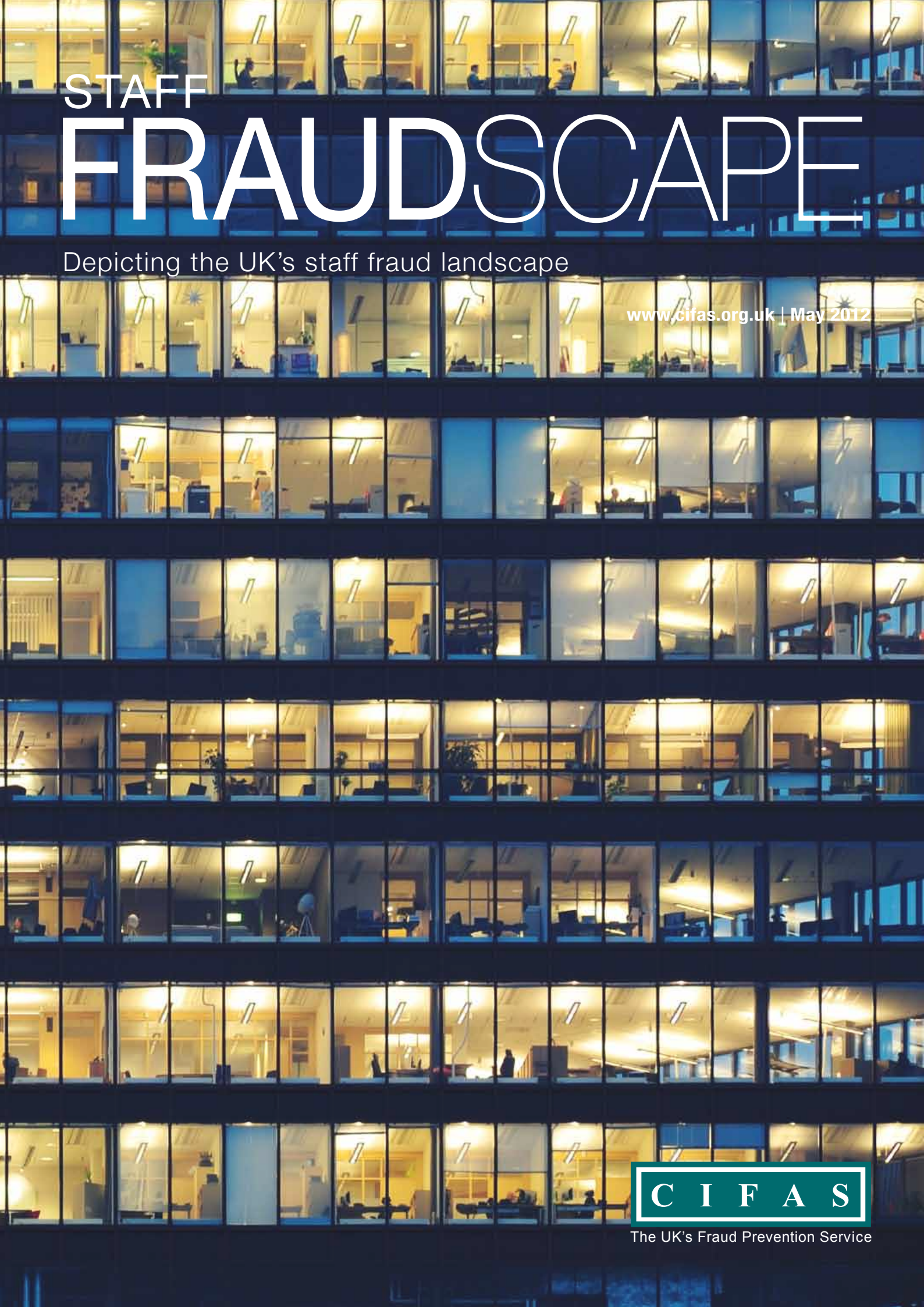


# STAFF FRAUDSCAPE

Depicting the UK's staff fraud landscape

www.cifas.org.uk | May 2012

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. Since February 1991 CIFAS has been an independent Company Limited by Guarantee. CIFAS Members are drawn primarily from the UK financial services industry, but also from telecommunications, insurance, recruitment, other business sectors and 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

CIFAS is the UK's Fraud Prevention Service, a not-for-profit membership organisation operating in the public interest and dedicated to the prevention of financial crime. It has 260 Member organisations spread across various business sectors. These include financial services, retail, telecommunications, customer service centres, call centres and public services. CIFAS operates two data sharing databases for its Members – who share information about frauds in the fight to prevent further fraud.

CIFAS launched its Staff Fraud Database in 2006. Research indicated that dishonest staff move freely between employers and, for most organisations, unknowingly recruiting a fraudster represents a risk too far. The CIFAS Staff Fraud Database, therefore, is a way for organisations to counter this threat. Participating organisations access the database for the purposes of filing data about their confirmed staff fraud cases and double checking potential employees against records of proven staff fraud cases filed by other CIFAS Staff Fraud Members. By the end of 2011, 79 CIFAS Staff Fraud Members covering 217 organisations participated in this data sharing scheme. CIFAS Staff Fraud Members are drawn from the UK financial services industry, but also from telecommunications, insurance, recruitment and other business sectors. In order to be recorded on the CIFAS Staff Fraud Database a case must satisfy a standard of proof. This means that there must be sufficient evidence to take the case to the police, although it is not mandatory to do so.

## In this Report

*Staff Fraudscape* examines and assesses the staff fraud cases identified by CIFAS Member organisations during previous years and 2011, to ascertain any key differences between the typology of the frauds seen.

The Report examines the staff frauds in terms of the overall numbers, types of fraud committed, demographics of the fraudsters identified and the means by which organisations were able to detect the fraud. Research into the Report has included close liaison with CIFAS Staff Fraud Members, other industry bodies, and the police in order to delve into the explanations behind the patterns identified and the *modus operandi* of fraudsters.

Numerous illustrations of the frauds identified by CIFAS Staff Fraud Members have also been interspersed throughout the Report; providing real life examples of the types of fraud that have been attempted and perpetrated by individuals.

An accompanying survey was sent to key fraud prevention and HR professionals in CIFAS Member organisations in the first quarter of 2012, which presented the overarching trends identified and asked respondents to give their insight into the factors that might explain the figures and the possible ramifications of these trends. Findings from this survey have fed into *Staff Fraudscape*; helping to offer further explanations for the fraud patterns identified. The key findings from this survey are set out in an appendix at the end of this Report.

# 1. Executive Summary

In 2011, CIFAS Members reported 378 frauds committed by staff inside an organisation: a 14.5% increase from 2010 and a stark contrast to the static levels of the previous two years, where no annual increase was recorded.

With staff fraud largely underestimated, under-detected and under-reported, the Staff Fraud Database is helping to resolve this issue; providing CIFAS Members with an effective means by which to counter it. Fraud committed by insiders undermines the reputation and management of an organisation, and no sector (whether private, public or third sector) will be immune to the consequences.

## Rising levels indicate dangers and obligations for organisations

The 14.5% increase in staff fraud seen in 2011 demonstrates that CIFAS Members are increasingly aware of, and looking out for, fraud committed by insiders. This surge in levels, however, also confirms the prevalence of the threat. While most individuals would hesitate to commit fraud against their employer, for any organisation to assume that it is immune from staff fraud is dangerous.

The most pronounced threat to a company appears to be 'Dishonest Actions by staff to obtain benefits by theft or deception'. Not only is this type of fraud the most commonly committed, but it also saw the biggest increase in 2011: 41% up from the level recorded in 2010. Counter fraud professionals have also highlighted it as the biggest threat to their organisation in future years. This type of fraud is (at least to some extent) a by-product of the challenging economic and employment climate of the UK. With purse-strings tighter than in previous years, more individuals are driven to steal from their employer or to manipulate systems such as incentive schemes in order to obtain funds. While the financial difficulties of staff may be deserving of sympathy, the risk that such hardship might lead to fraud only serves to confirm the need for organisations to review their internal controls and support mechanisms for staff who may feel that circumstances are getting the better of them.

## A more malignant threat

The links between serious organised crime and staff fraud have long been known and have previously been illustrated by CIFAS. This report, and the survey of counter fraud professionals that has helped to inform it, highlight many of the threats posed by such third party involvement. From attempting to 'plant' insiders, through to criminals targeting staff and using coercion in order to get hold of customer data, the problems posed by organised criminals are daunting. The stealing of personal data, in particular, is of grave concern. While the numbers have decreased by 25% from those recorded in 2010, the explosion in identity crime and data driven frauds (such as identity theft and account takeover frauds) must be seen as a part of the picture. If data is being stolen, it is only reasonable to expect that it will be used at some point. Therefore, the ramifications of data theft can never be overestimated.

## Fighting fraud – what must organisations do?

While the state of the economy is beyond the control of an individual organisation, this report reveals a number of areas for attention in terms of preventing and detecting staff fraud. For example, while internal controls (e.g. monitoring and the adequate vetting of staff) is the most common means of discovering a fraud (44% of all cases in 2011) the customer spotting an alteration to an account or the theft of money is equally important (31% of cases in 2011). This means that more can and needs to be done in order to put increased controls in place that will prevent a fraudster from committing a fraud before the customer notices it. The rarity of whistleblowing procedures being used in the workplace (only 3%), however, perhaps underlines some cultural questions that must equally be addressed in order to prevent frauds before they occur.

The idea that fraud might have been carried out by a trusted employee, peer, colleague and friend is uncomfortable and can be devastating. Unfortunately, many organisations who do not participate in the Staff Fraud Database remain more willing to acknowledge the risk of fraud from potential customers. This means that internal fraudsters are more likely to go undetected, and unchallenged when caught. Willingness to report such cases to the police is present in organisations, but the recognition of the conflicting priorities faced by the police often proves to be a barrier to this. The problem of identifying and preventing staff fraudsters, therefore, remains a challenge. It was to resolve this problem that the CIFAS Staff Fraud Database was established.

# 2. CIFAS Staff Fraud Database

## 2.1 An Overview

*Table 2.1.1* shows the number of cases recorded by CIFAS Staff Fraud Members over the last three years.

**Number of Staff Fraud cases recorded 2009-2011**
*Table 2.1.1*

| | 2009 | 2010 | 2011 |
|---|---|---|---|
| Staff Fraud cases recorded | 330 | 330 | 378 |
| **% change** | **-** | **-** | **+14.5%** |

After stable levels from 2009 to 2010, the number of cases increased markedly in 2011. While a number of new organisations joined the Staff Fraud Database during 2011, these new Members are ***not*** the driver behind the increase in identified cases of Staff Fraud. There has been a general increase in cases identified and recorded by Members who joined prior to 2011.

This both concerns and reassures. It is of concern that in testing times in the employment market, there are those who are prepared to commit fraud against their employer; risking their jobs and their future employment prospects. It is reassuring, however, that organisations are able to identify these instances of staff fraud, and are recording the details to the Staff Fraud Database in order to prevent the same person targeting other organisations.

While the figures may seem slight in comparison with those from the CIFAS National Fraud Database[1], there are numerous factors to remember:

1. With reference to the motivation of the fraudster, it must be remembered that while some people will have few qualms about attempting fraud when applying for a product or service, attempting to defraud their employer or prospective employer is something that they would never contemplate doing. The standard of proof required to create a record on the Staff Fraud Database, means that the figures are proved cases of fraud and not suspicions.
2. In cases of staff fraud, frequently an individual will only commit one instance of staff fraud. In terms of the frauds recorded onto the National Fraud Database, it is not unusual for numerous frauds to be committed by the same person.
3. With reference to the motivation of the fraudster, it must be remembered that while some people will have few qualms about attempting fraud when applying for a product or service, attempting to defraud their employer or prospective employer is something that they would never contemplate doing.

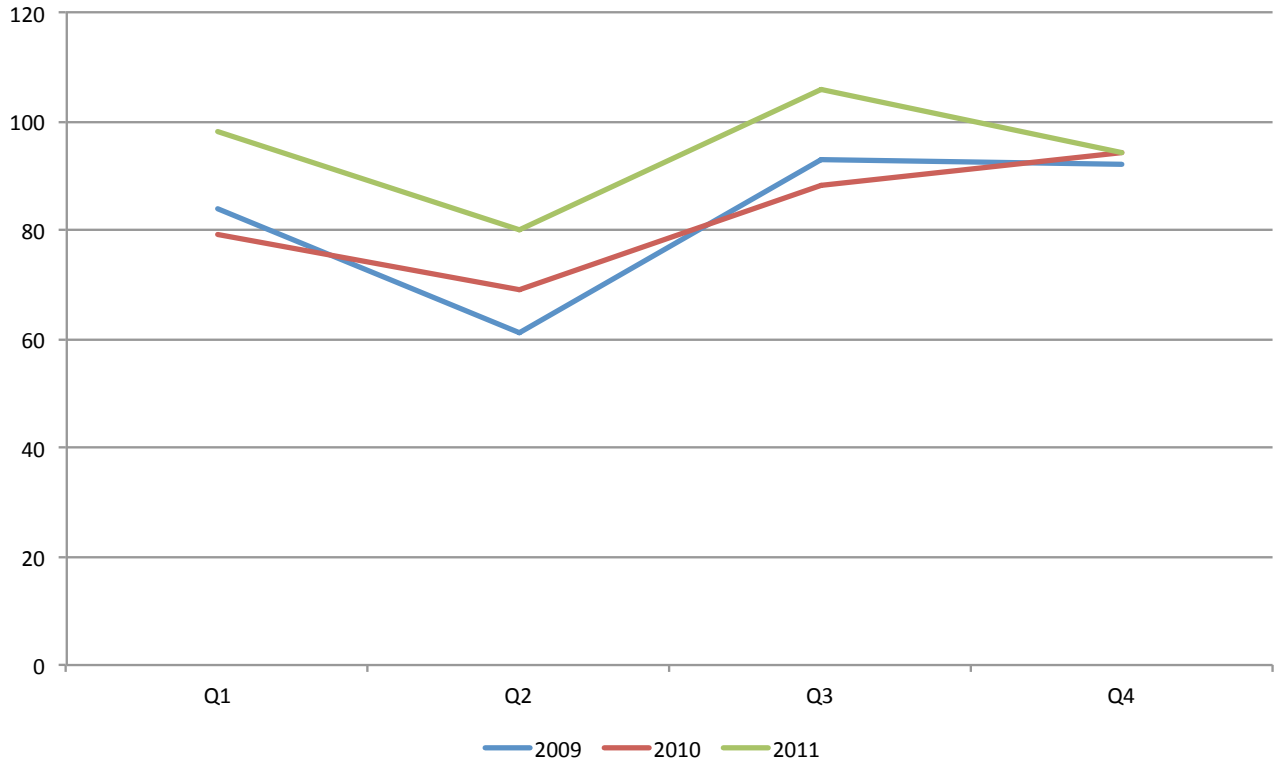
*Figure 2.1.1* (overleaf) shows the number of staff fraud cases identified in each quarter of 2009, 2010 and 2011. This shows that over the last three years, the distribution of cases over the four quarters has been remarkably similar. The first quarter has seen relatively high numbers of cases recorded, followed by: a dip in numbers in the second quarter of the year, a peak in the third quarter and (in two years) a slight decline in the fourth. This implies that there is an element of seasonality as to when instances of internal fraud are recorded (although not necessarily when they occur).

Following the survey of CIFAS Staff Fraud Members, 46% of respondents believed that the drop seen in the second quarter of each of the last three years could partially be explained by a 'Christmas hangover'. Higher levels of staff fraud in the first quarter could be attributed to overspending at Christmas, with the second quarter seeing a pendulum reaction caused by the increased attention organisations pay in reaction to the spike seen in the first quarter. ●

[1] www.cifas.org.uk/fraudscape_marchtwelve

**Staff Fraud cases recorded by quarter in 2009-2011**

*Figure 2.1.1*



## 2.2 Staff Fraud by Fraud Type

When frauds are recorded by CIFAS Members, they are categorised according to the nature of the fraud identified. Each case can consist of one or more fraud types and, therefore, can be counted in more than one category (which explains why the figures here may add up to a different total from the number of staff frauds noted in Chapter 2.1). *Table 2.2.1* presents the numbers and types of fraud case recorded in 2010 and 2011, and the differences between the two years.

Dishonest Actions by staff to obtain a benefit by theft or deception continues to be by far the most common type of insider fraud, and this has increased by over 40% in 2011 compared with the previous year. Many of these offences are carried out by more 'junior' staff (at least in terms of age – see Chapter 4.2), who are taking advantage of an opportunity that comes their way: for example, by seizing an opportunity to pocket some cash when it is deposited in a bank branch by a customer. In 2011, theft of cash from elderly customers was one of the most common frauds experienced by CIFAS Staff Fraud Members.

Other staff fraud offences did not see the same level of increase in 2011. There were more people who committed Employment Application Fraud successfully (the fraud only being identified after they had been appointed) which is a matter of concern, even though the number of cases involved was relatively low. The implications of this are that some organisations are still willing to give individuals access to their premises and systems without first completing all vetting checks, and/or that the preliminary checks that are carried out can be bypassed by a fraudster.

More encouraging, however, is the reduction in the number of cases of staff members being found to be disclosing personal information to third parties. Given the proliferation of personal data being used to commit identity related crimes (over 115,000 cases identified by CIFAS Members in 2011), it is heartening to see that this method of obtaining personal information seems to have been largely closed down by organisations. Increased data security protocols, (for example, using technical solutions to identify suspicious activity by employees with access to personal data), and a zero tolerance approach, have made data compromise by insiders a less attractive option. Such measures have also made it a less productive method of obtaining large quantities of personal data with which to commit identity related crimes. As a result, the unauthorised obtaining or disclosure of personal data has decreased by a quarter since 2010. •

**Staff Fraud cases recorded in 2010 and 2011 by Fraud Type**
*Table 2.2.1*

| Fraud Type | 2010 | 2011 | % change |
|---|---|---|---|
| Account Fraud | 40 | 43 | +7.5% |
| Dishonest Actions by Staff to Obtain a Benefit by Theft or Deception | 156 | 220 | +41.0% |
| Employment Application Fraud Successful | 14 | 18 | +28.6% |
| Employment Application Fraud Unsuccessful | 91 | 83 | -8.8% |
| Unlawful Obtaining or Disclosure of Commercial Data | 1 | 1 | 0.0% |
| Unlawful Obtaining or Disclosure of Personal Data | 52 | 39 | -25.0% |

# 2.3 Staff Fraud by Business Sector

**Staff Fraud cases recorded in 2010 and 2011 by business sector**
*Table 2.3.1*

| Business Sector | 2010 | 2011 | % change |
|---|---|---|---|
| Banking Services | 242 | 291 | +20.2% |
| Plastic Cards | 10 | 19 | +90.0% |
| Call Centre | 15 | 16 | +6.7% |
| Insurance Services | 58 | 40 | -31.0% |
| Other Financial Services | 4 | 6 | +50.0% |
| Other | 1 | 7 | +600.0% |

The organisations participating in the Staff Fraud Database have been divided into business sector groups to enable a more meaningful assessment of the staff frauds identified in 2010 and 2011. *Table 2.3.1* shows the number of cases of staff frauds recorded by organisations in different sectors.

Evidently, in both 2010 and 2011, the sector that identified the most cases of staff fraud was banking. This is unsurprising for a number of reasons:

- One of the original drivers behind the creation of the Staff Fraud Database was to stop organised criminal gangs placing insiders in banks and having these 'plants' move on to the next bank when their criminal connections were identified. This means that a lot of the founder Members of the Staff Fraud Database are, indeed, the providers of banking services.
- These organisations have staff in positions where they are well placed to perpetrate staff fraud – handling cash, for example, and it follows that some are more likely to succumb to temptation.
- The providers of banking services are among the largest employers participating in the Staff Fraud Database scheme. Put simply, the more employees, the greater the likelihood of having a rogue element within the workforce.

It is also worth noting that call centres frequently provide a workforce to the financial services industry (although the staff are employed by, and working for, the call centre) and so there is some potential crossover in terms of the sectors affected by the frauds. The 'Other' sector covers a broad spectrum of organisations, but those who have been identifying and recording the frauds are predominantly recruitment specialists.

All sectors have seen a proportionate increase in the number of cases of staff fraud identified, with the exception of the providers of insurance services. This is the second largest sector in Staff Fraud membership, but the number of cases identified decreased by 31%. Due to the heightened attention directed towards anti bribery and corruption in insurance services in 2010, the Financial Services Authority highlighted numerous concerns in their report: *Anti bribery and corruption in insurance broking: reducing the risk of illicit payments or inducements to third parties* [2]. This report recommended several new best practices for implementation (including in staff recruitment and vetting) which would, if implemented, reduce the risk of staff fraud in the insurance services sector. The reduction in insurance frauds recorded may well be a direct result of these measures.

[2] www.fsa.gov.uk/pubs/anti_bribery.pdf

>

The proportion of cases that each sector accounted for in 2010 and 2011 can be seen in *Figures 2.3.1* and *2.3.2*. The total frauds identified by the providers of banking services increased to over 75% of the total number identified, while the proportion of cases that the insurance sector accounted for decreased from 18% to 11%. The other sectors remained broadly the same; although the number of frauds recorded by these groups was comparatively low.

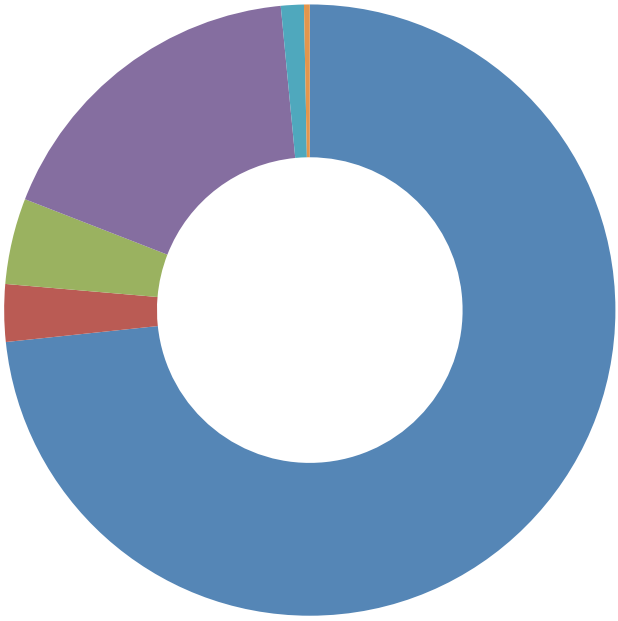
In 2011, joint research carried out by CIFAS and Serious Organised Crime Agency (SOCA) showed that serious organised criminals were infiltrating legitimate organisations deliberately to commit fraud. Initial research identified that, out of 911 employees who had been dismissed for fraud and appeared on the CIFAS Staff Fraud Database, about one tenth (94 people) had the potential to be involved in serious organised crime.

Of these 94 'high risk' fraudsters:

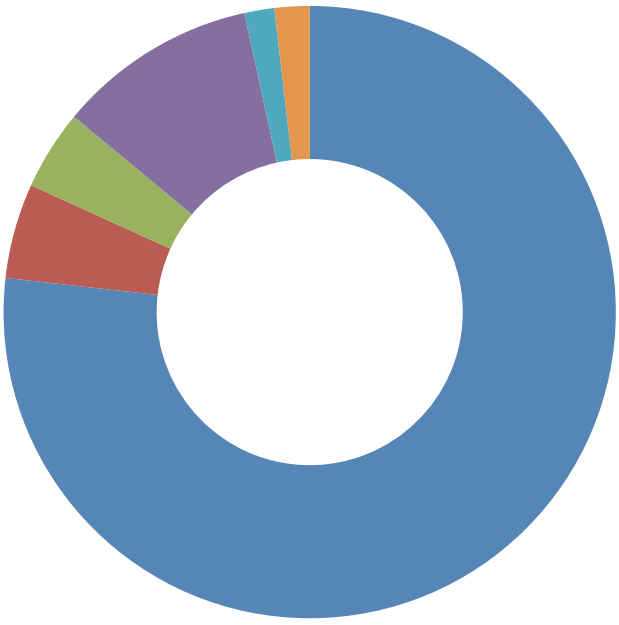
- 10 were confirmed as involved in serious organised crime.
- A further 31 were considered likely to be involved in serious organised crime.

The figures indicated that 4.5% of those filed on the CIFAS Staff Fraud Database were assessed as being involved in, or likely to be involved in, serious organised crime.[3]

**Staff Fraud cases by business sector in 2010**
*Figure 2.3.1*



**Staff Fraud cases by business sector in 2011**
*Figure 2.3.2*




[3] www.cifas.org.uk/organised_crime_sevennovember

# 3. Staff Fraud by Fraud Type

This section sets out further details of the types of fraud recorded to the Staff Fraud Database. Each fraud can be recorded under more than one Fraud Type and for a variety of reasons (called 'Reasons for filing'). These provide a greater insight into the nature of the frauds perpetrated in 2011. Tables in this section present the most common reasons for filing each Staff Fraud Type and, therefore, figures in these tables differ from the totals presented in Chapter 1 and the percentage totals in this chapter will not always add up to 100%.

## 3.1 Account Fraud

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

**Real examples:**

- A member of staff working in a call centre accesses a customer account without authority. He does this by using a colleague's login details and then transfers funds from this customer's account to his personal bank account.
- A member of staff working in a high street bank accesses the account of a vulnerable customer (who is known to lose his or her credit and debit cards). The fraudster enters details to the bank's computer system to say that the customer had ordered a new card and reported a change of address. The new address was the staff member's mother's home address to which he sends the new debit card. After issuing the instruction to send the debit card to the new address, the staff member then changes the customer's address back to the original address. The staff member picks up the debit card from his mother's house and goes to a local cash machine to withdraw cash.

There were 40 cases of Account Fraud in 2010, which increased to 43 in 2011 – an increase of 7.5%. *Figure 3.1.1* (page 11) illustrates the incidence of these cases over the two years.

*Table 3.1.1* below shows that the most common reason for recording an Account Fraud case to the Staff Fraud Database continued to be the fraudulent withdrawal from an account. This is where the staff fraudster withdraws funds from a customer account without the customer's knowledge or authority. The number of these cases increased by 19% in 2011 compared with 2010 – although it does need to be borne in mind that this increase, although sizeable in percentage terms, actually only

**Reasons for Filing Staff Fraud cases in 2010 and 2011**

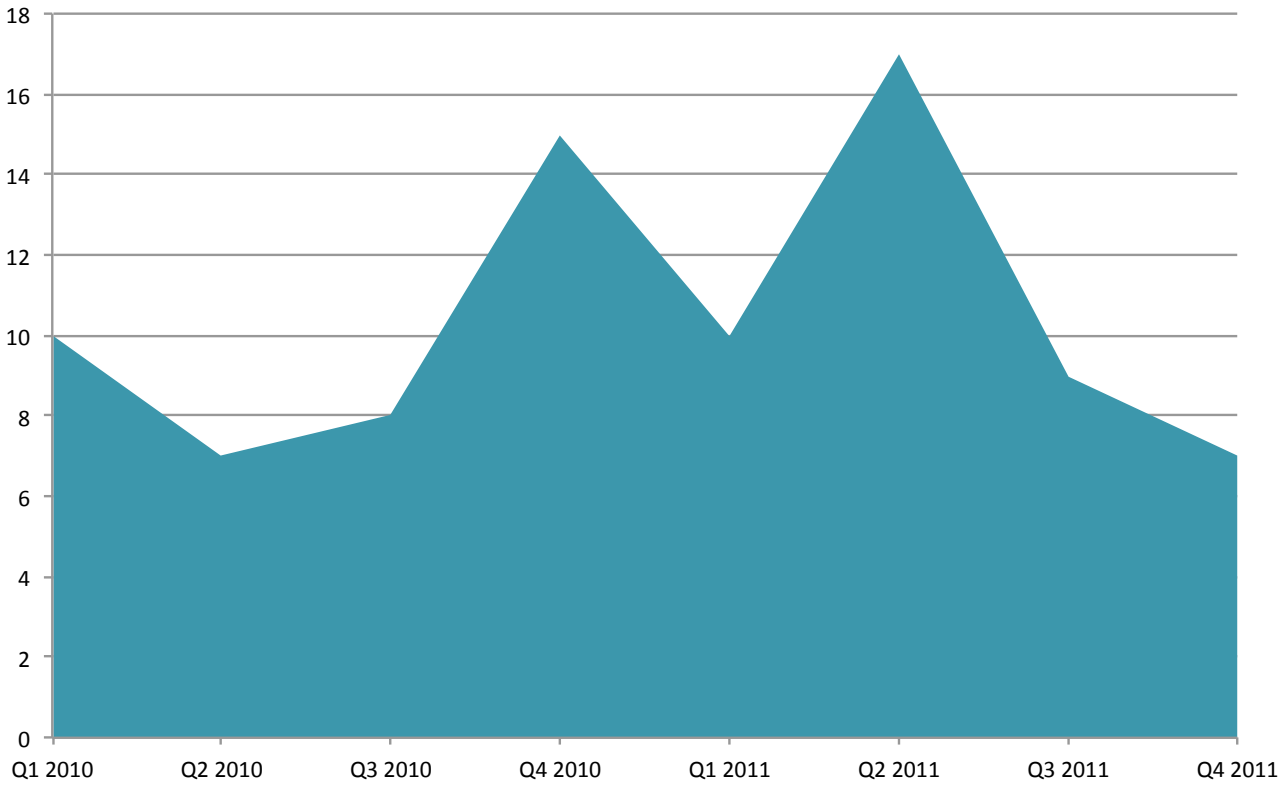
*Table 3.1.1*

| | 2010 | | 2011 | | |
|---|---|---|---|---|---|
| **Reasons for Filing** | **Cases** | **% of Total** | **Cases** | **% of Total** | **% change** |
| Fraudulent account withdrawal | 21 | 52.5% | 25 | 58.1% | +19.0% |
| Fraudulent account transfer to employee account | 7 | 17.5% | 13 | 30.2% | +85.7% |
| Fraudulent account transfer to third party account | 20 | 50.0% | 11 | 25.6% | -45.0% |

>

**Account Frauds recorded on the Staff Fraud Database 2010-2011**

*Figure 3.1.1*




represents an extra four cases. The other area of increase related to cases where the staff member moved funds from their victim's account into their own, up to 13 such cases from only seven in 2010.

The rise in these types of fraud (where the obvious implication is that they are being carried out purely for personal gain) is in many ways only to be expected in the current tight financial climate. People who find that their money is not going as far as they want, or need, may well be more inclined to resort to stealing from an account as a way of supplementing their income. It is most likely that these individuals hope that the account holders would fail to notice the missing funds, and so the crime would go undetected. There is also anecdotal evidence from Staff Fraud Members that some individuals have been targeting the accounts of the elderly, or those whom the fraudster might consider to be more 'vulnerable', to reduce the chance of discovery. Counterbalancing this desire for financial gain, though, will be the knowledge that unemployment and competition for jobs are increasing. This means that someone who is feeling the pinch and might contemplate stealing money from a customer's account, may think twice; as the consequences of getting caught would extend beyond simply being fired. The possibility of criminal charges is a real one, of course, and such actions might also result in being unable to obtain further employment – compounding the original problem.

This risk of being caught, however, is not solely down to the possibility of the victim spotting the missing funds. While fraudsters may attempt to reduce the risk of being caught by selecting customers who they judge to be less likely to notice, they are likely to be increasingly concerned about the chances of being found out by an organisation's internal controls. The tightening of internal controls and audits built into an organisation's systems and processes is borne out by the increase in the number of staff that have been identified as a result of them.

While the most common route for the identification of the offender continues to be the customer (unsurprising as it is their money that is being stolen), *Table 3.1.2* overleaf shows that the proportion of cases identified as a result of internal controls or audit increased from 17.5% in 2010 to almost 43% in 2011.

>

**Proportion of Account Frauds and the means of discovery 2010-2011**
*Table 3.1.2*

| | 2010 | | 2011 | | |
|---|---|---|---|---|---|
| **Means of Discovery** | **Cases** | **% of Total** | **Cases** | **% of Total** | **% change** |
| Customer | 23 | 57.5% | 23 | 53.5% | 0.0% |
| Internal controls/audit | 7 | 17.5% | 18 | 41.9% | +157.1% |
| Law enforcement | 1 | 2.5% | 0 | 0.0% | -100.0% |
| Other | 3 | 7.5% | 1 | 2.3% | -66.7% |
| Staff | 5 | 12.5% | 1 | 2.3% | -80.0% |
| Staff (whistleblowing) | 1 | 2.5% | 0 | 0.0% | -100.0% |

## When it is not strictly for personal use

*Table 3.1.1* also shows that there were fewer instances of staff members being identified as transferring money to a third party account in 2011 compared with 2010: with 11 cases recorded, down from 20 the previous year. It is, of course, too early to state whether this is a definite pattern or merely a symptom of what happened in 2011 – so the reasons for this reduction cannot be stated categorically. What can be said, however, is that this may indicate that organised criminals are looking for different routes to obtain and divert funds. Some cases where funds were transferred into third party accounts will have been as a result of 'incentives' offered by the recipient third parties, which suggests that the reduction in these cases being identified could be as a result of fewer such incentives being offered. Staff Fraud Members, as part of their investigations, often cite that the third party is an associate: for example, a family member or a friend.

Unsurprisingly, these Account Frauds have mostly been identified by the banking services sector. They hold accounts from which funds can be transferred or withdrawn, so it is entirely logical that they will be identifying and recording these cases. Banking services accounted for over 88% of these cases in 2011, with the remaining cases perpetrated by employees working in call centres and in providers of other financial services. •

## 3.2 Dishonest Actions by Staff to Obtain a Benefit by Theft or Deception

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

**Real examples:**

- An employee processed credit card applications for customers who had not applied. He did this by forging signatures on the application forms. The employee did this to exceed targets in order to gain a bonus.
- A member of staff submitted expenses that he or she knew were completely false.
- When processing a sale, a retail cashier took the customer's vouchers as payment, increased the vouchers' value when entering details on the cash till, and then stole the cash difference.

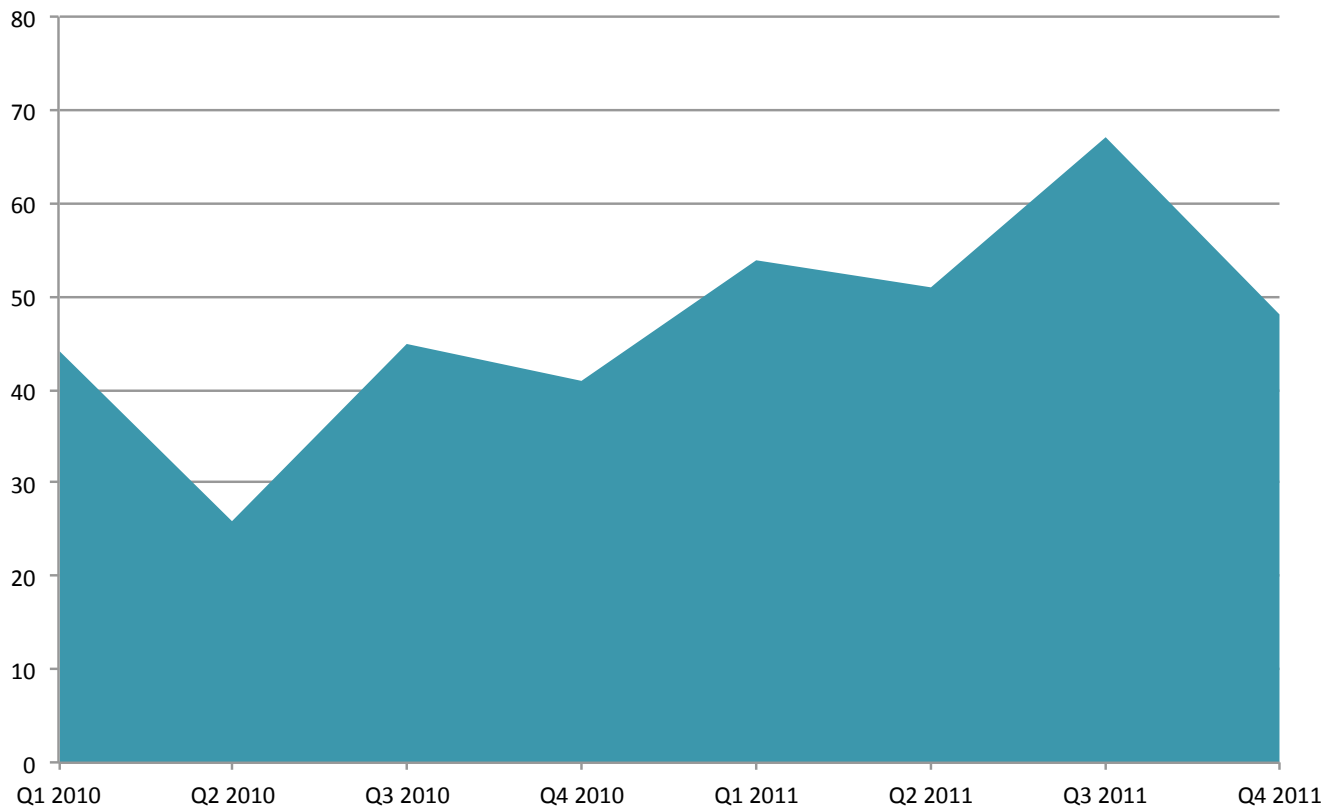
There were 220 recorded cases of staff perpetrating Dishonest Actions in 2011, compared with 156 in 2010: an increase of 41%. The number of cases of this type recorded for each quarter of 2010 and 2011 can be seen in *Figure 3.2.1* below.

The most common reasons for recording these frauds are shown in *Table 3.2.1* overleaf, and it can be seen that the theft of cash from customers continues to top the list. This is where, for example, a cashier steals cash deposited by a customer over the counter, as opposed to withdrawing it electronically from an account. This is not surprising

>

**Cases of Dishonest Actions recorded in 2010 and 2011 by quarter**

*Figure 3.2.1*



**Reasons for Filing Dishonest Action Frauds in 2010 and 2011**
*Table 3.2.1*

| | 2010 | | 2011 | | |
|---|---|---|---|---|---|
| **Reasons for Filing** | **Cases** | **% of Total** | **Cases** | **% of Total** | **% change** |
| Theft of cash from customer | 55 | 35.3% | 68 | 30.9% | +23.6% |
| Theft of cash from employer | 39 | 25.0% | 50 | 22.7% | +28.2% |
| Manipulation of a third party account | 14 | 9.0% | 25 | 11.4% | +78.6% |
| Facilitating transaction fraud | 15 | 9.6% | 19 | 8.6% | +26.7% |
| Facilitating fraudulent applications | 16 | 10.3% | 18 | 8.2% | +12.5% |
| Manipulation of personal account | 7 | 4.5% | 18 | 8.2% | +157.1% |

because, as with Account Fraud, in economically unforgiving times, temptation will be too great for some members of staff. However, CIFAS Members have also reported that the theft of cash is increasingly linked to gambling. These motivations also apply in the second most common reason for filing: cases where money has been stolen from the employer. An example would include cases where a manager is responsible for cashing up the tills at the end of a working day, but falsifies the balance in order to steal cash to fund a gambling habit.

While these two offences have increased in number in 2011 compared with 2010, it is worth noting that the proportion of these two offences has actually decreased – and that there was a broader spread of offences committed by dishonest members of staff in 2011.

## Further layers of manipulation

The manipulation of third party accounts increased both in number and proportion in 2011. This covers such actions as changing overdraft limits, interest rates or other material details on the account, like the address. Anecdotally, Staff Fraud Members' investigations have revealed that some cases were the result of the staff member 'altruistically' trying to help out struggling family or friends, such as changing details on an account in order to assist the account holder financially. Equally, other cases have revealed that the staff fraudster was paid to perform this service by the account holder. Of most concern, however, is the presence of organised criminality. Some of these cases are the result of the member of staff being paid by organised criminals to change details on a victim's account (allowing the criminal to take control of it). Examples include changing the delivery address for cards and statements or the security questions on accounts. In such cases, the actions of the staff member are obviously to the detriment of the account holder, as opposed to the manipulations of overdraft limits (for example) which would benefit the account holder.

The next most common Dishonest Action, facilitating transaction fraud, is also detrimental to the account holder, and often at the request of organised criminals: smoothing the way for someone else to take funds from an innocent party. This is where the employee knowingly accepts false identity documents to support fraudulent transactions and the processing of transactions on stolen/counterfeit cards or altered instruments. In addition to the obvious problems this will cause the victims attempting to recover these funds, it also has the potential to cause the organisations severe reputational damage. The customer will be angered that an organisation they trusted with their money employs someone who is prepared to help others to steal it from them. The organisation not only risks the loss of that individual's business, but also that of those whom they tell about their experience; not to mention the potential for damaging publicity. The organisation can, of course, go some way to mitigate this risk by making the experience of the victim as pain-free as possible when it comes to recovering those funds.

Furthermore, to reduce the risk of facilitating transaction fraud, organisations could not only educate their staff on fraud awareness but also their customers. In particular, organisations should emphasise what the customer can do if they lose their identity documents. This fraud involves staff colluding with other fraudsters, so organisations should look for early warning signs. The Fraud Advisory Panel has produced a fact sheet listing behavioural, financial and procedural early warning signs, which should

>

help organisations with early staff fraud prevention [4]. Colleagues of staff fraudsters should also be comfortable and confident in reporting their suspicions either to their line manager or through whistleblowing channels.

## Helping other fraudsters in

Like the theft of cash offences, the facilitation of fraudulent applications (where the fraudster helps fraudulent applications to succeed) is another type of case which has increased in number while accounting for a lower percentage of cases in 2011 than it did in 2010. This is another area where the member of staff may be carrying out the fraud on behalf of family or friends (either with or without financial inducement) or they may be carrying this out on behalf of an organised criminal element. The applications that the staff member is smoothing the way for may well be in an entirely fictitious name, or indeed in the name of an innocent victim of impersonation; meaning that the potential links between the levels of identity fraud and this type of insider fraud cannot be overestimated. With the derisory sentences given to insider fraudsters for offences that involved identity fraud, organised criminals will continue to find the infiltration of organisations (and collusion with staff) an attractive way to generate funds for further criminality.

## Where it is happening

Unsurprisingly, as with Account Fraud, many of these cases have been identified and recorded by the banking sector. Over 50% of these Dishonest Actions cases involved the theft of cash, either from the customer or from the employer. Banking branches have to provide access to money, which in turn provides an opportunity and temptation to steal. The banking services sector accounts for over 80% of all the Dishonest Actions identified.

Although the number of cases is relatively small, the cards sector identified a greater proportion of Dishonest Actions in 2011 than in 2010; while the insurance sector identified fewer. The increase in cases identified by the cards sector is reflected in the increase in the proportion that involved the manipulation of accounts. The decrease identified by the insurance sector is reflected in a reduction in the number of cases where the member of staff manipulates the details on an insurance proposal. The latter often involved brokers, who earned commission, changing the details supplied by the customer (possibly without their knowledge) in order to receive a lower quote, and therefore to make the customer more likely to go with that company and earn the broker his or her commission. As stated earlier, the Financial Services Authority has done much to raise awareness of anti bribery and corruption, and this may explain the decrease in insurance services identifying manipulation of accounts.

Unsurprisingly, 40% of the respondents to our Staff Fraud survey thought that their organisation was most at risk from Dishonest Actions by staff to obtain a benefit by theft or deception. Similarly, over 40% of the respondents thought that Dishonest Actions by staff would increase the most in 2012. •

[4] www.fraudadvisorypanel.org/pdf_show_170.pdf

# 3.3 Successful Employment Application Fraud

**Definition: 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.**

**Real example:**

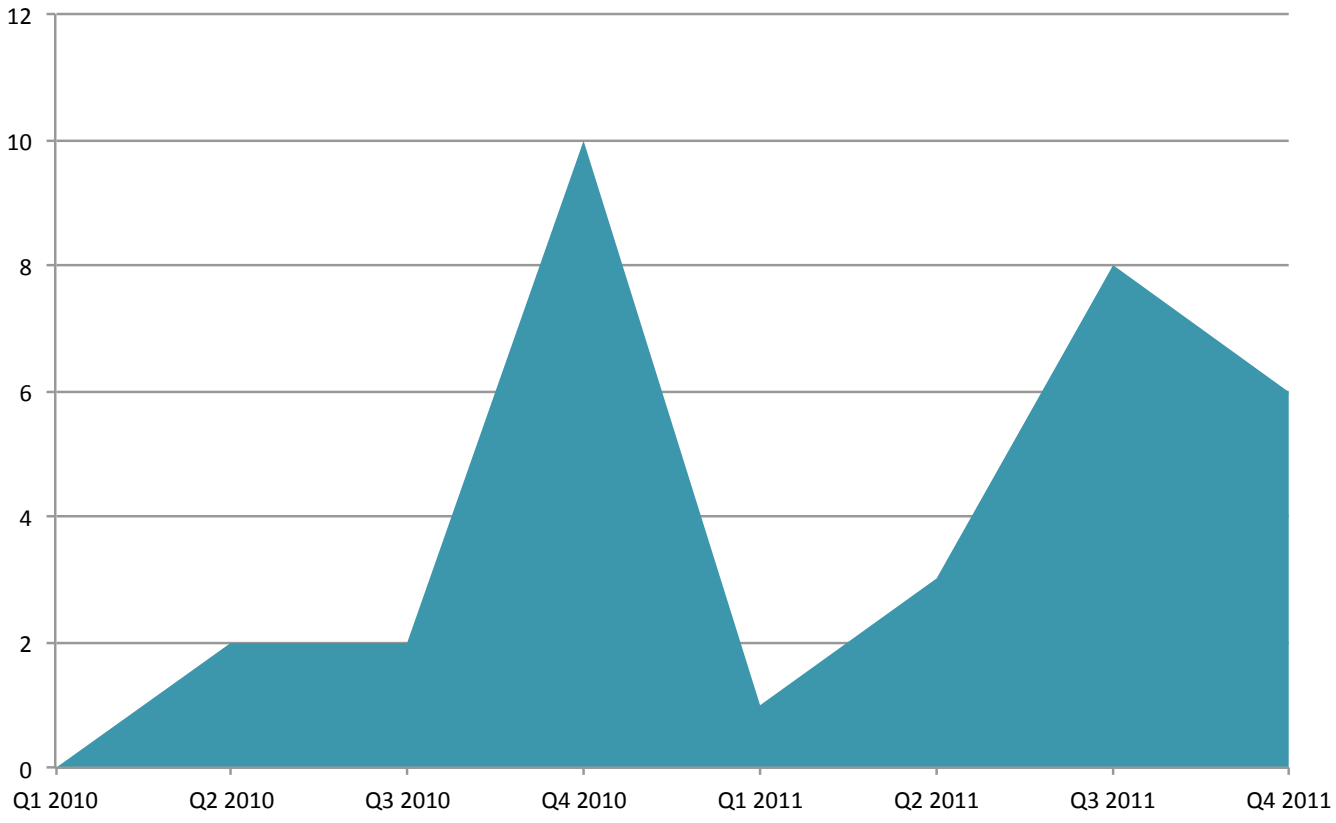
- An individual applies for a management position at a company which requires a minimum of an upper second class degree and MBA. In his application, the individual declared that he had a first class degree and MBA qualification. Following a successful interview, the individual was appointed, subject to checks. While in post, the individual was asked to provide all qualification documents, only for the employer then to identify these documents as counterfeits purchased from a diploma mill/fake degree website. Furthermore, the employer had made checks with the University and Business Schools declared by the applicant and confirmed that the individual had neither received any qualification nor attended those courses.

To be considered material, a falsehood would, or did, affect a decision to offer a post to an applicant.

There were 18 cases of successful fraudulent applications for employment recorded in 2011, compared with 14 in 2010: an increase of 29%. The number of cases of this type recorded in each quarter of 2010 and 2011 can be seen in *Figure 3.3.1* below.

**Cases of Successful Employment Application Fraud recorded in 2010 and 2011 by quarter**

*Figure 3.3.1*



**Reasons for Filing Successful Employment Application Frauds in 2010 and 2011**
*Table 3.3.1*

| | 2010 | | 2011 | | |
|---|---|---|---|---|---|
| **Reasons for Filing** | **Cases** | **% of Total** | **Cases** | **% of Total** | **% change** |
| Concealed employment history | 8 | 57.1% | 7 | 38.9% | -12.5% |
| Concealed employment record | 3 | 21.4% | 6 | 33.3% | +100.0% |
| Concealed unspent criminal convictions | 2 | 14.3% | 6 | 33.3% | +200.0% |
| Concealed adverse credit history | 0 | 0.0% | 1 | 5.6% | - |
| False references | 0 | 0.0% | 1 | 5.6% | - |

It is heartening that the numbers of these types of fraud, where applicants have successfully committed fraud in their applications for employment, remain at relatively low levels: accounting for just 18% of all Employment Application Frauds recorded in 2011.

The most common reason for recording such frauds was the concealment of employment history. This occurs when an applicant has falsely represented the dates when he or she was employed in a previous role. This would normally be carried out to disguise a period where the applicant had been unemployed, in the belief that this would have made him or her look like a less viable candidate. The second most common reason was concealing the employment record; e.g. falsely declaring that he or she had resigned from a previous employer when they had actually been dismissed. These are not mutually exclusive, however, and in a few cases both have been used; with the time at a previous employer manipulated to hide time in different employment that had been terminated.

## The minefield of previous convictions

Of greater concern, however, is the increase in the number of cases of concealed unspent criminal convictions. Any positive 'spin' that can be spun by the discovery of these frauds, however, can only be undermined by the fact that discovery was only *after* these people had commenced employment. While it is positive that these cases were subsequently discovered, it cannot be ignored that these people were able to start in post without the unspent convictions being known to the employer. Given the short period of time between employment starting and the fraud being discovered, the likeliest explanation is that they were allowed to start before the results of Criminal Records Bureau checks were known, and that when the results were returned this led to the swift termination of the employment. The concern, however, will always be around the damage that the individual might be in a position to cause during this short window of opportunity. While an unspent criminal conviction is not symptomatic of any intention to defraud (he or she may have had every intention of being an honest employee, merely considering themselves unemployable with an unspent conviction), access to cash and customer accounts or data is most likely not something that any employer would wish to give to those with unspent convictions.

The ramifications of an organisation allowing somebody to start working (without having completed all vetting checks) are of course financial and reputational in the first place. There will be, however, the additional costs of investigations, and then refilling the position through another recruitment process as well as any potential training. This means that it should be considered best practice, in all cases, for organisations to complete all vetting checks before the successful applicant starts in post.

## Do lies always mean fraud?

The current economic circumstances will be having an impact on the number of Employment Application Frauds that are recorded. On one hand, there are fewer jobs for the currently high number of unemployed to apply for, thus limiting the opportunities for Employment Application Frauds to be committed. Conversely, given the high degree of competition for available jobs, it is likely that the number of frauds within the applications that an organisation receives will be higher.

It is, however, worth remembering that there are – undoubtedly – a number of successful Employment Application Frauds that have been (as yet) completely unidentified. In addition, there will be many cases where an applicant lied as part of the application process purely

>

in order to gain employment and make an honest living: not with any intention of committing fraud. For example, where an individual exaggerates his or her qualifications even though it is not necessary to have any qualifications for the job that he or she is applying for.

Where organisations have failed to check details, and the employee has subsequently done nothing to arouse any suspicion, then it is possible that the employee may well work within that organisation without his or her history of fraud ever coming to light. This is something that can never be fully countered, and is – therefore – more a question for human resources and risk professionals to consider, regarding each organisation's stance on the operational and ethical ramifications. •

## 3.4 Unsuccessful Employment Application Fraud

**Definition: 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.**

**Real example:**

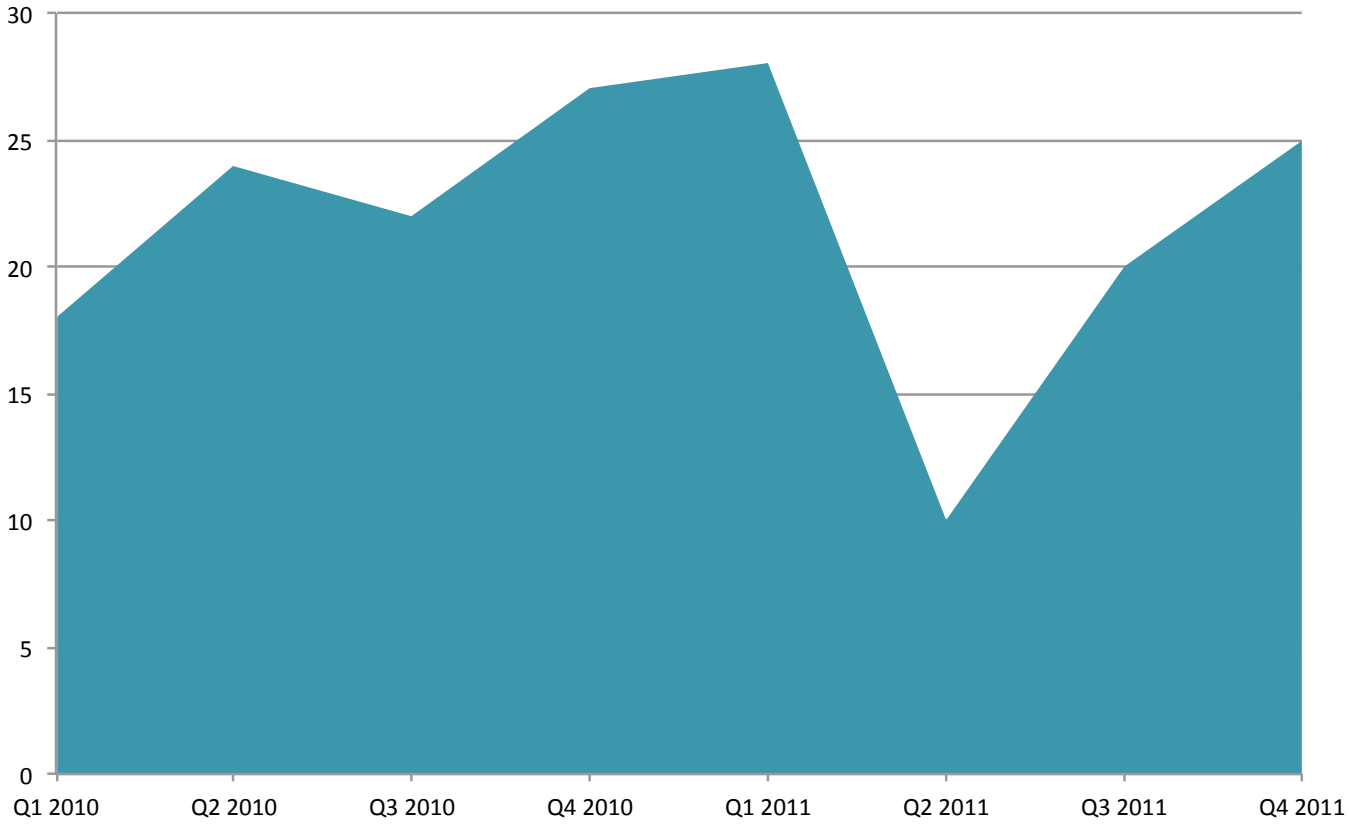
- An applicant applied for a position, declaring that he or she has no unspent criminal convictions. Before the potential employer hires the applicant, they carry out a Criminal Records Bureau check and identified that he or she has an unspent criminal conviction for theft.

The number of Unsuccessful Employment Application Frauds decreased in 2011; with 83 being recorded compared with 91 in 2010. This is a drop of 9%. The number of cases of this type recorded in each quarter of 2010 and 2011 can be seen in *Figure 3.4.1* below.

It can be seen from *Figure 3.4.1* that the second quarter of 2011 saw a dramatic drop in the number of cases identified. This is in keeping with the general decline in cases recorded in the second quarter.

**Cases of Unsuccessful Employment Application Fraud recorded in 2010 and 2011 by quarter**

*Figure 3.4.1*



**Reasons for Filing Unsuccessful Employment Application Frauds in 2010 and 2011**
*Table 3.4.1*

| | 2010 | | 2011 | | |
|---|---|---|---|---|---|
| **Reasons for Filing** | **Cases** | **% of Total** | **Cases** | **% of Total** | **% change** |
| Concealed adverse credit history | 32 | 35.2% | 48 | 57.8% | +50.0% |
| Concealed employment record | 23 | 25.3% | 21 | 25.3% | -8.7% |
| Concealed employment history | 22 | 24.2% | 10 | 12.0% | -54.5% |
| Concealed unspent criminal convictions | 20 | 22.0% | 9 | 10.8% | -55.0% |
| False documents | 4 | 4.4% | 4 | 4.8% | 0.0% |
| False references | 3 | 3.3% | 2 | 2.4% | -33.3% |
| Use of a false identity | 0 | 0.0% | 2 | 2.4% | - |
| Concealed spent criminal convictions | 2 | 2.2% | 1 | 1.2% | -50.0% |

On the face of it, a drop in the number of people identified as having attempted to commit a job application fraud to increase their chances of obtaining employment (in a time when unemployment has increased) is surprising. It must be borne in mind, however, that it is difficult to commit a job application fraud in a climate where jobs are scarce. When there are few jobs on offer, it follows that there are fewer opportunities to identify those who are dishonest in their application – although it would be expected that the number of fraudulent applications for each available position would increase.

## Concealing Adverse Credit History

What is not surprising is that there has been a 50% increase in the number of people who have tried to conceal an adverse credit history. As times get tighter, and redundancies and unemployment rise, so does the number of people unable to make ends meet and service their debts. Furthermore, more Staff Fraud Members are carrying out pre-employment credit checks. With that comes the increased likelihood of more people accruing adverse credit information against their names. These people will be attempting to get themselves on a more secure financial footing by obtaining new employment – but competition for jobs is high and they fear that the adverse credit information they have acquired will make them less viable candidates. This results in a failure to disclose such information when asked to do so (something that is often forgotten is the requirement to have a clean financial and credit history in certain roles within the financial services sector). Unfortunately for the candidate, the information is easy for companies to verify, and the lack of disclosure then makes them guilty of attempting to defraud the company to which they are applying. The very fact that these details are so easy to check means that few of these attempts will ever result in a successful Employment Application Fraud.

## A curious contrast

As noted previously (Chapter 3.3) an area for concern is that while the most common successful Employment Application Frauds (on the whole) increased, the instances where these actions and/or material falsehoods were identified prior to employment being granted decreased. There were fewer cases recorded where a concealed employment history, employment record or unspent criminal conviction were identified prior to the applicant starting in post. This suggests that, in 2011, these checks of references and the Criminal Records Bureau were more often still outstanding when the applicant started; exposing the employer to the associated risks of employing unvetted staff in potentially sensitive positions.

There were two instances of false identities being used to apply for employment in 2011. Although the numbers are low, they are an indication that these were attempts by criminals to place their contacts with employers in order to facilitate further fraud – otherwise why would it be necessary to disguise the applicants' true identities? Obviously, as the fraud was discovered before employment started, it is impossible to state categorically what the fraudsters' motives either were or were not. It might range from an illegal immigrant applying using a false identity, with every intention of working honestly, through to a convicted criminal seeking to escape past records. •

## 3.5 Unlawful Obtaining or Disclosure of Commercial/Personal Data

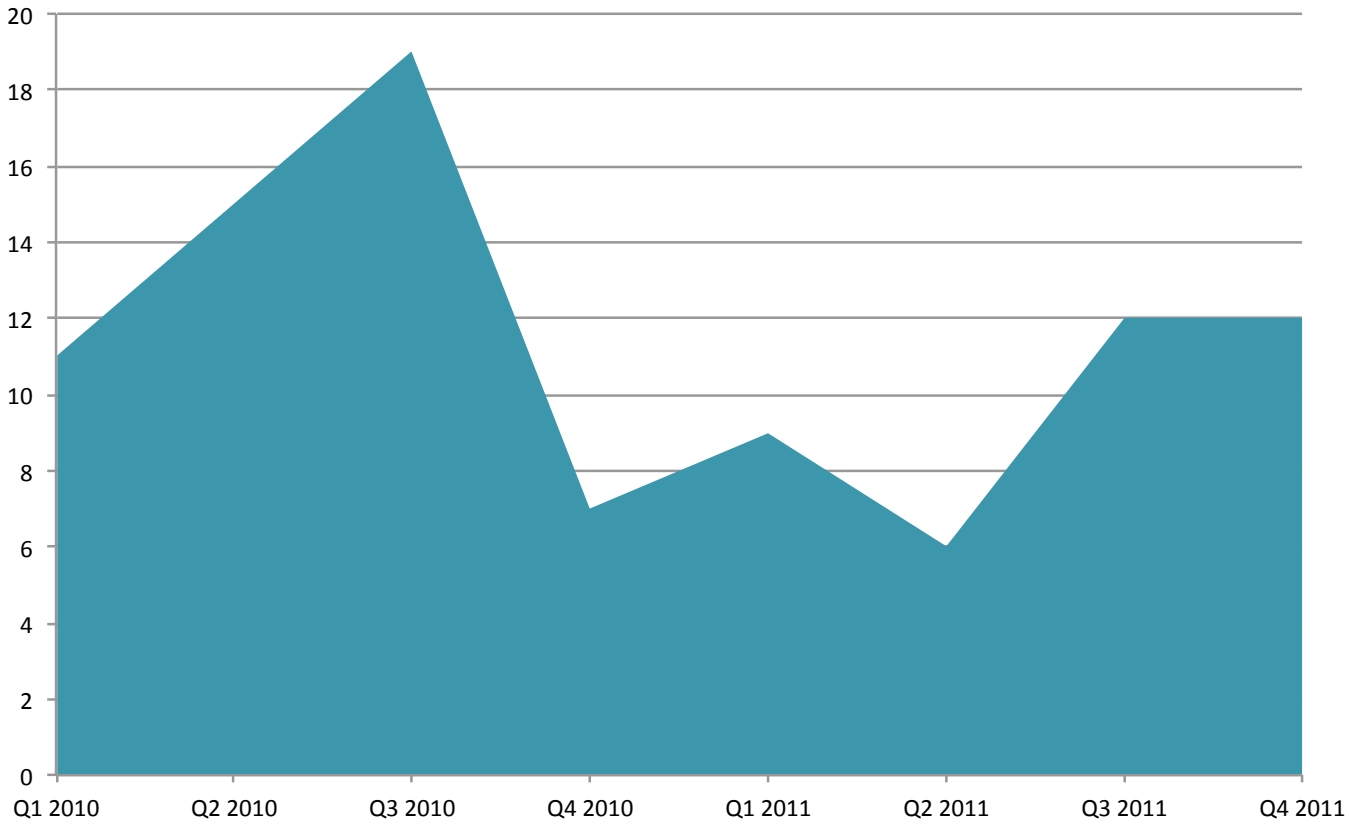
**Definition: the use of commercial/business/company or personal data where the data is obtained, disclosed or procured without the consent of the data owner/controller. This includes the use of commercial/personal data for unauthorised purposes that could place any participating organisation at a financial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

**Real examples:**

- Before the last day of employment, an employee steals company secrets and market data by emailing them to a personal email address. The fraudster was looking to use this data in their next employment.
- A call centre operator, who has access to customer data, notes down various personal items including card details. The operator then goes home and uses the data to purchase items from an online retail shop.

As in 2010, in 2011 there was one case of the Unlawful Obtaining or Disclosure of *Commercial* Data. The number of cases of the Unlawful Obtaining or Disclosure of *Personal* Data decreased from 52 cases in 2010 to 39 in 2011. This equates to a decrease of 25%. The number of cases of this type recorded each quarter of 2010 and 2011 can be seen in *Figure 3.5.1* below.

**Cases of the Unlawful Obtaining/Disclosure of Personal Data in 2010 and 2011 by quarter**
*Figure 3.5.1*



**Reasons for filing Unlawful Obtaining/Disclosure of Commercial/Personal Data Frauds in 2010 and 2011**
*Table 3.5.1*

| | 2010 | | 2011 | | |
|---|---|---|---|---|---|
| **Reasons for Filing** | **Cases** | **% of Total** | **Cases** | **% of Total** | **% change** |
| Disclosure of customer data to a third party | 39 | 75.0% | 29 | 74.4% | -25.6% |
| Fraudulent personal use of customer data | 17 | 32.7% | 7 | 17.9% | -58.8% |
| Contravention of systems access policy | 2 | 3.8% | 4 | 10.3% | +100.0% |
| Contravention of IT security policy | 2 | 3.8% | 3 | 7.7% | +50.0% |
| Modification of customer payment instructions | 4 | 7.7% | 1 | 2.6% | -75.0% |

Essentially, when it comes to the Unlawful Obtaining or Disclosure of Personal Data, the offender will either be carrying this out for his or her own benefit (fraudulent personal use of customer data) or to provide this information to another (disclosure of customer data to a third party). Three quarters of cases in both 2010 and 2011 were for the benefit of a third party. These third parties will generally be professional criminals who have either bribed members of staff to obtain this data, or have placed contacts within an organisation to extract the personal details of customers.

## Adding to the picture

It needs to be borne in mind that professional criminals have also, historically, used threats and coercion to induce unwilling members of staff to obtain and disclose customer information. Where the member of staff has been a victim of this tactic, then they would not be recorded to the Staff Fraud Database as they were not willingly complicit. This means that while the number of occasions where a staff member was willingly involved is counted, there are other, *unquantified*, occasions where the staff member was intimidated or coerced into the act. So, while it appears a positive sign that there were fewer instances of staff engaging with organised criminals to disclose customer data, this does not mean that it is the whole story. Any portrayal of this type of fraud must include the fact that organised criminal elements have a long established history of using the stick (like threats against the staff member's family) rather than the carrot (financial inducement).

## But if data is stolen, why?

Often the data that the staff members disclose will be used to commit identity fraud in the customer's name or to take over the customer's account. The number of these identity related and data driven crimes increased in 2011 compared with 2010. While there are numerous avenues that the perpetrators of these identity related crimes can use to obtain the necessary data (such as phishing emails and other cyber attacks), disclosure from members of staff is accepted as another common source. Staff Fraud Database Members have cited approaches to their staff as a continuing and worrying problem so, while the numbers of these cases have decreased, there is no room for complacency. It should be acknowledged, however, that although approaches are continuing, the fact that the number of complicit staff decreased in 2011 can also be taken as a sign of the success of staff education on this issue. Employers have made sure that staff are aware of the implications and are better equipped to withstand approaches from criminals.

There was also a large decrease in staff members compromising personal data for their own use – down to seven cases, from 17 in 2010. This is probably a sign that, in the present employment market, staff members are unwilling to risk their present employment for any added benefits that income from identity crime might bring them. Tighter system controls and the deterrent effect of the Staff Fraud Database are also likely to be persuading those people who may not be morally opposed to using customer data for their own ends, that the benefits do not outweigh the risk in this instance.

Many organisations hold customer data that would be attractive to those who might wish to obtain it for their personal use. Banking services providers, of course, hold the details of bank accounts and other products, thus making their customers some of the most 'obvious' targets for having their accounts taken over by insiders. This is in addition to any other crimes that may be committed with their personal information. It is therefore unsurprising that the majority of staff members identified as having

>

compromised data were employed in the banking sector. It is equally unsurprising that call centres were the other area affected by this type of fraud. After all, these areas and this fraud were some of the primary instigators that drove the establishment of the Staff Fraud Database.

## And in cases of commercial data?

In 2011, there was one instance of a member of staff being identified as stealing details of internal practices and disclosing them to a third party. While it would not be expected that a large number of these cases would be identified annually, the question was asked, “Why so few?”. Nearly 77% of survey respondents believed that the reason why there is only one case of unlawful obtaining or disclosure of commercial data is that it is difficult to detect this type of fraud. This, evidently, signals a challenge for the future. •

# 4. Who is the fraudster?

This section provides information about the individuals identified as having perpetrated staff frauds in 2011, covering gender, age, business area and length of service. When a case is recorded to the Staff Fraud Database, Members can also record demographic information such as gender and date of birth.

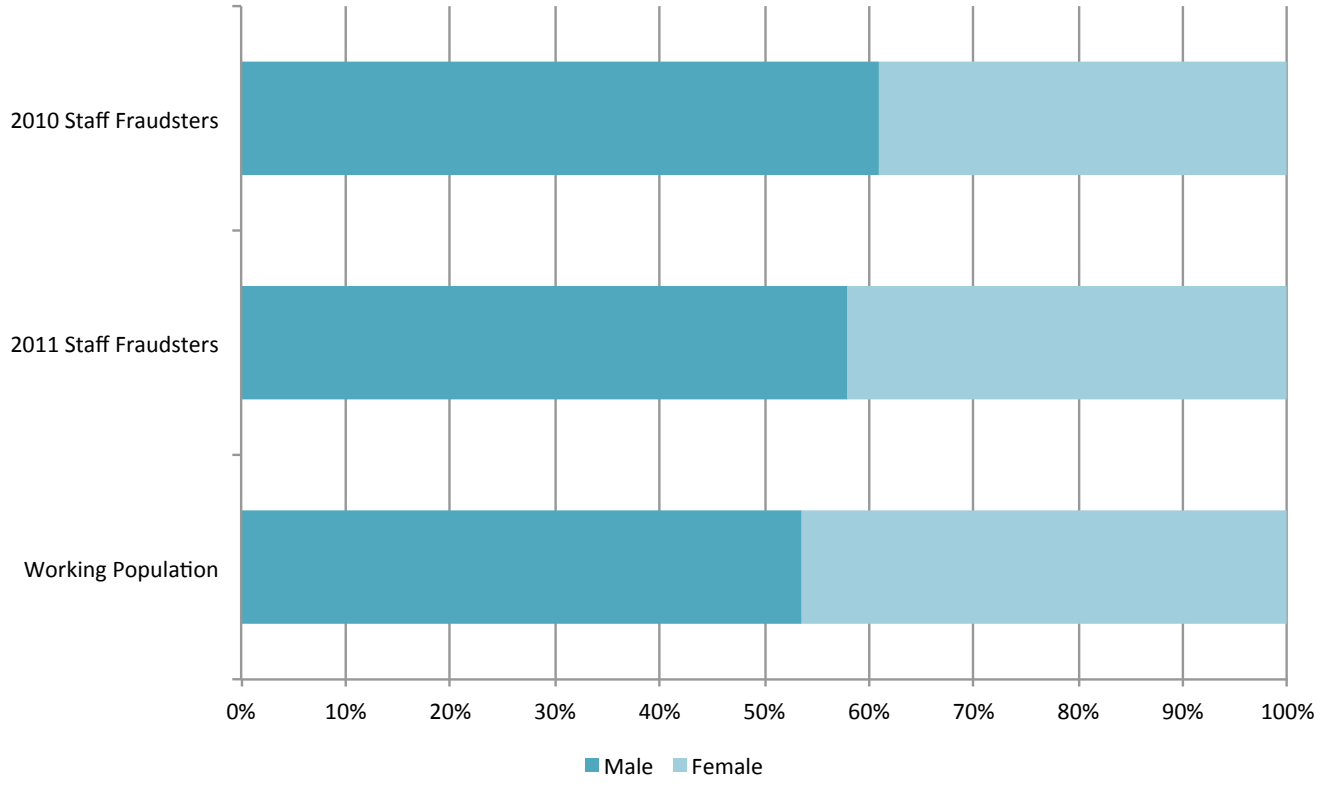
## 4.1 Gender

*Figure 4.1.1* below shows the gender distribution of the staff fraudsters recorded in 2010 (where gender was recorded – 89% of cases), staff fraudsters recorded in 2011 (95% of cases) and the working population of the UK for the 3 months October – December 2011[5].

Over 60% of staff fraudsters were male in 2010, with that figure decreasing slightly to 58% in 2011. This is getting closer to the UK working population figure (for men) of just under 54%. So, while there is still a disproportionately high number of men committing staff fraud, this figure seems to be coming more into line with what might be expected, if all other things were equal.

*Figure 4.1.2* shows the gender distribution of the staff fraudsters recorded in 2011, broken down by the type of fraud that they were involved in. This shows that a higher proportion of men was identified as perpetrating the Unlawful Obtaining or Disclosure of Personal Data and both successful and unsuccessful Employment Application Fraud; while comparatively more women were identified as carrying out Dishonest Actions and Account Fraud.

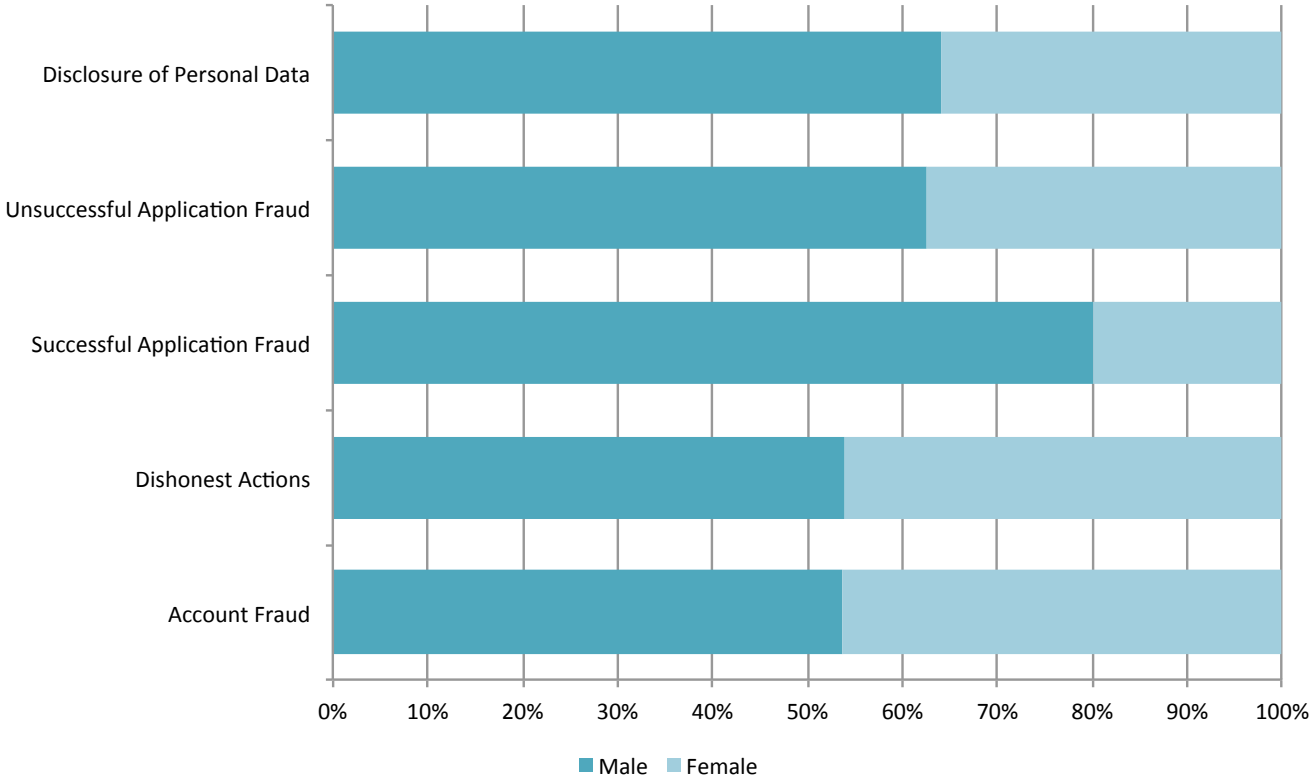
**Gender distribution of Staff Fraudsters and the UK working population**[5]
*Figure 4.1.1*




[5] ONS Labour market statistics: February 2012 - www.ons.gov.uk/ons/dcp171778_254579.pdf

**Gender distribution of Fraud Types 2011**

*Figure 4.1.2*




These findings would tend to imply that women were less often involved with organised criminals and the disclosure of personal data, while they were proportionally more involved in what could be considered the more opportunistic crimes (e.g. theft of cash from customer or employer).

The high proportion of men identified as successfully committing Application Fraud is closely tied in with the type of lies being told on the application. A number of these cases have been recorded for the failure to disclose unspent criminal convictions. If the proportion of the prison population which is male is considered (95%[6]) – and the fact that, by the age of 52, four times as many of the male population of England and Wales have a criminal conviction than the female population[7] – then it is clear that many more men than women have a conviction that they may feel they need to hide. These findings are borne out in *Table 4.1.1*, where it can be seen that, given the proportions of all cases that each fraud type represents, women are over-represented in Account Fraud and Dishonest Actions, while fewer women than would be expected (if all other things were equal) were involved in Application Fraud and Unauthorised Disclosure of Personal Data.

These statistics raise an interesting question however: why, given the substantially higher offending rate of men than women, is the gender distribution of staff fraudsters not skewed *more* towards men? One reason might be that, with a large number of job losses, more women are now the main source of income for their family. With added financial pressures in the current economic climate, these desperate measures may require desperate acts of dishonesty. One case reported to the Staff Fraud Database was a bank manager who stole more than £140,000 from customer accounts to help with her husband's failing business. •

**Staff Fraud cases recorded by Fraud Type in 2010-2011**

*Table 4.1.1*

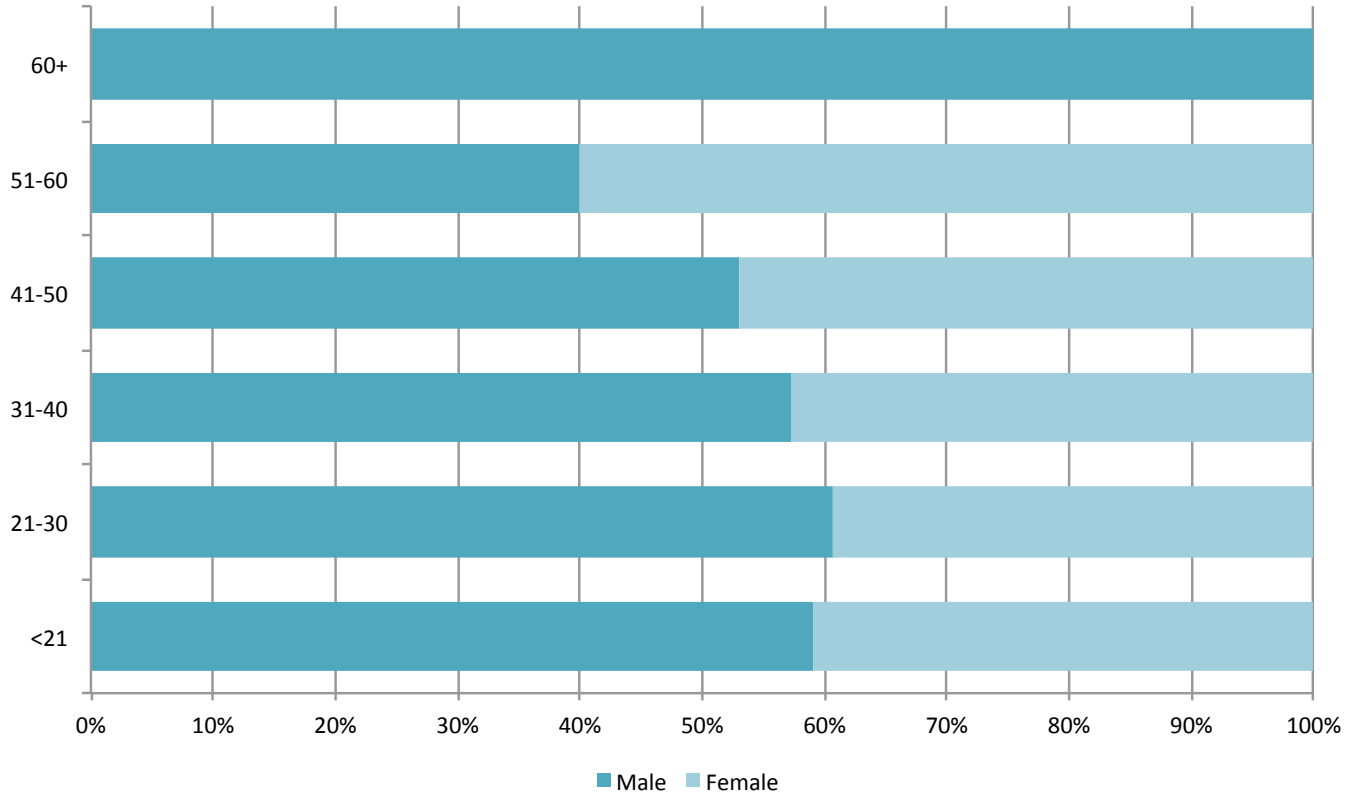
| Fraud Type | Women | Men | All |
|---|---|---|---|
| Account Fraud | 12.6% | 10.5% | 11.4% |
| Dishonest Actions | 64.2% | 54.1% | 58.2% |
| Application Fraud Successful | 2.0% | 5.7% | 4.8% |
| Application Fraud Unsuccessful | 19.9% | 23.9% | 22.0% |
| Unauthorised disclosure of personal Data | 9.3% | 12.0% | 10.3% |

[6] www.justice.gov.uk/statistics/prisons-and-probation/oms-quarterly [7] www.justice.gov.uk/downloads/statistics/mojstats/criminal-histories-bulletin.pdf

# 4.2 Age

**Gender distribution of Staff Fraudsters among age ranges 2011**

*Figure 4.2.1*




Between 2010 and 2011, there has been no real change in the average age of those committing staff fraud. At the time that they were recorded to the database, men had an average age of just under 30 while women were slightly older with an average age of just over 31.

*Figure 4.2.1* shows the gender distribution of the age ranges for staff fraudsters recorded to the Staff Fraud Database in 2011. This shows that the older the age group, the greater the proportion of female staff fraudsters identified (with the exception of the 60+ age range).

There were similarities between men and women in the relationships between their average age and the type of fraud committed. For both genders, the average age of those Disclosing Personal Data and successfully committing Application Fraud was a bit younger than the overall average; particularly for the Disclosure of Personal Data, where the average age of women was 28, and 24 for men. This might indicate that younger staff were more susceptible to approaches from organised criminals, and possibly failed to grasp the implications of their actions. Moreover, younger members of staff have a clean employment history and are able to infiltrate an organisation more easily than older staff with a previous work history. Furthermore, there is a strong perception that younger members of staff are more technologically savvy. Therefore, they may more readily learn how to bypass internal controls to carry out data theft.

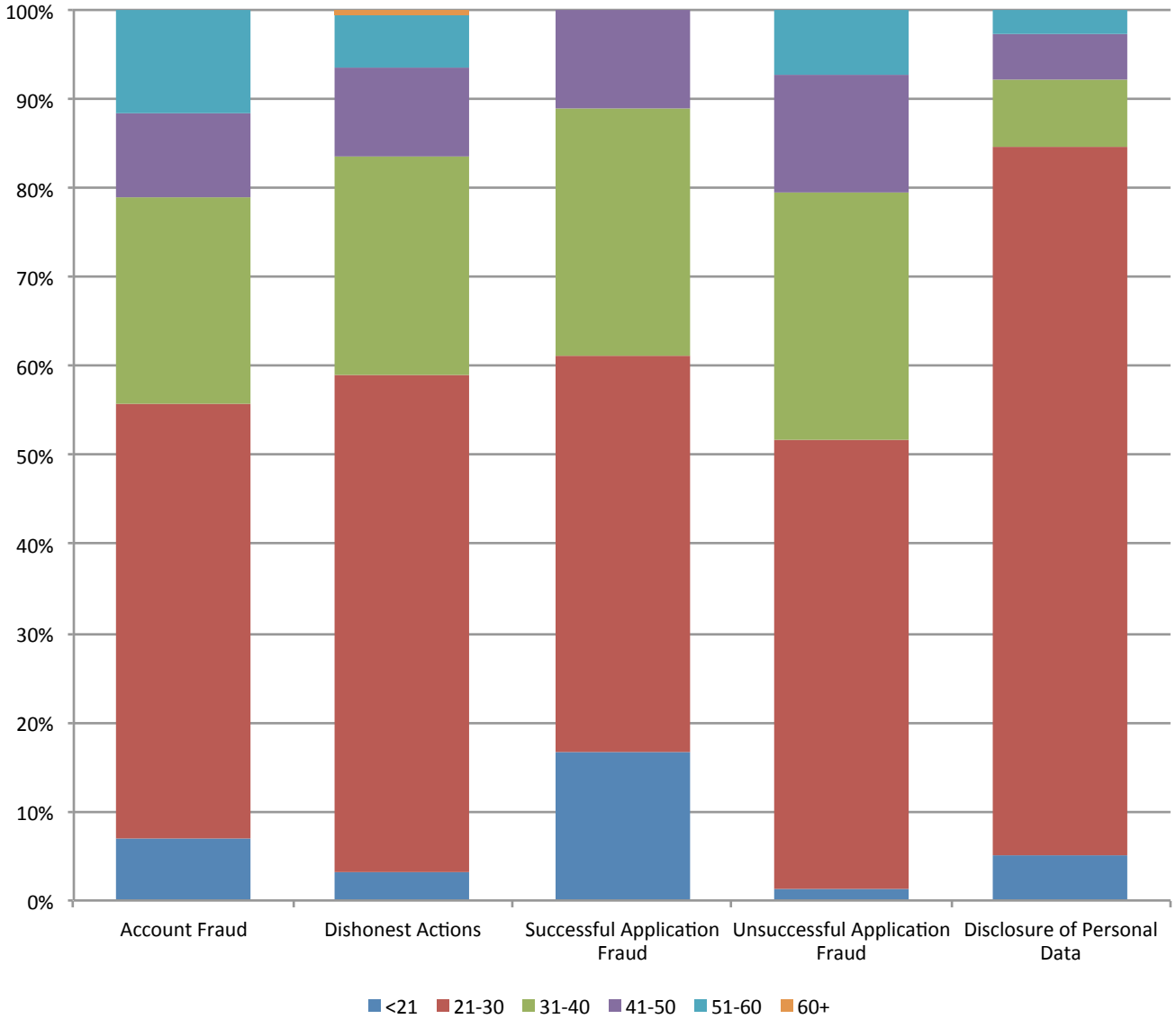
It is interesting, however, that there was a discrepancy between the average ages for those who were successful in their application for employment and those who were not. The successful applicants had a younger average age than the overall average, while the average age of those who were unsuccessful. As with gender, this was largely due to the types of material falsehood that were spotted at an early stage and those revealed further down

>

the line. The older fraudster would appear to be more concerned about hiding an adverse credit history than their younger counterpart, while the impetuosity of youth has led to feeling the need to try and hide such things as unspent convictions and/or being fired from a previous position. This is illustrated in *Figure 4.2.2*.

**Age distribution of Staff Fraudsters across Fraud Types**

*Figure 4.2.2*



## 4.3 Business Areas

It is not surprising, given the nature of many of the cases of staff fraud identified, that the majority of fraud takes place in high street branches, stores or retail outlets. In bank branches particularly, the staff, who may well be relatively junior, are handling money and have access to customer accounts. The proportion of fraud taking place in branches, stores or outlets, however, has decreased in 2011 compared with 2010. There has been an increase, though, in the proportion that took place in customer contact centres/call centres. In these locations the staff have access to accounts and account information, if not the physical cash. This can be seen in *Table 4.3.1*.

It is notable that there was an increase in the number of cases of disclosure of personal information that were identified in customer contact centres. This is due to an increase in frauds identified in these locations coupled with a decrease in the number identified in branches, stores and outlets. It may be the case that, as mentioned earlier in this report, education is helping branch staff to refuse the approaches from criminals intent on obtaining personal data.

**Business Areas where Staff Fraud cases were recorded in 2010 and 2011 by Fraud Type**
*Table 4.3.1*

**Key**
**ACF** = Account Fraud
**DIS** = Dishonest Actions by Staff to Obtain a Benefit by Theft or Deception
**EAS** = Employment Application Fraud Successful
**UDP** = Unlawful Obtaining or Disclosure of Personal Data

| | 2010 | | | | 2011 | | | |
|---|---|---|---|---|---|---|---|---|
| **Business Area** | **ACF** | **DIS** | **EAS** | **UDP** | **ACF** | **DIS** | **EAS** | **UDP** |
| Branch/Retail outlet/Store | 81.8% | 67.1% | 40.0% | 79.3% | 77.3% | 64.0% | 45.5% | 58.3% |
| Customer contact centre | 13.6% | 15.8% | 60.0% | 20.7% | 18.2% | 21.6% | 36.4% | 33.3% |
| Field unit | - | 11.8% | - | - | - | 1.8% | 9.1% | - |
| IT department | - | - | - | - | - | 0.9% | - | - |
| Other | - | 2.6% | - | - | - | 8.1% | - | 8.3% |
| Other support services | - | 2.6% | - | - | - | 3.6% | 9.1% | - |
| Staff contact centre | 4.5% | - | - | - | 4.5% | - | - | - |

# 4.4 Length of Service

**Average length of service of staff fraudsters**

*Figure 4.4.1*


Overall, there was a slight drop in the average length of service before an employee was identified as having carried out a fraud. The staff fraudster recorded in 2011 had been in post for for an average of 5½ years – whether they had been carrying out fraud for that length of time or had previously been honest employees is unknown.

*Figure 4.4.1* clearly illustrates that female staff fraudsters are in post for longer than men. Those who carried out Account Fraud had been in post the longest although the average length of service for female members of staff who carried out Account Fraud decreased in 2011 while it increased for men.

The lower average length of service of those who compromised personal data is an indication that some of these individuals were placed in an organisation with the intention of carrying out that fraud. Moreover, as previously stated, the technologically savvy younger members of staff may be more able to bypass internal controls to commit data theft. However, they may be able to do this more quickly than the overall average length of service of a staff fraudster. 21% of respondents to our survey stated that they believed that their organisation had suffered infiltration from organised criminals.

Respondents to this same survey also suggested the following reasons why more established members of staff were committing fraud:

1. Increased knowledge of internal controls
2. Loss of commitment to the employer
3. Feelings of entitlement
4. Members identifying more established staff involved in fraud due to increased monitoring levels
5. Financial pressures including debt and greed
6. Collusion with organised criminals

Most respondents particularly cited that the increased knowledge of internal controls and loyalty issues were major factors why more established staff were involved in staff fraud.

# 5. Identifying frauds and taking action

This section gives some indication of the actions taken by organisations to uncover the fraud and against the fraudster, beyond recording them to the Staff Fraud Database.

The proportion of staff who were dismissed after being identified as having committed staff fraud increased in 2011 to 65%, from 58% in 2010. In the majority of other cases, the fraudster resigned during the course of the investigation. This increase in dismissals is likely to be due to the nature of the cases identified. If a case is quite cut and dried, then the time taken to complete an investigation is less, and therefore the opportunity for the member of staff to resign while an investigation is continuing is minimal. However, it is encouraging that the CIFAS Staff Fraud Members decided to continue the internal fraud investigation even when the fraudster had resigned. If this had not been the case i.e. that the investigation of staff fraud was not taken seriously, then it is likely that the number of staff resigning during the investigation would have risen.

Pleasingly, in 2011 fewer frauds only came to light after the staff member had resigned, as these were essentially cases where the fraudster got away with it. There were 17 of these cases in 2010, but only 9 in 2011. Reasons for this range from: improved internal controls making the fraud harder to disguise, and also to an uptake of best practice in ensuring that staff members take at least two continuous weeks of leave a year. It may be possible for a staff member's workload to wait for their return if they are only off work for one week, but if they are off for two, then it is more likely that a colleague will have to take over the workload; providing an opportunity to uncover any fraud.

## 5.1 Means of discovery

The means of discovery of the different types of staff fraud are shown in *Table 5.1.1* below.

**Means of Discovery of Staff Fraud cases by Fraud Type in 2010-2011** (See page 28 for key)
*Table 5.1.1*

| | 2010 | | | | | 2011 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Means of Discovery** | **ACF** | **DIS** | **EAS** | **UDP** | **Total** | **ACF** | **DIS** | **EAS** | **UDP** | **Total** |
| Customer | 57.5% | 35.3% | 0.0% | 40.4% | **36.7%** | 53.5% | 30.0% | 5.9% | 43.6% | **31.4%** |
| Internal controls/audit | 17.5% | 34.0% | 54.5% | 26.9% | **31.2%** | 41.9% | 49.5% | 17.6% | 20.5% | **44.3%** |
| Law enforcement | 2.5% | 3.2% | 18.2% | 0.0% | **3.4%** | 0.0% | 1.4% | 17.6% | 10.3% | **3.0%** |
| Other | 7.5% | 7.7% | 0.0% | 21.2% | **9.7%** | 2.3% | 5.9% | 47.1% | 12.8% | **8.8%** |
| Staff | 12.5% | 17.3% | 9.1% | 7.7% | **15.2%** | 2.3% | 10.5% | 0.0% | 10.3% | **9.5%** |
| Staff (whistleblowing) | 2.5% | 2.6% | 18.2% | 3.8% | **3.8%** | 0.0% | 2.7% | 11.8% | 2.6% | **3.0%** |

It is heartening that internal controls and audit appeared to be performing increasingly well when it comes to identifying where fraud had taken place. These controls identified almost half of Dishonest Actions in 2011, and over 40% of instances of Account Frauds (up from 34% and 17% respectively in 2010). This means that a lower proportion of these cases were reported to the employer by the customer. That can only be good news for employers as considerable reputational damage can be done by customers being aware of rogue members of staff and therefore viewing the organisation as untrustworthy.

>

The customer, however, continued to be the most effective method of highlighting instances of disclosure of personal data to the employer. This is on the one hand disappointing for the employer, as this would imply that internal controls are failing to highlight the issue adequately; leaving the employer exposed to the risk of severe reputational damage. On the other hand, however, where the issue was compromised personal data, the fact that the customer was able to recognise when a member of staff had done this can be seen as a success for the education of the public on the dangers of identity fraud.

Fewer frauds were reported to the employer by other members of staff. This begs the question "why were more cases not reported by colleagues?" Is it the case that other staff were just not noticing what their co-workers were getting up to, or were they choosing not to see? Were they choosing not to report for the same reasons as they did not report through whistleblowing? 80% of the respondents to the staff fraud survey stated that the comparatively low level of whistleblowing could be attributed to the whistleblower's fear of repercussions. Also, approximately 60% of the respondents believed that their staff members' view that reporting fraud was not their responsibility and their fear of repercussions for their work colleagues were the reasons why there was a low rate. Some respondents also suggested other reasons for the low level of reporting e.g. staff may fear that they might be wrong in their suspicions; staff located in branch/retail businesses have close relationships with their colleagues, which may prevent them from reporting; staff still think that whistleblowing is not completely confidential. Conversely, staff may be comfortable in reporting fraud through other non-confidential channels, e.g. through their line manager and this may have had an effect on the low rate of whistleblowing. Furthermore, the internal controls may have picked up the fraud before staff were aware that a colleague was involved in a fraud. It is worth noting that larger organisations who responded to the survey stated that they did not experience a low rate of whistleblowing.

## 5.2 Reported to the police

There was a slight decrease in the proportion of cases that were reported to the police in 2011 (25% of cases) compared with 2010 (27%).

The drop in the proportion of cases reported to the police was likely to have been a reflection of the perceived seriousness of the offences committed. Often, fraud is not considered to be worth the time and resource required to make a report to the police and to produce an evidential package to support a prosecution. This resource requirement will also have played a bigger part during the present economic circumstances, with many organisations operating with a reduced headcount. The downside of not making a report to the police, of course, is that it risks giving the impression that the organisation doesn't have a zero-tolerance policy with regard to fraud. The greater the number of cases reported and prosecuted, the greater the deterrent effect on other members of staff.

This more 'risk based' policy was illustrated by the types of fraud which were reported to the police, however. In 2011, the proportion of those Disclosing Personal Data (the most commonly reported fraud type) who were reported to the police increased to 54% of cases compared with 36% the year before. The proportion of Dishonest Actions reported decreased from 38% of cases down to 30%. Employment Application Frauds are almost never reported.

When we asked the participants of the staff fraud survey about the low reporting of staff fraud; between 55% - 60% of the respondents stated that the police were not interested and not sufficiently resourced. However, 57% of the respondents also considered that reporting to the police could damage their organisation's reputation. 43% were satisfied with their current avenues for reporting fraud, e.g. the Staff Fraud Database, regulator, civil proceedings. It is worth noting that all respondents were willing to report fraud to the police, but that it was recognised that the police would have other priorities.

# 5.3 Staff Fraud convictions

As highlighted in Chapter 5.2, only a quarter of cases recorded in 2011 were reported to the police. Of those cases, just under a quarter resulted in either a guilty verdict or plea or the court case was still pending. The other three quarters had not been progressed.

This was a slight decrease from 2010, so in 2011 not only was a smaller proportion reported to the police, but a lower proportion of the ones that had been reported resulted in a criminal conviction or were still awaiting trial. The good news, though, was that although the proportions were lower, there was still one more person recorded to the Staff Fraud Database in 2011 who was either found guilty or was awaiting trial compared with the previous year.

It does need to be borne in mind, however, that there can be a lengthy time lag between a fraud being identified and reported to the police, and the outcome of a court case. Interestingly, the same number of cases recorded on the Staff Fraud Database resulted in a guilty verdict, where that verdict was reached in 2011, as in 2010 – 14 cases.

It is, also, interesting to see that almost 30% of the individuals convicted in 2011 were found guilty of stealing personal data. This is an offence that can have serious repercussions for the organisation from which the data is stolen, the organisation against which that data may be used and last but by no means least, the person whose details have been stolen. It is a crime that is invariably linked to further criminality and puts affected customers and organisations equally through the process of undoing the damage done.

The following examples give some flavour of the varying actions and motivations of individuals recorded to the Staff Fraud Database. These individuals were all convicted in 2011. •

### Case Study 1: Feeding the habit

A member of bank staff pleaded guilty to four counts of fraud by abuse of position after targeting the accounts of elderly and wealthy individuals and transferring funds to his own account in order to fund his gambling habit. He targeted those who had little activity on their accounts in the hope that they wouldn't notice, and he used other staff members' identities to perpetrate the frauds to cover his tracks. He even targeted his own father's account.

### Case Study 2: Well paid executive who steals staff bonus

An executive at an insurance company, who had worked for the organisation for 25 years, was jailed for expenses fraud. He made a number of fraudulent expenses claims (including expenses for cricket matches and journeys that he had not made). He also diverted vouchers intended for staff bonuses into his own pocket. The fraud was to support a lifestyle he could not maintain because he had expected a promotion and spent money that would have been covered by the pay rise associated with that promotion.

### Case Study 3: Infatuated bank worker stole account details for boyfriend

A bank worker, who was described as infatuated with her boyfriend, stole the account details of 12 customers she had served, giving them to her boyfriend who then stole £20,000 from their accounts. They were both sentenced to 10 months in prison.

# 6. Final Thoughts

CIFAS Staff Fraud Adviser, Arjun Medhi, concludes: "*Staff Fraudscape* has revealed that a web of issues contribute to create an environment where fraud by insiders can be committed. From the personal circumstances of the fraudster - e.g. debt, gambling, personal problems - through to organisational issues such as lapses in security and controls, or a culture of silence: all of them highlight areas that need to be put under constant review.

"Building closer working relationships between fraud and HR teams will be an essential ingredient in combating staff fraud, as will education and security reviews.

"Instilling an anti fraud culture of zero tolerance – with clear reporting structures and key checks and balances built into everyday processes – remains a vitally important part of any anti fraud strategy. While there have been numerous successes in countering fraud, there will always be a challenge in ensuring that fraud is never treated complacently; as it is such complacency that helps to breed the atmosphere in which fraud will thrive."

# Appendix: Staff Fraud Survey

The survey received 67 full responses in total from across the CIFAS membership.

## Q1. What do you think are the contributory factors to the increase in staff fraud?

Please rate the options from 1 (no contributory factor) to 5 (a major contributory factor).

| | No. of Responses | | | | | | |
|---|---|---|---|---|---|---|---|
| **Factors** | **1** | **2** | **3** | **4** | **5** | **Average Response (Mean)** | **Most Common Response** |
| Lack of clear policy/procedures | 22 | 16 | 17 | 9 | 3 | 2 | 1 |
| Poor security | 14 | 9 | 20 | 19 | 5 | 3 | 3 |
| Weak internal controls | 7 | 11 | 17 | 19 | 13 | 3 | 4 |
| Debts | 3 | 8 | 16 | 17 | 23 | 4 | 5 |
| Personal problems (e.g. gambling, addictions) | 4 | 7 | 18 | 18 | 20 | 4 | 5 |
| Greed | 2 | 8 | 20 | 23 | 14 | 4 | 4 |
| Fear of redundancy | 17 | 24 | 16 | 9 | 1 | 2 | 2 |
| Malice/revenge | 19 | 17 | 18 | 10 | 2 | 2 | 1 |
| Organised crime | 7 | 7 | 18 | 25 | 9 | 3 | 4 |

All factors were listed as contributing to the increase in staff fraud but, when looking at the frequency of the ratings, the most common contributory factors mentioned were debts, personal problems, weak internal controls, greed and organised crime. Other suggested factors were: lack of staff training/awareness; lack of an anti fraud culture; and other financial pressures from a recession.

## Q2. Why do you believe there is such a low rate of whistleblowing?

Nearly 80% of the respondents believed that the reason for such a low rate of whistleblowing was due to the whistleblowers' fear of personal repercussions; with over 60% believing that the whistleblowers feared repercussions for their colleagues Approximately 60% of the respondents also believed that the prevailing view among staff was that reporting fraud is not their responsibility. Some respondents also commented on other reasons for low levels of reporting: e.g. staff may fear that they might be wrong in their suspicions; staff located in branch/retail businesses

| | No. of Responses | | Proportions | |
|---|---|---|---|---|
| **Reasons** | **Yes** | **No** | **Yes** | **No** |
| Not their responsibility | 39 | 27 | 59.1% | 40.9% |
| Fear of repercussions for themselves | 51 | 15 | 77.3% | 22.7% |
| Fear of repercussions for colleagues | 40 | 25 | 61.5% | 38.5% |
| Don't regard it as necessary | 32 | 32 | 50.0% | 50.0% |
| No formal procedures in place | 16 | 49 | 24.6% | 75.4% |
| Unaware of what constitutes a fraud | 33 | 32 | 50.8% | 49.2% |
| Other | 10 | 31 | 24.4% | 75.6% |

>

have close relationships with their colleagues which deter them from reporting; staff still fear that whistleblowing is not completely confidential. Conversely, staff may be comfortable in reporting fraud through other non-confidential channels: e.g. through their line manager. Furthermore, internal controls may have picked up a fraud before staff were aware that a colleague was involved. Larger organisations who responded stated that they did not experience a low rate of whistleblowing.

Half of the respondents stated that their staff did not understand what constituted a fraud. The problem is that there is no single definition of fraud. As there is much emphasis on the procedure (i.e. the deceptive act that is carried out before theft), truly defining fraud can be a challenge because it "does not exist as a coherent or single activity" (Alan Doig, 2006, *Fraud* p.19). Despite being legally established under the Fraud Act 2006, fraud is a "grey area": spanning from an "outright criminal offence, to being the result of poor business management, ignorance or even sharp business practice". Fraud will "always have supplementary and wider definitions than those in law" (Attorney General's Office, 2006, p.25).

## Q3. Why are so many employee frauds not reported to the police? (Please select all that apply)

Well over half of all respondents stated that the reasons why so many staff frauds were not reported to the police was that the police were either not interested (60%) or not sufficiently resourced (55%). However 57% of the respondents also believed that reporting to the police could damage their organisation's reputation. 43% were satisfied with their current avenues for reporting fraud (e.g. through the Staff Fraud Database, regulator, or civil proceedings). It is worth noting that all respondents would have been willing to report to the police but recognised that the police had other priorities.

| Reasons | No. of Responses | % of Respondents |
|---|---|---|
| Damage to reputation | 37 | 56.9% |
| Impact on morale of the existing workforce | 7 | 10.8% |
| Lack of clear policy | 18 | 27.7% |
| Police are not interested | 39 | 60.0% |
| Police are not sufficiently resourced | 36 | 55.4% |
| Police provide no feedback | 17 | 26.2% |
| Other avenues are sufficient e.g. Staff Fraud Database/Dismissal/Reported to regulator/Civil proceedings | 28 | 43.1% |

## Q4. Has your organisation experienced frauds committed by the following?

Nearly 80% of the respondents had experienced frauds committed by non-management staff, with almost half having experienced frauds committed by management. 57% had experienced frauds committed by staff that were supplied by an employment agency, contractor or other third party supplier.

>

| | No. of Responses | | | Proportions | | |
|---|---|---|---|---|---|---|
| | Yes | No | Not Known | Yes | No | Not Known |
| Non-management staff | 51 | 13 | 1 | 78.5% | 20.0% | 1.5% |
| Board | 3 | 53 | 9 | 4.6% | 81.5% | 13.8% |
| Senior management | 9 | 47 | 9 | 13.8% | 72.3% | 13.8% |
| Management | 27 | 32 | 6 | 41.5% | 49.2% | 9.2% |
| Agency/Third party/Contractors | 36 | 26 | 3 | 55.4% | 40.0% | 4.6% |

## Q5. What do you think are the reasons for more established staff being involved in fraud?

Please rate each option from 1 (not a factor) to 5 (the most significant factor).

All the listed reasons have had some contribution to the increase in more established staff fraudsters; in particular, increased knowledge of internal controls and lack of loyalty to the employer appear to be significant factors. However, respondents also cited financial pressures including debts and greed as additional factors, as well as organised criminal involvement.

| | No. of Responses | | | | | Average Response | Most Common Response |
|---|---|---|---|---|---|---|---|
| Factors | 1 | 2 | 3 | 4 | 5 | | |
| Increased knowledge of internal controls | 4 | 4 | 13 | 33 | 11 | 4 | 4 |
| Loss of commitment to the organisation | 5 | 12 | 22 | 25 | 1 | 3 | 4 |
| Feelings of entitlement | 9 | 14 | 25 | 14 | 3 | 3 | 3 |
| Increased monitoring levels within the organisation | 10 | 21 | 25 | 4 | 2 | 2 | 3 |
| Other factor(s) | 18 | 2 | 8 | 3 | 2 | 2 | 1 |

## Q6. What forms of organised crime (if any) has your organisation experienced?

Over 65% of the respondents had experienced some form of staff fraud linked to organised crime. 40% of the organisations who had done so had also experienced organised criminals colluding with their staff; and 40% had experienced organised criminals coercing their staff. 21% of those who had experienced organised criminal involvement in staff fraud had been victims of infiltration.

| | Yes | No | Not Known | Yes | No | Not Known |
|---|---|---|---|---|---|---|
| Infiltration | 14 | 40 | 11 | 21.5% | 61.5% | 16.9% |
| Collusion | 29 | 25 | 11 | 44.6% | 38.5% | 16.9% |
| Coercion | 26 | 29 | 10 | 40.0% | 44.6% | 15.4% |
| No experience | 13 | 42 | 10 | 20.0% | 64.6% | 15.4% |

## Q7. In your opinion, what is the reason for only one case of 'unlawful obtaining or disclosure of commercial data' being recorded on the CIFAS Staff Fraud Database?

Nearly 77% of the respondents believed that the reason why there had been only one case of Unlawful Obtaining or Disclosure of Commercial Data was that it was difficult to detect this type of fraud, with over 60% considering that it was difficult to prove such frauds when they were discovered. Only just over 15% of respondents believed that these frauds were not being committed.

| | No. of Responses | | | Proportions | | |
|---|---|---|---|---|---|---|
| | Yes | No | Not Known | Yes | No | Not Known |
| These frauds are not being committed | 10 | 42 | 13 | 15.4% | 64.6% | 20.0% |
| It is difficult to detect these frauds | 50 | 12 | 3 | 76.9% | 18.5% | 4.6% |
| It is difficult to meet the standard of proof when such frauds are detected | 40 | 19 | 6 | 61.5% | 29.2% | 9.2% |
| Other | 5 | 26 | 34 | 7.7% | 40.0% | 52.3% |

## Q8. What is the purpose of – or what is gained from – profiling staff fraudsters? (Select all that apply)

Professional services firms who consult on staff fraud have often stated that there is no point in profiling fraudsters, as they come 'in different shapes and sizes'. However, over 95% of respondents see a use in profiling. 55% use profiling to highlight potential dangers and 46% use profiling to help detect fraud at an earlier stage (e.g. one respondent uses profiling in its recruitment process). Although it is worth keeping an open mind, there is scope for organisations to develop an internal fraud risk profile.

| Reasons | No. of Responses | % of Respondents |
|---|---|---|
| Increases general awareness | 22 | 33.8% |
| Highlights potential danger zones | 36 | 55.4% |
| Helps to detect frauds at an earlier stage | 30 | 46.2% |
| It captures the interest of the media | 5 | 7.7% |
| No use | 3 | 4.6% |

## Q9. Which fraud type(s) do you think your organisation is at risk from/vulnerable to? Which fraud type(s) do you think will increase in 2012?

For both questions, 'Dishonest Action by Staff to Obtain a Benefit by Theft or Deception' was cited as the biggest threat. Over 40% of the respondents expected this type of fraud to increase the most in 2012.

**For further information, please contact our Research, Staff Fraud and Communications Teams**

**CIFAS**
**6th Floor, Lynton House**
**7-12 Tavistock Square**
**London**
**WC1H 9LT**

**press@cifas.org.uk**
**staff.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