is having difficulty at work and fears for his or her future (due to possible redundancy or his or her performance being seen as 'below minimum standard'). As a result, he or she starts submitting fraudulent applications in order to appear to be 'indispensable' in comparison with other colleagues.
- Those who have difficulties in their lives due to addictions to drugs, alcohol, gambling etc. In order to maintain habits or dig themselves out of trouble, they take to stealing, or committing frauds, either due to pressure from other sources (e.g. illegal money lenders, drug dealers etc) or because they have decided that the frauds they commit are justified in view of the circumstances that they face.
- Individuals who are being threatened or blackmailed to commit frauds, frequently accompanied by threats of violence should an individual not comply.

These cases, while still fraud, potentially include some with which many people can empathise. The fraudulent action may not be condoned, but the circumstances that led an individual to decide to commit fraud are – from a human perspective – understandable. These frauds underline why organisations must consider having support mechanisms for their employees who face difficulties, in order to provide practical support that will help mitigate the risk of staff turning to fraud.

3 – The 'other' miscellaneous factors

One final group of motivations must be considered – and these can often be seen as far more complex. These include:

a) Malice/Revenge (long standing or responsive)
c) Competitive (Sabotage) /Espionage
d) Peer or Family Pressure/Loyalty
e) Psychological Problems
f) Excitement/Entertainment/Ego
g) Idealism/Terrorism
h) Stupid/Naïve (i.e. no deliberate motive)
i) Mole/Cell (i.e. only purpose to employment).

Examples of how these factors might lead to an individual committing fraud include:

- Someone who simply does not think through what they are going to do. They have either not considered that what he or she is doing is fraud, or simply do not recognise the harm that it might do.
- An individual who was passed over for employment or has served the organisation faithfully for some time, but sees or perceives superiors in the organisation to be behaving in a way that others are not allowed. As a result, a sense of entitlement or desire for revenge builds up and they make the decision to 'get their own back'.
- An employee who was effectively placed inside an organisation with the sole purpose of obtaining insight and divulging it to third parties (frequently cases of theft of commercial data or intellectual property).

As with cases of fraud for need, these frauds underline the vital importance of organisations taking steps to counter such motivating factors.

These include providing support mechanisms – from confidential helplines, employee support groups etc. – in order to help staff deal with difficulties. There is also a need for organisations to measure employee engagement, whether through surveys or other means, in order to identify any 'flash points' that are beginning to emerge.

Finally, such employee frauds underline the ever-increasing expectation that organisations will operate in a fair and transparent way: not only with their customers but also with their employees. If an organisation has a culture where it is perceived that the rules which apply to those in lower grades do not apply also to management (or that management can get away with actions that would be considered disciplinary offences for lower salary bands) then this creates a culture of resentment. This, fundamentally, can become a recipe for someone to decide to 'get their own back'.

Organisations need not only to instill an anti-fraud culture, where fraud is not tolerated by anyone, but also to marry this to a sense of fairness: where the responsibility for being transparent and fair is something all parties play a part in. ●

4. Analysis of Internal Fraud Types

To analyse the nature of the frauds in more detail, this section outlines and explains each type of fraud, focusing on the most common reasons for recording each fraud type in 2013 compared with the previous year.

ALL of the tables in Chapter 4 present the most common reasons for filing Internal Frauds and, therefore, figures in these tables differ from the totals presented in Chapter 2 and the percentage totals in this chapter will not always add up to 100%.

4.1 Account Fraud

Unauthorised activity on a customer account by a member of staff knowingly, and with intent, to obtain a benefit for himself/herself or others.

Reasons for Filing Account Frauds in 2012-2013

Table 4.1.1

	2013		2012		
Reasons for Filing	Cases	% of Total	Cases	% of Total	% Change
Fraudulent account withdrawal	23	50.0%	33	60.0%	-30.0%
Fraudulent account transfer to third party account	16	34.8%	17	30.9%	-6.0%
Fraudulent account transfer to employee account	14	30.4%	17	30.9%	-18.0%

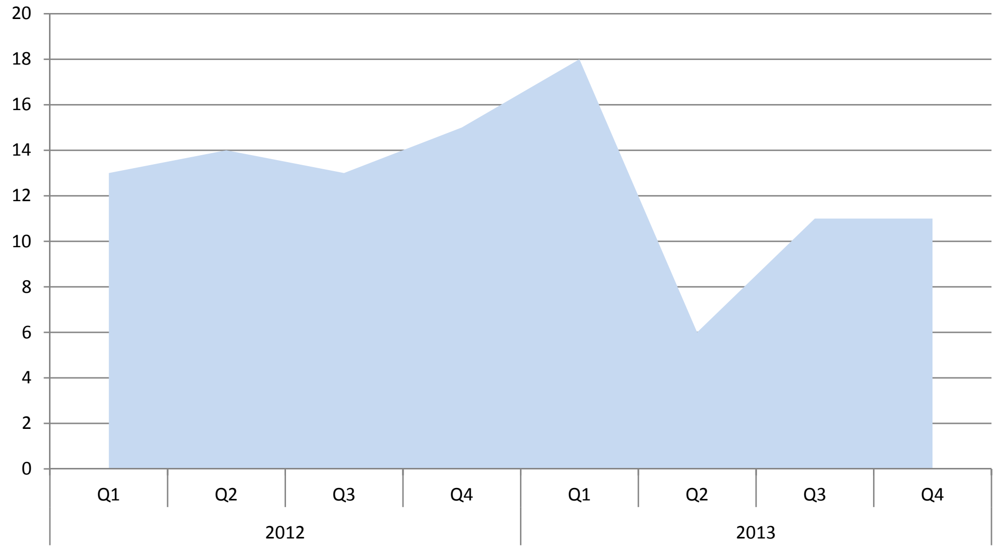
46 Account Frauds were identified and recorded to the CIFAS Internal Fraud Database in 2013. *Figure 4.1.1* shows the quarterly change in the volume of Account Frauds recorded in both 2012 and 2013. Despite the peak in the first quarter of 2013, the overall number of Account Frauds recorded in the whole of 2013 decreased by just over 16% compared with the total number recorded in 2012.

Table 4.1.1 shows the most common reasons for recording Account Frauds in 2013, compared with those recorded in 2012. It also displays the overall decrease in fraudulent account withdrawals (not to be confused with theft of cash), and how the number of reported fraudulent account transfers remained relatively stable. Internal Fraud Database users have reported multiple issues with internal fraudsters targeting the accounts of the vulnerable (e.g. individuals who are elderly or who have additional needs). The perpetrator's rationale appears to be that such individuals will either not notice fraudulent activity on their accounts or, in some circumstances, have built sufficient 'trust' with the member of staff to believe any explanations regarding any missing money. The fraudsters' activities are usually most evident where they have identified individuals whose account values are particularly large or where there has been a recent, high value credit to the account. With regards to the question 'how can organisations counter this fraud threat more successfully?' it should be remembered that it isn't necessarily easy for organisations to identify their most vulnerable customers: such vulnerability being far more easily identified by someone closer to the victim (e.g. someone in the branch who deals with the customer regularly). In addition, an organisation should always be able to rely upon their staff to act honestly, professionally and in the interests of their customers. While it should be remembered that the vast majority of staff are indeed hard working and trustworthy, there are a small number of employees who are willing to abuse that trust, meaning that organisations need to have controls and preventative measures in place.

That said, with organisations carrying out more and more internal checks and audits, it is perhaps not surprising that there has been an overall reduction in the number of fraudsters choosing to commit this type of fraud (exactly half of Account Frauds in 2013 were discovered by internal controls or audit). Unlike, for example, the theft of cash from a branch till, account withdrawals and transfers leave an audit trail and can therefore be more easily recognised and

Account Frauds recorded on the Staff Fraud Database 2012-2013

Figure 4.1.1



traced by internal systems. This highlights the importance of regular audits and staff checks, not just for the purpose of uncovering illicit activity, but also to serve as a strong deterrent. Potential fraudsters will think more carefully before committing fraud if they believe that the chance of getting caught is too high.

Interestingly, the proportion of Account Frauds that were reported to the police by CIFAS Members in 2013 (59%) outweighed the proportion of those that were not. This is the only fraud type in which this happened in 2013. For all other fraud types, the majority were not reported to the police. In 2012, there was a slightly lower rate of reporting Account Frauds (42%), which shows that the upward turn in 2013 was encouraging in terms of taking strong action. There are various reasons why this proportion of police reporting was so high. Many organisations are increasingly adopting a 'zero tolerance approach' which results in mandatory reporting to police where a case has been investigated. Additionally, unlike other types of fraud, Account Fraud is very often easier and quicker to prove as the illicit transactions carried out by the fraudster will nearly always be recorded within the company systems and are easily identified in the organisation's audit procedures. Of those reported to police in 2013, 40% of cases were taken forward to court and more reporting should lead to more convictions, which will undoubtedly increase the deterrent effect on other potential fraudsters. The message that this sends to remaining staff is also crucial: that a zero tolerance attitude goes hand in hand with legal action being taken. ●

4.2 Dishonest Action by Staff to Obtain a Benefit by Theft or Deception

Where a person knowingly, and with intent, obtains or attempts to obtain a benefit for himself/herself and/or others through a dishonest action, and where such conduct would constitute an offence.

There were 254 Dishonest Actions by Staff to Obtain a Benefit by Theft or Deception recorded in 2013, a 5.2% reduction compared with 2012. *Figure 4.2.1* shows the quarterly change in the number of dishonest actions recorded to the database in 2012 and 2013. Despite this small decrease in 2013, this kind of fraud still accounted for approximately 40% of all internal frauds in 2013.

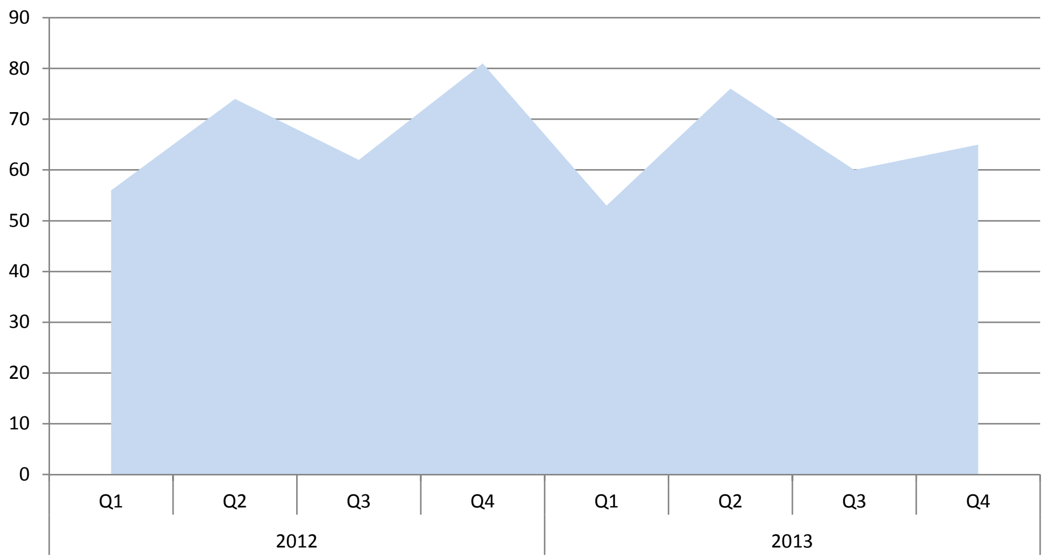
The term 'dishonest action' can refer to a number of different offences. *Table 4.2.1* illustrates the breadth of such actions by outlining the most common reasons given for recording this type of fraud in 2012 and 2013.

Over 56% of the frauds recorded as a Dishonest Action by Staff to Obtain a Benefit by Theft or Deception in 2013 related to the theft of cash by the employee: either from a customer or the organisation. In 2012, the figure was slightly lower at around 50%. This shows that, no matter what the levels when compared with previous years, the theft of cash is still pervasive. What are less well known, however, are the fraudsters' motives for stealing the cash in the first place. Criminlogists have frequently cited common reasons such as debt, gambling or drug addictions, resentment at being passed over for promotion and numerous others (see chapter 3). With the length of service of staff fraudsters perpetrating dishonest actions averaging around seven years (and, in some instances, several decades), many were established members of the workforce. This indicates that the circumstances of the fraudster may well have changed during that time, explaining why the fraud occurred a long time after they had started in the role.

It is not always known, however, for how long the individual had been perpetrating their fraud before he or she was discovered. One report states that 93% of internal frauds are carried out in multiple transactions*, so it would be fair to assume that many of these fraudsters committed their fraud(s) on numerous occasions and over a period of time.

Dishonest Actions by Staff to Obtain a Benefit by Theft or Deception recorded on the Internal Fraud Database 2012-2013

Figure 4.2.1



* *Global Profiles of the Fraudster www.kpmg.com/fraudster*

Reasons for filing Dishonest Action by Staff to Obtain a Benefit by Theft or Deception Frauds in 2012-2013

Table 4.2.1

	2013		2012		
Reasons for Filing	Cases	% of Total	Cases	% of Total	% Change
Theft of cash from customer	86	33.9%	86	32.1%	0.0%
Theft of cash from employer	57	22.4%	48	17.9%	+18.8%
Manipulation of a third party account	35	13.8%	39	14.6%	-10.3%
Facilitating fraudulent applications	21	8.3%	26	9.7%	-19.2%
Facilitating transaction fraud	30	11.8%	20	7.5%	+50.0%
Perpetrating fraudulent applications	15	5.9%	18	6.7%	-16.7%
Manipulation of personal account	17	6.7%	17	6.3%	0.0%

Once again, it comes back to the role of the organisation not only to have procedures and controls in place by which they are able to monitor staff and their actions, but to take into account other factors such as the triggers that can lead employees toward committing fraud and doing all they can to mitigate them. Additionally, organisations should not restrict their efforts to understanding and monitoring new members of staff but should extend their controls to all employees. If done carefully, this can help to foster a greater sense of equality because rules are applied to all, rather than only to some members of staff.

It's not just about the theft of cash

While it's easy to associate dishonest actions with the theft of cash from banks and other financial institutions where there is access to cash, this isn't the whole picture. Of all the frauds recorded by the call centre sector, for example, the greatest proportion of these (76%) were dishonest actions relating to the manipulation of personal and third party accounts. Considerable damage can also be done by individuals who do not work on the organisation's 'frontline' e.g. in branches, outlets or stores. Call centre or head office staff very often have access to customer data and account details and a small number of individuals have obviously taken advantage of this to conduct fraudulent activity such as the removal of account charges or the editing of account details (e.g. altering overdraft limits and changing personal details).

>

Case Study: A bank employee fraudulently opens multiple credit card accounts on behalf of others

A member of staff in the sales team of a bank facilitated fraudulent credit card applications in order to defraud the bank of thousands of pounds. The individual input details of wealthy clients into credit card applications to pass credit scoring, before changing the details to those of individuals recruited by external fraudsters. In many instances, the external fraudsters targeted those who had previously been turned down for a credit facility. The successfully obtained credit cards were subsequently used to defraud the bank of over £36,000.

Interestingly, the proportion of females recorded as carrying out a Dishonest Action by Staff to Obtain a Benefit by Theft or Deception increased from 42% in 2012 to 50% in 2013, showing that female employees are now just as likely to commit this type of fraud as their male colleagues. Traditionally, for many organisations, women are more likely to be found working in front of house roles and positions within the branches and financial institution outlets. This of course means that they have direct access to cash – theft of cash being the top reason for recording this type of fraud. This goes some way to explaining the higher proportion of female fraudsters who perpetrate this particular type of fraud. In other words, males may still be the most likely to commit fraud generally, but the greater volume of female workers in these roles will have skewed the proportions slightly. ●

Case study: A bank cashier stole £17,000 to fund an expensive lifestyle

A 25-year-old cashier carried out over 100 transactions at the bank branch where she worked in order to steal over £17,000 from elderly customers. She carried out her actions over a period of two years and explained the transactions on customers' accounts as 'banking errors'. The worker used the money to fund a lifestyle beyond her means, as she was in debt but still wanted to treat her boyfriend to expensive meals and lavish nights out.*

* www.dailymail.co.uk/news/article-2535177/Barclays-cashier-25-jailed-stole-17-000-bank-pay-romantic-nights-boyfriend.html

4.3 Employment Application Fraud (Successful)

A successful application for employment (or to provide services) with serious material falsehoods in the information provided. This includes the presentation by the applicant of false or forged documents for the purpose of obtaining a benefit.

In 2013, there were 31 successful Employment Application Frauds recorded to the Internal Fraud Database, a decrease of just under 9% compared with the year before.

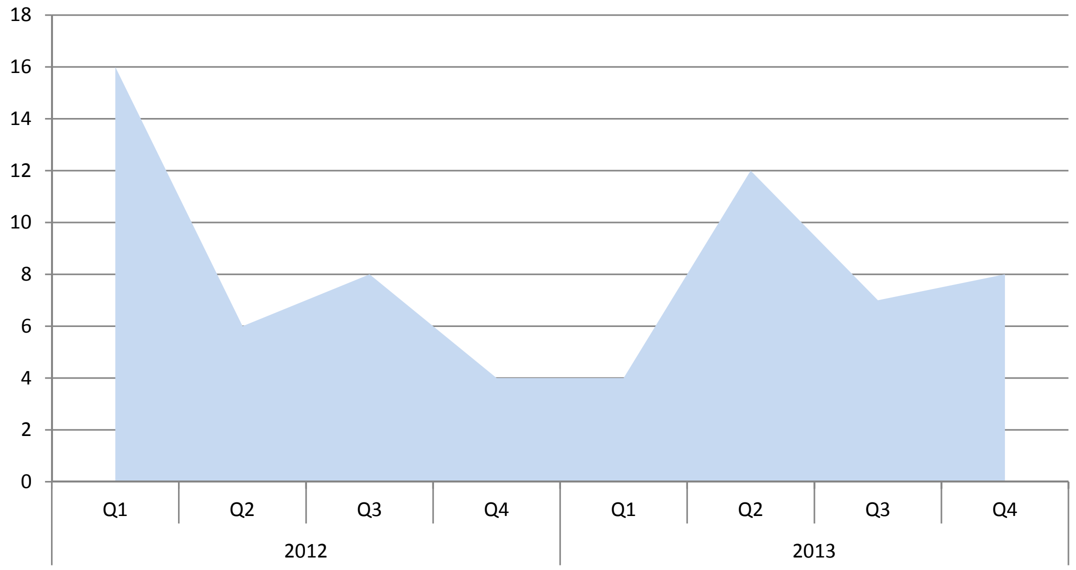
In 2013, successful Employment Application Frauds made up just 11% of *all* Employment Application Frauds. This was actually a decrease compared with 2012, where the number of successful frauds accounted for 17% of all Employment Application Frauds. *Figure 4.3.1* shows the quarterly variation in the number of these frauds recorded in 2012 and 2013.

Understanding what this fraud really constitutes

When asking ‘why do some applicants feel the need to provide falsehoods or conceal information when applying for a job?’, the obvious answer is to make them appear more employable than they actually are, particularly if they are lacking specific skills or experience required for the role. This is – in some ways – entirely understandable in light of the past five years of high unemployment, and squeezed standards of living due to stagnation in wages. As a result, some prospective employees mistakenly feel that there is little wrong in ‘embellishing the truth’. But it is vitally important to differentiate between those who have claimed to have (for instance) a higher grade in a school qualification and those whose actions are deemed fraudulent because the information that they supplied has or had a direct influence on whether the organisation would then offer them the job. Falsehoods such as concealing unspent convictions, previous positions from which they were dismissed, or adverse credit history (when relevant to the position) are understandably pieces of information that the applicant would rather withhold from potential employers, especially when competing for jobs with many other good quality candidates. An issue related to this is the Information Commissioner’s Office’s decision to prohibit ‘enforced subject access’ practices which means that any

Number of Successful Employment Application Frauds recorded in 2012-2013

Figure 4.3.1



Reasons for Filing Successful Employment Application Frauds in 2012-2013

Table 4.3.1

	2013		2012		
Reasons for Filing	Cases	% of Total	Cases	% of Total	% Change
Concealed unspent criminal convictions	12	38.7%	7	20.6%	+71.4%
Concealed employment history	11	35.5%	11	32.4%	0.0%
Concealed employment record	4	12.9%	7	20.6%	-42.9%
False documents	4	12.9%	3	8.8%	+33.3%
False references	3	9.7%	10	29.4%	-70.0%
Concealed spent criminal convictions	2	6.5%	3	8.8%	-33.3%
False qualifications	2	6.5%	1	8.8%	+100.0%
False immigration status	1	3.2%	0	0.0%	-
Concealed adverse credit history	0	0.0%	3	8.8%	-100.0%
Use of a false identity	0	0.0%	3	8.8%	-100.0%

organisations that use such practices will have to rethink their policies, especially for roles that are ineligible for Disclosure and Barring Service checks*. Other examples of falsehoods might be false professional qualifications which are stated as being mandatory or desirable in an application, false references or the use of false documents to support an application (e.g. forged qualifications). *Table 4.3.1* highlights the reasons for recording successful Employment Application Frauds in 2013.

Over 35% of successful Employment Application Frauds were recorded as a result of applicants concealing unspent criminal convictions, which could be a reflection of both the length of time it takes to process a DBS (formerly CRB) check and also an increase in the number of checks carried out by employers. It is likely that the successful applicant was appointed to the position subject to checks, and those checks then revealed the concealed convictions. The same situation applies to concealing employment history and employment records; in these instances the checks were probably conducted just after the applicant had begun employment. Although the individual was unlikely to have been in employment for very long before these checks were undertaken, the fact still stands that anyone purporting to be someone or something that they are not can be a dangerous individual to allow into an organisation. Employers need to be safe in the knowledge that their employees are trustworthy and capable of doing their job. It is clear that, wherever possible, carrying out comprehensive vetting procedures *before* their chosen candidate has been appointed should be a priority. The challenge for organisations, therefore, is to ensure that checks are done quickly: and balancing the time taken to conduct such checks with the perceived 'need' to fill a position quickly.

* www.infosecurity-magazine.com/view/37014/graham-reappointed-as-uks-information-commissioner/

4.4 Employment Application Fraud (Unsuccessful)

An unsuccessful application for employment (or to provide services) with serious material falsehoods in the information provided. This includes the presentation by the applicant of false or forged documents for the purpose of obtaining a benefit.

There were 293 unsuccessful Employment Application Frauds recorded to the Internal Fraud Database in 2013, an increase of over 70% compared with 2012. *Figure 4.4.1* shows the number of this type of fraud recorded in each quarter of 2012 and 2013. Although stable throughout 2012, the number increased substantially in 2013 and peaked in the third quarter of the year. The increase in the number of unsuccessful Employment Application Frauds was the primary driver behind the overall increase in internal fraud in 2013. The scale of the increase in this type of fraud in 2013 is interesting, and raises some questions and points for consideration.

Organisations have recognised the risks

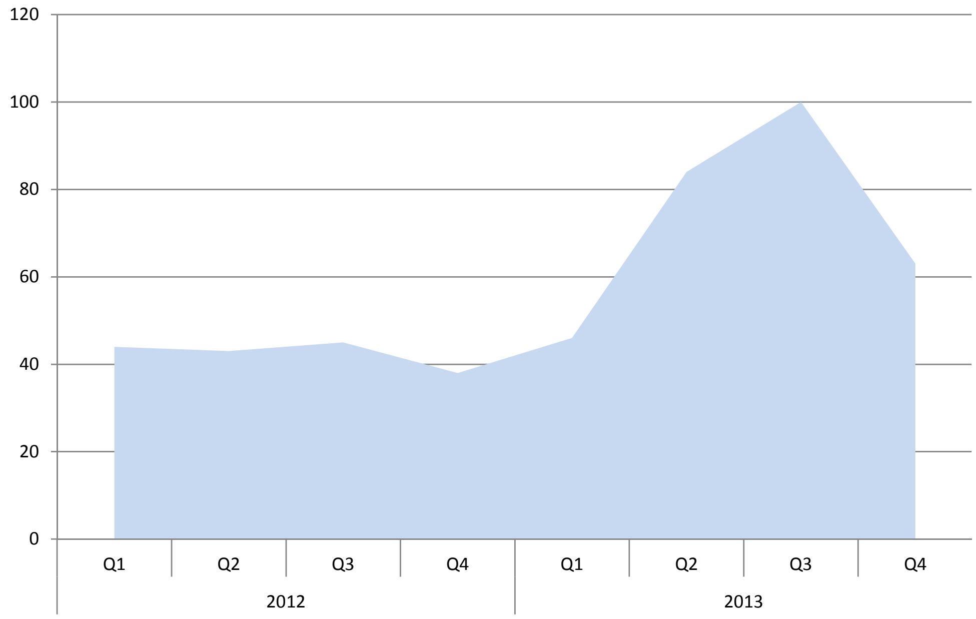
When comparing the numbers of Employment Application Frauds that were unsuccessful with those that were successful, it is obvious that many organisations have got better at identifying such fraudulent applications before the fraudster had a chance to take up employment. This is a sign that organisations have started to take their internal vulnerabilities as seriously as the threats that might be posed to them from outside the organisation.

Unsuccessful Employment Application Frauds accounted for 83% of all Employment Application Frauds in 2012, but in 2013 this proportion had risen to 90%. This further underlines the ways in which employers are effectively detecting these frauds at an early stage and protecting themselves against hiring applicants who are not precisely who or what they claim to be. While it is important to note that there is no cast iron guarantee that a successful application fraudster will go on to commit further fraud within the organisation, for many employers this represents a risk too far, especially if the candidate is not qualified or suitable for the job.

>

Number of Unsuccessful Employment Application Frauds recorded in 2012-2013

Figure 4.4.1



Reasons for Filing Unsuccessful Employment Application Frauds in 2012-2013

Table 4.4.1

	2013		2012		
Reasons for Filing	Cases	% of Total	Cases	% of Total	% Change
Concealed adverse credit history	253	86.3%	116	67.8%	+118.1%
Concealed employment record	18	6.1%	27	15.8%	-33.3%
Concealed employment history	15	5.1%	24	14.0%	-37.5%
Concealed unspent criminal convictions	11	3.8%	8	4.7%	+37.5%
Concealed spent criminal convictions	2	0.7%	2	1.2%	0.0%
False documents	1	0.3%	7	4.1%	-85.7%
Use of a false identity	1	0.3%	4	2.3%	-75.0%
False references	1	0.3%	3	1.8%	-66.7%
False immigration status	1	0.3%	0	0.0%	-

In some situations, the risk is very easy to understand. For example, if a doctor was found to have forged his or her medical qualifications – or if a teaching applicant had failed to disclose a past conviction which made him or her unsuitable for work with children – then the risks are obvious. These are the dramatic ends of the spectrum; and so many will think 'how can this be compared with someone who has inflated their previous experience in an office based environment or failed to disclose a poor credit history?' The potential consequences are of course very different, but the risks are comparable. Should an organisation advertise for an IT project manager (for instance) and specify that the applicant must have specific knowledge, experience and qualification attributes or time spent undertaking a specific role, then the risk of employing someone who has fraudulently claimed to have these skills or abilities is immense. What would happen if someone who did not have the experience that they claimed to have was put in charge of the IT capabilities of an organisation? The reputational risks, as well as the danger of irrevocable damage being caused to the organisation, its employees and its customers could result in lost business, huge fines, not to mention a public relations disaster. For financial services organisations handling customers' funds, the risks associated with such frauds are equally clear. This explains why organisations are increasingly aware that verification of qualifications and experience is absolutely essential: recognising that it is not about 'not trusting' an applicant but making sure that the risks have been removed.

Previous research carried out between CIFAS and the Serious Organised Crime Agency in 2011 (now a part of the National Crime Agency) demonstrated that organised criminals were known to target organisations too – in order to 'plant' someone inside – emphasising even further the risks of not vetting applications*. By weeding out such individuals early, organisations can do much to build their resilience to potential insider threats.

What is a falsehood?

As seen in Chapter 4.3, Employment Application Fraud can cover a variety of falsehoods in an individual's application. On one level, this can mean inflating a grade in a qualification where there is a stated minimum, and on another it could be an attempt to conceal relevant adverse credit histories. But it can also cover the complete fabrication of an essential professional qualification or the hiding of serious criminal convictions. Fundamentally, this fraud relies on the fraudulent declaration being relevant – therefore, having a direct influence upon the organisation's decision to offer the position to a prospective applicant. These falsehoods only constitute a fraud if the prospective employer would have made their hiring decision based on the false information supplied.

What frauds took place?

Table 4.4.1 outlines the reasons for recording unsuccessful Employment Application Frauds in 2013, compared with 2012.

Just over 86% of unsuccessful Employment Application Frauds were recorded after an applicant had concealed

* www.cifas.org.uk/organised_crime_sevennovember

Financial Conduct Authority (FCA) requirements for 'Fit and Proper Persons'

The Financial Conduct Authority (FCA) stipulates a set of requirements that individuals applying for or working in certain positions within regulated organisations must meet. If the individual meets the FCA requirements and is deemed a 'fit and proper person', then he or she is able to be employed in a position which involves the carrying out of work relating to a regulated activity.

The three overarching requirements are 'honesty, integrity and reputation', 'competence and capability' and 'financial soundness'. Each of these overall headings is broken down into a number of far more specific pieces of information, of which the relevant organisation must be aware in order to make a decision about the suitability of the individual in question. The fact that an individual has (or is subject to) any of the conditions below doesn't mean that they will be automatically rejected for a position; any information provided by an individual has to be assessed on a case by case basis and the surrounding circumstances taken into account. The more detailed criteria are as follows:

(1) Honesty, integrity and reputation

- Criminal offences
- Adverse findings or settlements in civil proceedings
- Previous investigations or disciplinary proceedings
- Justified complaints relating to regulated activities
- Involvement in a company which has been refused registration, a licence or trading
- Director/partner/substantial management in an insolvent/liquidated/administered business
- Investigated, disciplined, censured or suspended or criticised by a regulatory or professional body
- Dismissed/asked to resign from employment or position of trust

(2) Competence and capability

- Experience
- Training
- Competency

(3) Financial soundness

- Subject of bankruptcy
- Subject of judgment debt that is outstanding or has not been satisfied in a reasonable period

some form of adverse credit history (for example, hidden previous addresses with recorded CCJs or payment arrears) after the employer had requested information regarding their financial situation or any debts they may have had.

Risk factors

Individuals applying for jobs obviously want to 'beat the competition' and ensure that they stand the best possible chance of being successful with their application. For many with poor financial histories, they wrongly believe that hiding such adverse information will mean that their prospective employer does not become aware of it. Prospective employees may also think that if they have, for example, defaulted on payments in the past, then such adverse information would be taken into account when assessing their overall integrity and consequently their suitability for the role that they have applied for. In addition to this, a lack of disclosure on the employee's part can hide the potential susceptibility to coercion from outside criminal advances. In other words, an employee who has substantial debts or financial problems can often be more vulnerable to bribes and incentives from external criminals seeking to commit fraud. This is clearly something that the employer would need to be aware of and is a risk that organisations will take into account. The fact that an applicant has made declarations that can be proved to be fraudulent, therefore, represents a risk too far.

>

Whose responsibility is it?

The reality is that concealing this information will put the applicant in a far worse position than before, having committed fraud in order to hide certain aspects of their past. This raises a debate that mirrors one currently taking place regarding consumer education and fraud: whose responsibility is it? Certainly, the vast majority of people would not want to take a risk and make serious fraudulent declarations in any application: whether it is for a credit card or a new job. But how far should organisations go to underline the necessity and requirement for people to be truthful in their application? Does being very proactive and underlining the need to make truthful declarations 'put people off' or send out the wrong message? But by doing nothing and not explaining what constitutes fraud (and the potential consequences), are organisations failing to help dissuade applicants who incorrectly believe that 'there is no other way'? In a time where a wider debate is being held about ethics and honesty in public positions, or at boardroom level, shouldn't organisations and individuals alike recognise that this integrity and honesty can only take root at all levels if all individuals adhere to the standards? •

4.5 Unlawful Obtaining or Disclosure of Personal/Commercial Data

the use of commercial/business/company or personal data where the data is obtained, disclosed or procured without the consent of the data owner/controller. This includes the use of commercial/personal data for unauthorised purposes that could place any participating organisation at a financial or operational risk.

In 2013, there were 48 cases of the Unlawful Disclosure or Obtaining of Personal Data (a slight increase from the 46 recorded the previous year). The number of cases for commercial data doubled from two instances in 2012 to four in 2013. *Table 4.5.1* outlines the reasons for recording this type of fraud.

The internal fraud with the biggest external implications

The most common reason for recording the Unlawful Obtaining and Disclosure of Data in both 2012 and 2013 was the disclosure of customer data to a third party. The proportion of this type of fraud increased; accounting for 56.3% of unlawful disclosure frauds in 2012 and 61.5% in 2013. Due to the potential criminal use of personal information, the ramifications of disclosing customer data to a third party can be huge, and the fraud itself is often not the end of the story.

Data harvested from organisations by internal fraudsters is often done for the sole purpose of committing further fraud, usually by trading it online with other fraudsters for use in identity frauds. This obviously has implications beyond the actions of the internal fraudster, with each customer's personal and financial details having the potential to be exploited multiple times by identity fraudsters and similar. Aside from that, many internal fraudsters may choose to carry out fraud on the existing accounts or facilities held by individuals whose data they have stolen. Access to personal information means that fraudsters have the relevant data needed to bypass security questions and take over existing accounts. This too has far reaching consequences for the

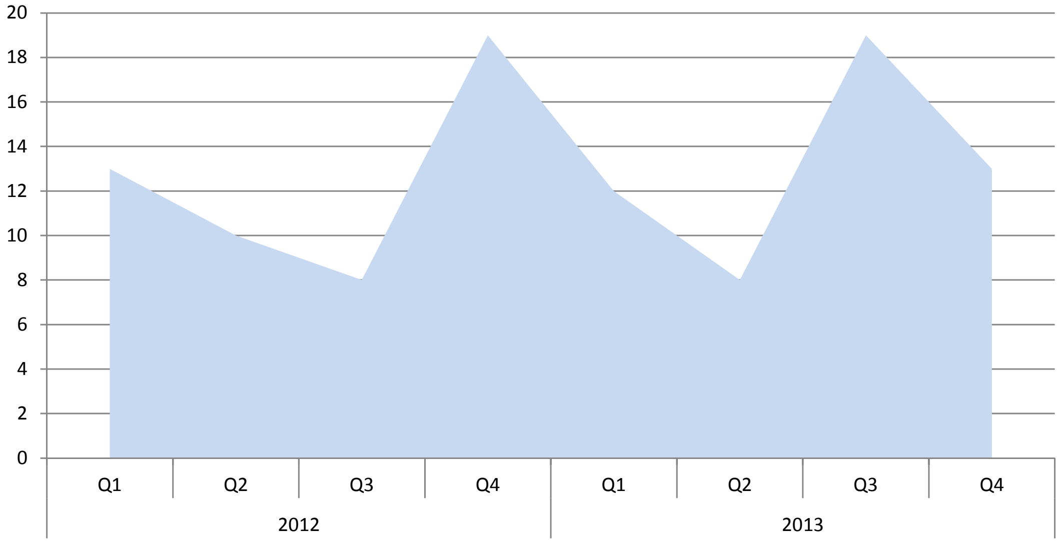
Reasons for filing Unlawful Obtaining or Disclosure of Personal/Commercial Data frauds in 2012-2013

Table 4.5.1

	2013		2012		
Reasons for Filing	Cases	% of Total	Cases	% of Total	% Change
Disclosure of customer data to a third party	32	61.5%	27	56.3%	+18.5%
Fraudulent personal use of customer data	15	28.8%	12	25.0%	+25.0%
Contravention of IT security policy	11	21.2%	5	10.4%	+120.0%
Contravention of systems access policy	9	17.3%	10	20.8%	-10.0%
Unauthorised alterations to customer data	4	7.7%	9	18.8%	-55.6%
Contravention of email policy	2	3.8%	0	0.0%	-
Theft of internal practices	1	1.9%	0	0.0%	-
Theft of intellectual property	1	1.9%	0	0.0%	-
Disclosure of internal practices to third parties	0	0.0%	2	4.2%	-100.0%
Modification of customer payment instructions	0	0.0%	1	2.1%	-100.0%

Total number of Unlawful Obtaining or Disclosure of Personal/Commercial Data Frauds recorded in 2012-2013.

Figure 4.5.1



employer, as they will be the ones carrying the customer loss and reputational damage, as well as the direct costs associated with their internal fraudsters' actions.

Disclosing the data is not necessarily the only role that the internal fraudster plays in this scenario. An insider is often a key element of an organised fraud gang, as they not only have access to the data but they have the knowledge and information needed to filter the 'worthwhile' targets (for example, harvesting details belonging to vulnerable or high net worth individuals). In these instances, it can be assumed that the internal fraudster is working closely with organised criminals but how this has arisen is often unclear. The fraudster could have been working within the organisation lawfully before an approach from an outsider made them decide to act fraudulently, possibly with the promise of a financial incentive. Alternatively, the internal fraudster may have been placed in the organisation by an organised crime group for the sole purpose of committing this specific fraud. Despite the average length of service of the fraudsters committing these data disclosure crimes remaining lower than for other fraud types at 4.7 years, it doesn't necessarily mean that this length of time is particularly low. When taking into account the possibility that these members of staff could have been planted by organised criminals, 4.7 years suddenly seems to be a long time for these employees to have been committing their frauds.

It is worth noting that these data theft figures tie up with the pattern in data driven identity crimes that have been recorded to CIFAS' National Fraud Database during the

Identity Crimes

Identity crimes are those frauds which rely on the personal data of the victim (e.g. name, date of birth, address and postcode, email addresses and passwords). Identity crimes predominantly take one of two forms:

Identity Fraud – where a fraudster uses the identity details of an innocent party in order to obtain products and services in their victim's name.

Facility (or Account) Takeover Fraud – where the fraudster has enough data (e.g. log in details, passwords etc.) to access the account and hijack it.

Data from the CIFAS National Fraud Database shows that identity crimes have constituted over 60% of all recorded fraud during recent years*. Considering that one case of data theft on the Internal Fraud Database can involve thousands of customer records, and that the takeover of plastic card accounts – in particular – shows a specific bias towards a favoured type of victim (men aged 50+ years), then it is impossible not to draw a connection between one fraud (theft of customer data) and another (identity crime).

With data driven identity crime being consistently recorded as the predominant fraud in the UK, this link will undoubtedly be one of the key battlegrounds in the future of fraud prevention.

* *Fraudscape (2014 Edition)* www.cifas.org.uk/research_and_reports

past five years: where such identity crimes have gone from a serious challenge in the pre-recessionary period to accounting, now, for over 60% of all fraud (see the 'Identity Crimes' text box). This, in itself, acts as a stark warning to organisations to use whatever techniques are practicable throughout the length of their employees' service to keep internal fraud at bay including: vetting, auditing, monitoring, instilling an anti-fraud culture and raising staff awareness of how they can spot and report instances of fraud without fear of reprisal.

The generation gap

Interestingly, 65% of individuals who unlawfully disclosed personal or commercial data in 2013 were between 21 and 30 years of age – a higher proportion of younger people than for any other fraud type, which tells us something about the individuals involved. Younger individuals are often (rightly or wrongly) perceived to be more technologically capable than other individuals, and having these skills would certainly aid them in the unlawful accessing of data from company systems. Perhaps being young, some of these individuals (but certainly not all) may be more naïve and more susceptible to approaches from external criminals.

To understand more about those who commit fraud, CIFAS conducted a piece of collaborative research with Experian using their consumer classification tool, Mosaic. One of the key findings highlighted that young and well educated city dwellers (named as 'Bright Young Things' by Mosaic's classification system) have an unusually high tendency both to commit – and be victims of – fraud. Being young and having just started out in their careers means that these individuals may have low disposable incomes but high aspirations; a toxic mix that might lead them to commit various types of fraud in order to support their new lifestyles. If organisations are unable to influence the motivation or limit the opportunity of these individuals (e.g. if their job involves working with sensitive data), it then becomes essential that they focus their efforts on monitoring these staff members. Implementing comprehensive controls and auditing techniques in order to detect the fraud will also help to prevent it at an early stage. In addition, as CIFAS has commented previously, the digital revolution means that a generational difference does exist: between those who have learned to use the internet and those who grew up as children with the internet. This latter group – the 'digital natives' – are perhaps more acutely aware of the importance and the power of data; meaning that they are the ones most

Social Engineering Techniques

Organised criminals often try to recruit members of staff for the specific purpose of using them to commit or facilitate fraudulent activity. The criminals offer a financial incentive which (for some) is too tempting to resist. The first step the criminals must take, however, is to persuade staff members to engage with them, and to do this they will try a range of techniques, the most common of which are outlined below.

(1) Street approaches
The criminal identifies staff member(s) leaving their place of work and approaches them.

(2) Social approaches

- The criminals might identify suitable staff and 'befriend' them, for example, in the local pub before introducing them to the idea of carrying out the fraud. The aim is simply for the criminal to build up sufficient rapport/trust with the individual.
- Carrying on from this, the criminals might go one stage further and specifically target their approaches. For example, young male criminals have been known to target middle-aged single women: believing them to be more susceptible to an approach which is disguised through the means of a 'potential relationship'. The criminal will use the trust that they have built with the staff member to get them to carry out illicit activity or simply turn a blind eye to it.

(3) Online/social media approaches
The techniques outlined above will often be used in an online environment. Staff members often list employment details on social media websites, making it easy for fraudsters to identify those who could be targeted. The criminals may then email/message the staff members to build up rapport and trust with the individual.

capable or most likely to see what use they can make of the data that they work with.

Organisations that use CIFAS have also reported an increasing number of instances where their existing employees have been approached by organised criminals to carry out fraudulent activity on their behalf. In some cases, the external criminals want procedural information, for example, transaction values that would arouse suspicion or processes that the organisation may have in place to identify fraudulent activity. In other situations, the criminals may be more forthcoming in their approaches, again with incentives or bribes for staff members who can facilitate data compromises or to allow organised criminals access to certain systems. The tactics that organised criminals employ range from approaches on social media sites to stopping staff members on the street as they leave their place of work. Not captured in the data and also a problem for employers are the instances where an individual has been coerced or blackmailed into carrying out fraud for the benefit of external criminals. Organisations should be particularly vigilant about this sort of activity, not only to prevent the far-reaching consequences of the employee's actions in aiding organised criminals, but also as a duty of care to ensure the wellbeing of their employees.

Commercial data theft

The number of cases of commercial data theft recorded to the Internal Fraud Database remained low. The question is 'why was this?'

Some organisations will be utilising Data Loss Prevention (DLP) solutions. These are designed to detect potential data breaches or data exfiltration transmissions and prevent them occurring, for example screening outgoing emails to check for any being sent out that might contain intellectual property owned by the organisation. This type of monitoring will be highlighted in a staff handbook or an information security policy, so these controls will doubtless provide a clear disincentive to attempt any type of commercial data theft. It is, though, often cited by participating organisations that if a breach does occur, it can be very difficult to prove the case against the individual responsible to the standard required to record the case to the Internal Fraud Database.

Although not often recorded, the damage caused to an organisation by the theft of commercially sensitive data (which can include the likes of key financial information or technical product design) can be substantial. This means that organisations who suffer such a loss will be heartened by the establishment of a dedicated police unit to tackle intellectual property thefts. The Police Intellectual Property Crime Unit (PIPCU), housed within the City of London Police, was established to tackle serious and organised intellectual property crime (counterfeit and piracy) affecting physical and digital goods. The unit has only been operational since September 2013 and it is likely that over time the remit of the unit will develop to mirror the evolving threat from intellectual property crime, and it is hoped that this will include cases of theft of commercial data. This should ensure more successful prosecutions of those committing these offences, and therefore serve to provide a stronger deterrent to those tempted to steal the intellectual property of their employer. ●

The Pros and Cons of Staff Monitoring

Pros

- Detects fraudulent activity at an early stage.
- Exposes weaknesses in company systems and security processes.
- Allows an understanding of staff behaviour, for example, being able to recognise changes in activity.
- Promotes an anti-fraud culture – if staff know that they are being monitored, it will act as a deterrent.

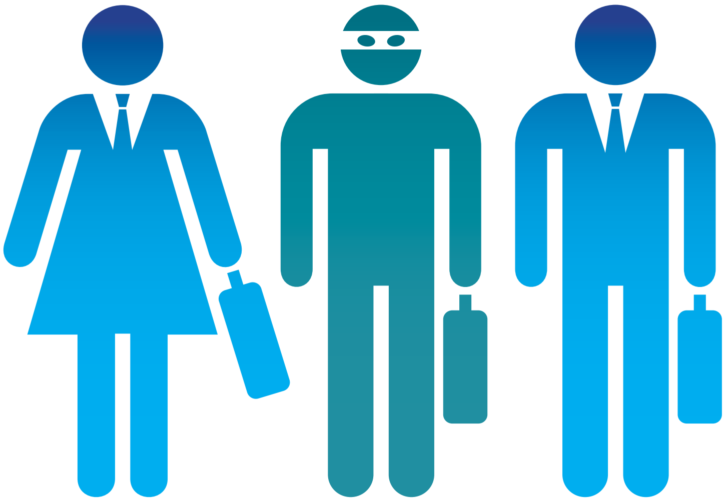
Cons

- Has the potential to create an difficult working environment – perception of 'big brother' style monitoring.
- Could result in a lack of staff loyalty if the employees believe that they're not trusted.
- Could introduce feelings of unfairness if not all staff are subject to the same checks.
- Could force dedicated fraudsters to employ more sophisticated techniques to avoid detection which would fall under the radar of the usual monitoring procedures.

5. Demographics and Employment

The question posed by many individuals and organisations alike is ‘who is the internal fraudster?’ This question is not easy to answer, as there is no particular profile that fits every single one. Each fraudster has different motives and characteristics, often defined by more than just the type of fraud that they commit. This section explores the key information about the fraudsters recorded to the Internal Fraud Database; for example, their age, gender and employment details.

While it may not provide a comprehensive picture of each and every fraudster, certain patterns and similarities can be useful elements in the identification and prevention of internal fraud. By looking back at previous cases, an organisation has the means with which they can identify not just who the fraudsters were (based on their age, gender and employment), but how and why they did what they did. Recognising patterns, weaknesses and opportunities can enable organisations to identify and rectify gaps in their procedures and processes, which (in turn) allows them to be more proactive in the fight against internal fraud. ●



5.1 Age

Average age of internal fraudsters in 2012-2013
Table 5.1.1

	2013		2012	
Fraud Type	Male	Female	Male	Female
Account Fraud	28.3	29.7	29.1	37.3
Dishonest Action by Staff to Obtain a Benefit by Theft or Deception	30.9	34.0	28.4	32.9
Employment Application Fraud (Successful)	32.0	26.7	30.8	30.0
Employment Application Fraud (Unsuccessful)	31.6	32.4	30.8	30.1
Unlawful Obtaining or Disclosure of Commercial Data	32.5	-	25.0	-
Unlawful Obtaining or Disclosure of Personal Data	28.6	35.3	26.3	36.9
Overall Average Age	**30.9**	**32.8**	**29.2**	**32.6**

Based on the frauds recorded in 2013, the average age of the internal fraudster was just under 32 years, a slight increase on the figure of 30 years recorded in 2012. *Table 5.1.1* shows a breakdown of the average ages recorded for each fraud type and gender combination in both 2012 and 2013.

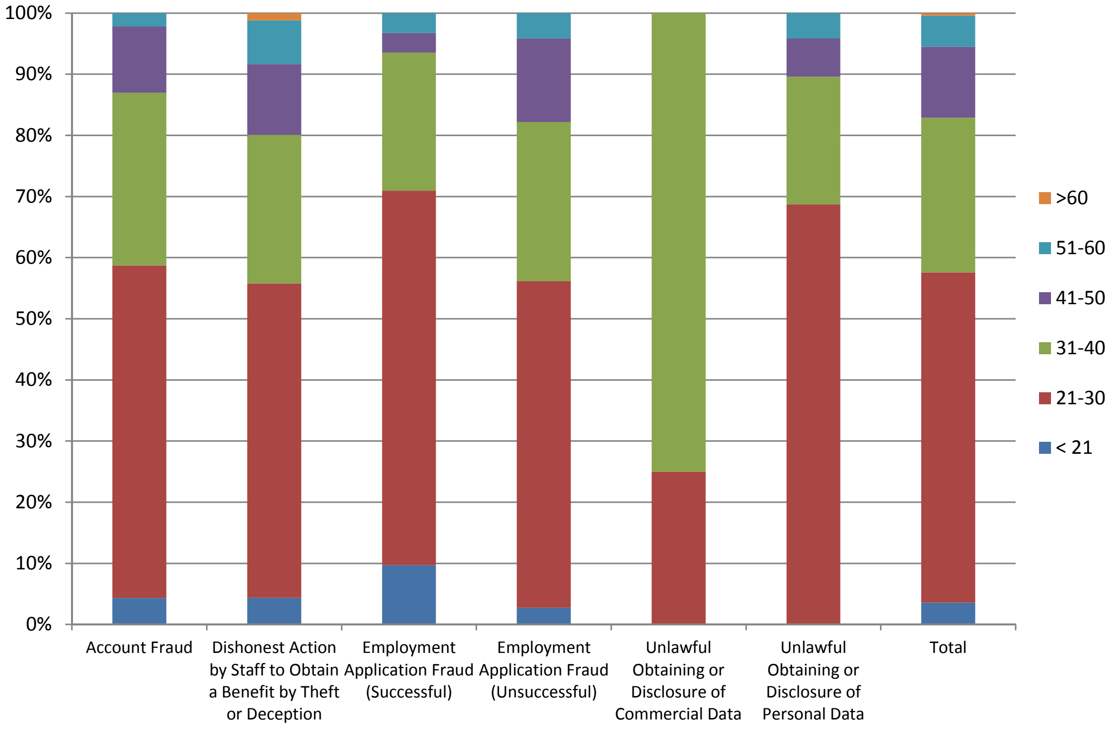
There are many reasons why people commit fraud, but the overall average ages of the individuals involved do not always point towards a demographic that is young and naïve, despite the trends shown under the unlawful disclosure frauds. With the average recorded age of internal fraudsters being in the early thirties, it might be reasonable to assume that a good proportion of these fraudsters were well established in the workforce. As a result, it could be that many of these individuals were trying to maintain a certain standard of living, but circumstances such as pay freezes or wage stagnation, lack of job progression or financial pressures meant that they were struggling to live on their existing salaries, especially those with families to provide for and/or mortgages to pay.

Aside from need, some fraudsters act purely out of greed, and this is not restricted to those on lower salaries. Seemingly successful employees who are progressing well in their careers have also been known to commit internal fraud (often at a greater financial cost to the organisation than, for example, fraud committed by lower level staff members); their belief being that they have the 'authority' or 'entitlement' to do so and that the likelihood of their being caught is somewhat reduced due to their position within the company. Where the fraud prevention efforts of an organisation can often be concentrated on the newly appointed, younger staff (particularly those in 'front line' roles), it would certainly be beneficial for organisations to carry out regular audits of all staff, not just those who are most commonly perceived to be the most likely to commit fraud. Interestingly, in their 2013 *Global Profiles of the Fraudster* report, KPMG identified that the most common fraudster profile was a 34-45 year old individual working in senior management, having been with their organisation in excess of six years. This clearly goes against the perception of internal fraudsters as young, naïve workers and further reinforces the point that fraudsters could be the people within the company whom you least expect. ●

* *Global Profiles of the Fraudster* www.kpmg.com/fraudster

Average age of internal fraudsters across the different fraud types

Figure 5.1.1



5.2 Gender

In 2013, the proportion of female fraudsters recorded to the Internal Fraud Database increased considerably compared with that recorded in 2012.

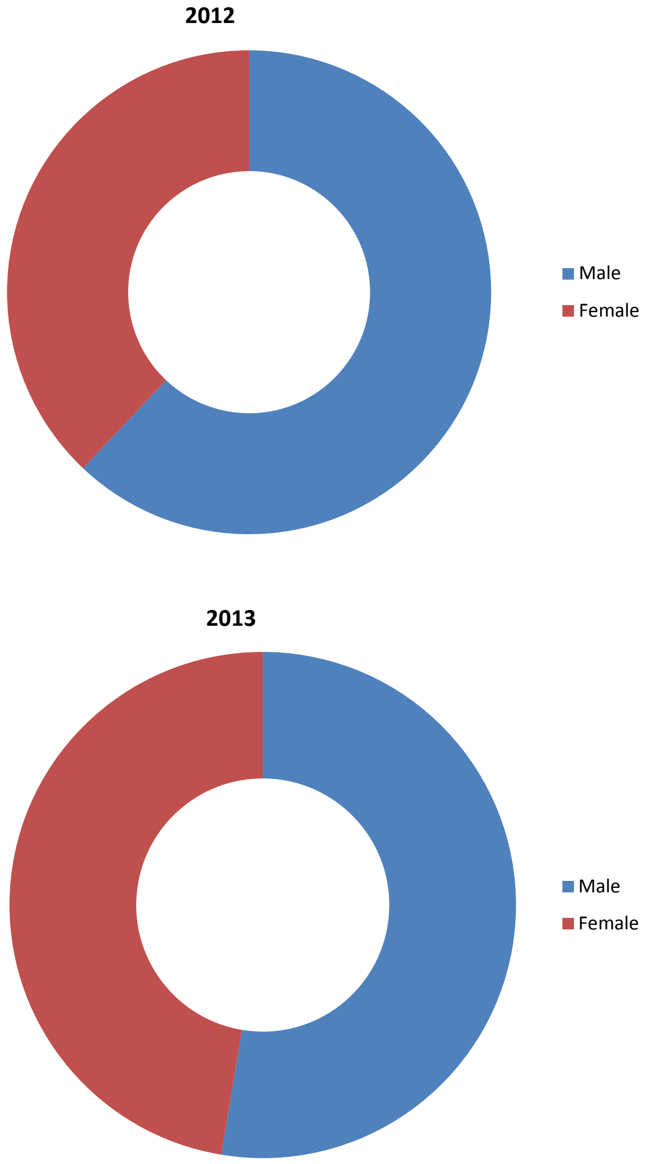
As a percentage of all internal fraudsters, the proportion of females increased from 38% in 2012 to 47% in 2013. It is not clear, however, whether this was the result of an increase in the proportion of females working overall (which would in turn lead to more instances of females committing fraud) or simply a higher level of female criminality.

These increased proportions were particularly noticeable in relation to Account Frauds and Dishonest Actions to Obtain a Benefit by Theft or Deception; but males, on the other hand, still accounted for the greater proportion of Employment Application Frauds and Unlawful Disclosure of Commercial and Personal Data frauds.

In 2013, the proportion of female first party fraudsters recorded to the CIFAS National Fraud Database (consumer fraudsters) was just 26%. So why was there such a discrepancy between the gender breakdown of these fraudsters and the internal fraudsters? One simple explanation could be the higher proportion of female employees working in frontline roles, for example the bank clerk or branch worker dealing with customers and handling cash. This then leads to a higher proportion of female employees carrying out the dishonest actions and Account Frauds purely due to their role within the company and the opportunity they have to commit these frauds. The proportion of males in unlawful disclosure frauds, however, was much greater than the proportion of females, largely due to the higher propensity for males to be involved in crimes with more organised criminals elements (as demonstrated by the unlawful obtaining/disclosure cases recorded to the Internal Fraud Database). This was also highlighted by the majority of National Fraud Database frauds that were carried out by males; females appeared mainly to commit frauds where the temptation was more readily presented, whereas males seemed more prepared to carry out the more sophisticated or organised frauds, for example, the harvesting and selling of data. ●

Proportions of male and female internal fraudsters 2012-13

Figure 5.2.1



5.3 Business Area

There is more to the internal fraudster than merely their age and gender. The type of fraud an internal fraudster commits often depends on what access they have to information and what techniques they use to carry out their crimes. In other words, what opportunities fraudsters have to commit different types of fraud. Staff members in a department with unrestricted access to customer data are clearly going to have different ways and opportunities available to them for perpetrating fraud when compared with someone working in a branch with ready access to cash in a till. *Table 5.3.1* outlines the proportion of internal fraudsters recorded as working in each area of the business, broken down by the fraud type.

In 2013, over 70% of internal fraudsters were working in branches, retail outlets and stores – similar to the proportion recorded the year before. The proportion of staff fraudsters in customer call centres also remained high in 2013, with 20% reported to be working there. This is perhaps unsurprising; given that organisations would

Proportions of fraud taking place in each recorded area in 2012-2013

Table 5.3.1

		Branch/ Retail outlet/Store	Customer contact centre	IT department	Other	Other support services	Staff contact centre
2013	Account Fraud	84.8%	10.9%	-	-	2.2%	2.2%
	Dishonest Action to Obtain a Benefit by Theft or Deception	74.1%	17.5%	0.8%	4.8%	1.6%	1.2%
	Employment Application Fraud (Successful)	33.3%	43.3%	6.7%	13.3%	3.3%	-
	Unlawful Obtaining or Disclosure of Commercial Data	25.0%	50.0%	-	-	25.0%	-
	Unlawful Obtaining or Disclosure of Personal Data	64.6%	27.1%	-	4.2%	-	4.2%
	Total	**70.4%**	**20.0%**	**0.9%**	**5.2%**	**2.0%**	**1.4%**
2012	Account Fraud	92.7%	5.5%	-	1.8%	-	-
	Dishonest Action to Obtain a Benefit by Theft or Deception	69.3%	22.3%	-	4.2%	1.5%	1.9%
	Employment Application Fraud (Successful)	16.7%	20.0%	-	20.0%	40.0%	-
	Unlawful Obtaining or Disclosure of Commercial Data	100.0%	-	-	-	-	-
	Unlawful Obtaining or Disclosure of Personal Data	76.1%	23.9%	-	-	-	-
	Total	**69.5%**	**19.9%**	**-**	**4.5%**	**4.0%**	**1.3%**

In 2012, 0.8% of total internal frauds were recorded as having taken place in the finance department. As there were no cases in 2013, this figure has been ommitted.

have large numbers of employees working in these areas and they would be sure to have access both to account information and personal details, making it simpler for them to perpetrate their fraud.

While this gives an outline impression of the type of employee likely to commit certain types of fraud based on their area of work, this by no means gives the full picture; not least because it does not give any detail about the specific roles that they undertook within that area of the business. It would be easy to assume that all internal fraudsters worked in branch outlets and committed fraud by stealing cash, but fraud perpetrated by senior workers and managers in well-respected roles was also a problem. Many of these fraudsters were abusing their positions of authority within the company in order to facilitate fraud. There were various motivations for these fraudsters; some felt that they were entitled to more money or were in need of cash in order to fund more lavish lifestyles, but a common feature was the element of belief by individuals that they did it simply because they did not think that they would get caught. The single weak link in the chain of events could well have been the lack of appropriate measures taken by an organisation to ensure that these individuals were caught; in other words, adequate monitoring procedures and processes for all levels of staff which could pick up their actions.

Internal controls and audits can go a long way to protect an organisation, but there are many other aspects of internal fraud prevention which can also help. Research has identified that an individual is likely to commit fraud where there is a motivation, an opportunity/target and a lack of a capable guardian. By eliminating one or more of these factors, organisations can limit their exposure to fraud. To reduce a staff member's motivation for committing fraud, an organisation must cultivate a good working environment and constantly assess the staff satisfaction rate in order to measure the likelihood of fraud (e.g. through anonymous surveys). In order to minimise the opportunity, a staff member's activities should be monitored regularly, and appropriately, while setting up controls for areas of the business which may not need to be accessed by all (being careful to ensure that these are not done to the detriment of having a good working environment). Finally, the organisation must instil a robust organisation-wide anti-fraud culture where staff members can be confident both in identifying and reporting suspicious activity. By making cases of internal fraud public, organisations can also create effective deterrents by making staff members fully aware of the seriousness of their fraudulent actions; though some organisations will proceed with particular caution, due to the potential reputational damage that they fear. Furthermore, an increased volume of employees in an organisation will provide a greater level of anonymity for the fraudster in question. ●

Case study:
A senior employee stole over £87,000 from elderly clients

A 37-year-old senior relationship manager siphoned off over £87,000 from two of his elderly clients' accounts over a four month period. He forged the signatures of his clients and made multiple transactions which resulted in the funds being paid into his own accounts. Although on a salary of £50,000, he stole money in order to cover gambling losses, claiming that he spent the money on betting websites in order eventually to 'win' the money back.*

* www.kidderminstershuttle.co.uk/news/10657313.Bank_worker_jailed_after_siphoning___87_3k_from_clients__accounts/

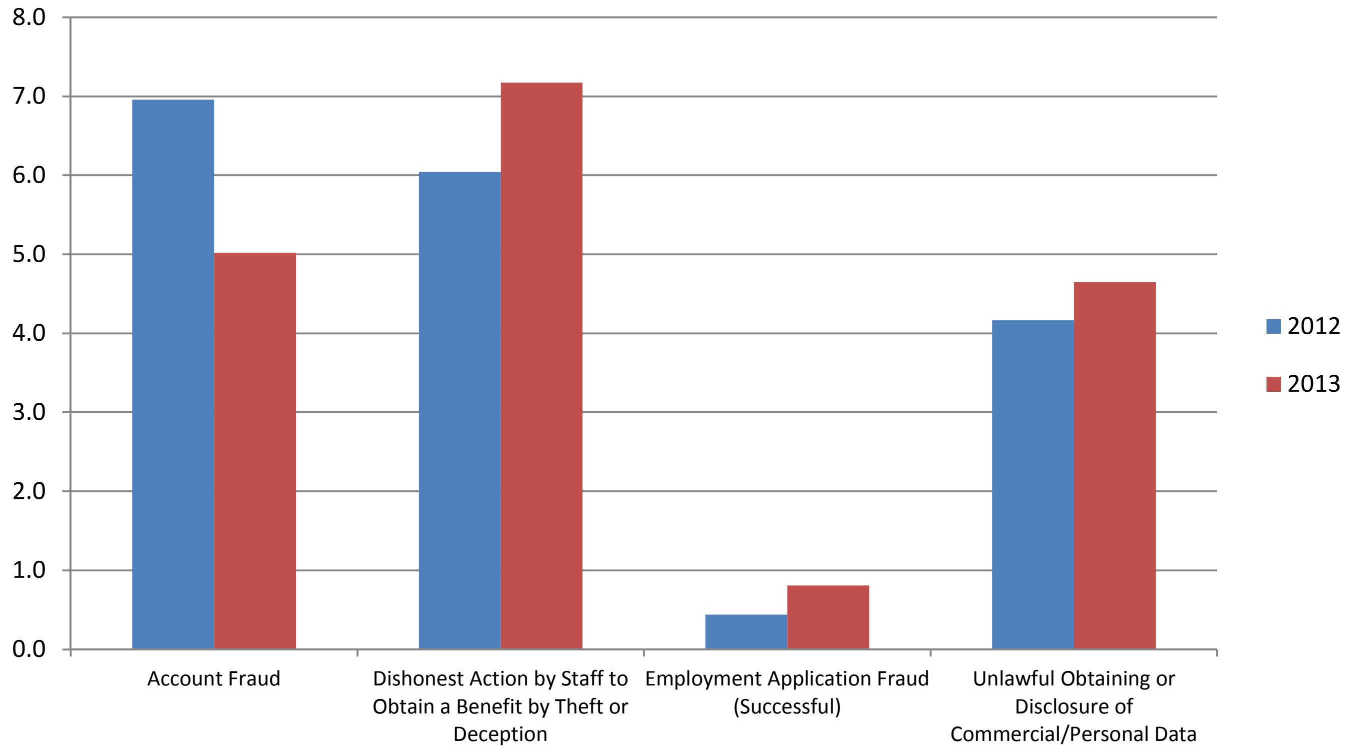
5.4 Length of Service

The length of service of an individual on the Internal Fraud Database indicates how long they were employed with the organisation before they left (either through dismissal, resignation or as a result of their contract ending). In 2013, the overall average length of service increased to 6.5 years, with increases noted across all fraud types except Account Fraud. *Figure 5.4.1* outlines these changes between 2012 and 2013.

One of the most interesting features shown in *Figure 5.4.1* is the change in the average length of service of the fraudsters committing Account Fraud, which reduced from 7 years in 2012 to 5 years in 2013. There are various scenarios that can determine the length of service of an internal fraudster. Sometimes they have been committing the fraud for a long time and the length of service reflects how long it was before they were discovered. In other cases, it will have been committed after a long, lawful employment ended with them being caught for their single offence. Sometimes an individual may commit fraud initially out of 'need' (for example, they may have fallen behind on their bill payments) and, having been successful in their endeavours, they continue to commit the frauds for other, less urgent reasons. There is no way of knowing in all cases what the situation was, but it can be assumed that a substantial proportion of Account Fraudsters had been carrying out their actions for a while before being discovered, mainly due to their slightly more complex and premeditated nature (e.g. facilitating fraudulent account transactions) compared with, for example, the simple theft of cash. The reduction in the length of service of these fraudsters is certainly good news, as a considerable number of these would have been effectively stopped in their tracks, most likely having been discovered by an organisation's internal systems or auditing procedures.

The fraud type with the shortest length of service was, of course, successful Employment Application Fraud. In most cases, the length of service for these frauds will simply have been however long it took for the organisation to

Average length of service for internal fraudsters by fraud type
Figure 5.4.1



complete their employment checks after the individual had been appointed (which subsequently would have uncovered the falsehoods on their application). This aside, the frauds with the next shortest overall average length of service (4.6 years) were those recorded under Unlawful Obtaining or Disclosure of Personal Data. As noted before, this fraud type is often most associated with more organised elements of fraud, particularly relating to the illegal gathering and selling of personal data for use in identity related fraud. When focusing on organised criminals, their length of service within an organisation reflects the balance they need to strike in order to stay long enough to gain trust and understand the company's systems, but at the same time aim to act quickly enough to reduce the chances of being caught and dismissed.

The longest service length of all fraud types, at 7.2 years, was for Dishonest Action by Staff to Obtain a Benefit by Theft or Deception. As always, there is no way of knowing for certain the motives and actions of all of the fraudsters committing these crimes, but it would be safe to say that different types of fraud will often have been perpetrated depending on the opportunities available to the potential fraudster. The efforts of organised fraudsters would be concentrated on yielding greater results (for potentially a greater risk), like for example, the selling of data. By contrast, the more opportunistic or first time fraudsters would be much more likely to be carrying out lower level frauds, such as the theft of cash or the manipulation of an account.

Obviously, the situations behind these fraud types are going to be very different; with at least some individuals carrying out dishonest actions having never originally joined the organisation with that intention. There are circumstances that have the potential to cloud the judgement of these well-established and previously trustworthy employees. These include: a change in personal circumstances, a failure in motivation or loyalty towards the company, pressure/coercion from external organised criminals or simply an increase in the available opportunities for the employee to get their hands on some extra cash. ●

6. Dealing with Internal Fraud

It is important to understand how these internal frauds were identified and how the organisations dealt with them. This section outlines how the frauds were discovered, the reason for the staff member leaving and the details around those reported to the police, particularly those that were taken forward to court.

Of all the frauds recorded in 2013, just fewer than 60% were discovered by the organisations' internal controls, processes and audit procedures, while around 21% were discovered by the customer. This was, in one way, good news for many organisations, as it does show that their continued focus on internal security carried on being effective in combating fraud. Of greater concern, of course, was that 1 in 5 internal frauds were not picked up by the organisation and were brought to the organisation's attention by the customer who was affected by the fraudster's actions. This represented a potentially irrevocable breakdown in the relationship between customer and organisation.

Reporting by staff remains very low

It is worth nothing that the rate of flagging by other staff members remained low in 2013; only 11% of internal frauds were reported by staff (whistleblowing or otherwise), compared with just under 12% in 2012. The reasons for the low rate of identification by other staff members remain unclear. Other staff members could play a bigger role in recognising fraud and reporting suspicions before it becomes too late, preventing situations where the fraudster resigns and moves on (having seemingly 'got away' with their fraud) or before they cause irreparable damage to the organisation's reputation. Employers need to engender a culture where the committing of fraud by staff members is never accepted and as a result, they should work hard to create an environment where employees are capable of and comfortable with identifying and reporting instances of fraud committed by their colleagues (see 'whistleblowing – invaluable reporting mechanism or kiss of death' on page 36).

When the fraudster leaves

In around 63% of cases recorded in 2013, the staff member in question was dismissed following the investigation of the fraud, which was a slight increase on the previous year's figure of 60%. In the remaining cases, 26% of fraudsters chose to resign during the internal investigation, while 10% managed to resign before the fraud was identified. This doesn't necessarily indicate all bad news however. Just because an individual who committed fraud has moved on, it certainly doesn't mean that their criminal activity at the organisation won't ever be detected or investigated. Whether the individual is caught before or after they leave the organisation, reporting to the Internal Fraud Database will ensure that the fraudster is inhibited from moving on to commit fraud further down the line. Additionally, it also gives organisations the opportunity to review their practices and to identify the weaknesses in their systems which allowed the fraud to go undetected. Many occurrences such as this present a learning opportunity for organisations to take advantage of, for the purpose of ensuring that the same situation does not happen again.

Case study: A branch worker steals £127,000 from bank

A 29-year-old female operations specialist stole £127,000 over a period of three years. She carried out over 200 separate transactions on internal bank accounts (not customer accounts) for the purpose of repaying multiple payday loans that she had taken out in order to fund a serious gambling addiction. A mistake made in one of her transactions prompted an internal investigation which subsequently resulted in a jail sentence of two years. *

Legal action

Following an internal investigation, some organisations (or sometimes the customers) choose to report the fraud to the police. In 2013, around a quarter of frauds recorded to the

* www.dailymail.co.uk/news/article-2385311/Former-Barclays-worker-stole-127-000-Birmingham-bank-cover-payday-loans-took-feed-gambling-addiction.html

Whistleblowing – invaluable reporting mechanism or kiss of death?

whis•tle-blow•er
[hwis-uh l-bloh-er, wis-] noun
a person who informs on another or makes public disclosure of corruption or wrongdoing

Whistleblowing broadly falls into two categories: internal and external. Internal whistleblowing would typically involve a member of staff reporting on wrongdoing perpetrated by a colleague through a dedicated company whistleblowing line. External whistleblowing involves reporting outside the organisation to a regulator, government or, in some cases, the media. There would seem to be, though (as shown by the persistently low levels of cases recorded to the Internal Fraud Database that had been reported through whistleblowing), a distinct reluctance for employees to go down the whistleblowing route.

This low level of reporting may well be down to the way in which whistleblowers are perceived and how they get treated. Even though workers who blow the whistle should be protected by the Public Interest Disclosure Act, which states that the worker has the right not to suffer detriment on the grounds that the worker has blown the whistle, there are many cases in the public domain of whistleblowers ending up worse off as a result of having tried to do the right thing. Sharmila Chowdhury was sacked from her position as radiology service manager for Ealing Hospital NHS Trust after raising concerns over moonlighting senior doctors dishonestly claiming thousands of pounds each month. An employment tribunal ordered the Trust to reinstate her on full pay, but this followed months of financial hardship*. Kay Sheldon, who blew the whistle on the failings at Morecambe Bay NHS Trust found her mental health called into question and was threatened with the sack. Whistleblowers have found themselves bullied by colleagues, marginalised at work or finding that they are unable to find re-employment in the sector that they blew the whistle on.

In the light of this perception, it is perhaps not surprising that some employees are unwilling to come forward when they identify wrongdoing. Government has recognised this and is in the process of strengthening the law to protect whistleblowers, including introducing vicarious liability for employers where a worker is subjected to detriment by a co-worker after coming forward. While clearly a step in the right direction, this alone will not change a negative attitude towards whistleblowing – organisations must work to engender a culture where employees are prepared to ‘do the right thing’ at an early stage, thus helping to minimise losses or possibly (in some cases) head off regulatory sanction by putting a stop to illegal actions by their employees.

Internal Fraud Database was reported to the police – the same proportion as the previous year. This figure doesn’t tell the full story, however, as there were actually notable increases in the proportions of certain fraud types that were reported to law enforcement in 2013 compared with 2012. The proportion of Account Frauds reported to the police increased from 42% to 59% and Dishonest Action by Staff to Obtain a Benefit by Theft or Deception increased from 41% to 48%. It’s important that organisations send a message to their staff that they take cases of fraud very seriously and reporting these crimes to the police is a clear signal. Some organisations are still hesitant about reporting their cases to the police for a variety of reasons, however. Many believe that their cases won’t be looked at and that they may not warrant the investment in terms of police time and resource, while others are concerned about reputational damage arising from police involvement. The actual outcomes of the reporting are not necessarily the most important aspects of involving the police, but rather the message it sends as a deterrent. If an employee believes that cases of staff fraud within their organisation never get as far as the police, then they will think that there will be no serious ramifications as a result of their actions, leaving them to think that they can essentially ‘get away’ with the fraud even if discovered.

Reporting the frauds to the police isn’t necessarily the last step. Of all staff frauds identified in 2013, 61 cases were taken to court (an increase from just 39 cases in 2012); meaning that 40% of cases reported to law enforcement were taken further in 2013 (this figure was just 28% in 2012). This increase is a very positive sign and reinforces the message that reporting cases of internal fraud to

* www.independent.co.uk/life-style/health-and-families/health-news/sacked-nhs-whistleblower-vindicated-2023809.html

** www.independent.co.uk/life-style/health-and-families/health-news/exclusive-nhs-watchdog-claimed-that-whistleblower-kay-sheldon-was-mentally-ill-8046640.html the police will be taken seriously and that they will be investigated.

The Need for Transparency

When dealing with serious cases of internal fraud, the way in which an organisation presents the situation to the public can seriously influence the way in which that organisation is viewed. Understandably, some organisations decide to remain quiet about their internal frauds and would rather not speak publicly about them for fear of the 'reputational cost'. While this is impossible to put a figure on, the possibility of continued damage is one that no organisation would wish to contend with. Staying quiet and not 'going public', isn't always the best option, however.

By downplaying an internal fraud case, an organisation risks losing ownership of the situation: with the danger that the news will eventually reach the public domain – with various media giving their interpretation of events. This is one of the reasons why some organisations are choosing to take a different stance by being seen to be open and honest about an internal fraud that happens to them. This gives them the chance to take control of the situation, explaining what happened truthfully and on their terms. Crucially, this also allows organisations to explain how they are addressing the situation.

In order for organisations to cultivate a sense of trust from the marketplace and their customers, it is incredibly important that they are, wherever possible, seen to be both honest and transparent about all aspects of their business. Coming clean with reference to a case of fraud can never be a 'PR exercise'. For many organisations, this is already true for other types of fraud: having to state realistically the threats that they face, and some of the counter measures that they are taking. As noted previously, the same can't always be said for cases of internal fraud. By appreciating what can be gained from being open about internal fraud, organisations can take additional steps to enhance their reputation with their customers and by promoting a zero tolerance internal fraud policy can be seen to 'take ownership' of this issue.

Using Internal Fraud as a Mirror

Understanding insider fraud is a continuing process, and every case dealt with by an organisation brings several opportunities to learn more about the effectiveness of their internal fraud prevention strategy and to improve it. Each case of internal fraud will offer a chance to reflect and examine what the fraud might say about the organisation. Why was the fraud committed? What were the motivations for the fraudster? What internal processes allowed the fraud or failed to prevent it? What were the triggers that meant the fraud went from something simply thought about to a crime committed? These are some of the questions which organisations will have to ask, and the answers (where found) will help to provide a reflection on the culture of the organisation. At the point where the fraud has been discovered, the organisation's first port of call should be to look at any gaps in their security and/or monitoring processes. By reviewing their procedures and identifying weaknesses in them, organisations can aid their understanding of what enabled the staff member to carry out the fraud and most importantly, what extra prevention measures they can implement to protect themselves in future.

It is not just systems and processes that can be reviewed, however. The culture of an organisation should also be a focus. It is important that organisations use their past experiences to recognise when staff members might be facing particular problems or have particular reasons for being unhappy in their work, as this can often be a good way of gauging any potential motivations or triggers that might cause someone to act out of character. A member of staff, for example, might be tempted to commit a fraud out of feelings of resentment against their employer who they believe treats them unfairly (e.g. overlooking them repeatedly for promotion). Furthermore, if the culture of an organisation is seen as unfair, or permissive (e.g. in turning a blind eye to abuses of rules and processes by senior managers) then what kind of impact does this have upon staff? Does it ultimately provide that trigger for an individual to commit fraud? Another feature of internal fraud is that it tends to be committed or discovered after a number of years of service within a company, so identifying exactly what has made the individual carry out the fraudulent actions at that particular point is vital. Learning the reasons and motivations behind actions such as these gives the organisation the knowledge needed to introduce preventative practices such as satisfaction monitoring and counselling, which in turn allows problems to be identified and dealt with before any real damage is done. ●

7. Conclusions

Internal fraud is still a substantial problem for many organisations, as represented by the overall rise in the numbers reported to CIFAS throughout 2013 compared with 2012. While not as prevalent as frauds committed by those who would otherwise be classified as potential or existing customers, the frauds committed by insiders are – fundamentally – not that different, and so any distinction between them should not extend to how organisations view the risk of either type of fraud.

For many, the most serious problems continue to be around data theft and disclosure, because the security of customer data is understandably a priority for all organisations. Not only do such frauds have the potential to cause a huge level of financial damage (enabling identity crimes), but the loss of reputation can be just as damaging, if not more so. On a lesser scale, the number of Employment Application Frauds recorded in 2013 also increased considerably, possibly because organisations were facing a higher number of relevant material falsehoods on applications than ever before. Crucially, over the past few years, more effort has been made to identify and investigate these frauds, not just by fraud investigation departments, but most importantly, by employers' HR departments.

This has certainly had an impact on the number of cases recorded to the database and has had positive effects with regard to the implementation of robust fraud prevention measures within organisations. At a time where competition for jobs is at a peak, candidates are increasingly hiding adverse information in order to make themselves appear more suitable for the position but obviously either do not care about, or are unaware of, the consequences or the seriousness of their actions. It is certainly encouraging that 90% of these fraudulent applications were identified by organisations prior to an offer of employment being made and were, as a result, unsuccessful. If a candidate makes fraudulent declarations on an application, then it will call into question the integrity of the individual and has implications about whether the employer would then choose to hire them.

Turning to Account Frauds and dishonest actions, these actually reduced in 2013 compared with 2012, but this definitely did not mean that the problem had in any way been solved or eradicated. Worryingly, there were reports from CIFAS Members detailing the work of organised criminals who place individuals within organisations for the purpose of establishing them over time as trustworthy and decent employees, only to exploit their more advanced position within the company much further down the line. The full extent of these organised practices remains to be seen and employers should be exceptionally vigilant against this type of activity.

There is, unfortunately, no single measure or 'magic fix' to prevent internal fraud. A good combination of measures needs to be implemented by multiple areas of the company which ensure the most comprehensive protection. With thousands of individuals working within all areas of organisations, it certainly wouldn't be realistic to say that all internal frauds can be identified and completely eradicated. Organisations are, however, continuing to work hard to reduce their exposure to internal fraud and to minimise the risk.

In the first instance, organisations should ensure that their vetting procedures are comprehensive and that where possible, all checks are carried out before the prospective employees are appointed. Some organisations that have implemented robust vetting procedures have discovered that potential fraudsters were actually deterred by the thoroughness of the checks and were likely to withdraw their applications because of this. Genuine applicants, on the other hand, expect such checks and, as a general rule, remain unperturbed by the process.

It isn't always possible to detect a potential staff fraudster at recruitment stage, however. Secondary measures that organisations have worked hard to implement include the more robust internal security precautions, controls and processes for monitoring the activities of their staff members throughout the duration of their employment. With around 60% of the internal frauds reported to CIFAS in 2013 having been identified by such controls, this clearly shows the effectiveness of the procedures and just how much an organisation can gain from implementing them across the board – at all levels of seniority. With the overall average length of service of an internal fraudster having been around 6.5 years, the importance of continual monitoring is key to identifying fraudulent activity committed both by new and established employees.

There are, however, other actions that companies could take in order to minimise internal fraud, without the need for introducing new technologies or processes for this purpose. A third effective measure would be the engendering of a strong anti-fraud culture, through which organisations would commit to clear policies that emphasised a zero tolerance stance, with all staff members having been trained in identifying fraudulent activity to the point that they would be comfortable in reporting it, should the need arise. With only 11% of internal frauds having been discovered by staff, this is clearly still an area where many organisations can improve. Whistleblowing, in some instances is still seen as uncomfortably detrimental to the whistleblower. Resolution of this issue is becoming ever more important because, where internal fraudsters manage to bypass controls and remain under the radar of monitoring processes, their colleagues are one of the most (if not the only) effective weapons an organisation has in uncovering the crimes.

Finally, there are further efforts that an organisation can make beyond the usual fraud prevention measures detailed above. By creating a culture where staff are happy in their work and feel a sense of loyalty to their employer, the organisation can reduce feelings which often lead to them being targeted. If front line employees are suffering pay freezes and a lack of job progression while senior executives are enjoying substantial pay increases and bonuses, it therefore follows that those front line employees are more likely to feel undervalued and disillusioned, increasing the risk of them being tempted to commit fraud (both to obtain the money which they feel they are entitled to, but also in retaliation against the culture of unfairness in their workplace). From a fraud prevention perspective, there is a lot that an employer can gain by improving the overall working environment and by constantly monitoring the satisfaction and wellbeing of staff (e.g. staff surveys), which in turn would ensure that the intrinsic levels of staff morale remained high within all levels of the organisation.

It is apparent that internal fraud remains a major issue. What has changed, however, is the recognition that it is no longer viable for organisations to ignore this. By speaking out and sharing information, organisations can more successfully tackle the problem, which in turn not only aids them in the identification of fraud, but it also supports their anti-fraud culture and messages. Furthermore, it is encouraging to see that data sharing to prevent internal fraud is growing. This is demonstrated both by the increase in organisations participating in the sharing of data and by the increases in the number of cases recorded on the Internal Fraud Database. It is vital that organisations recognise the benefits of fraud data sharing in order to continue the good work already done in the effective identification and prevention of internal fraud. ●

For further information, please contact our Research and Communications Teams

press@cifas.org.uk
internal.fraud@cifas.org.uk

CIFAS
The UK's Fraud Prevention Service

CIFAS – The UK's Fraud Prevention Service
6th Floor, Lynton House
7-12 Tavistock Square
London
WC1H 9LT

www.cifas.org.uk

CIFAS - A company limited by Guarantee. Registered in England and Wales No.2584687 at
6th Floor, Lynton House, 7-12 Tavistock Square, London WC1H 9LT