Staff FRAUDSCAPE

Depicting the UK's staff fraud landscape

www.cifas.org.uk | May 2011

CIFAS

The UK's Fraud Prevention Service

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 over 250 Members spread across banking, credit cards, asset finance, retail credit, mail order, insurance, savings and investments, telecommunications, factoring and share dealing. 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, and currently 205 organisations participate. 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 burden 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.

This *Report* examines and assesses the staff fraud cases identified by CIFAS Member organisations during previous years and 2010, to ascertain any key differences between the typology of the frauds seen. It looks at all frauds identified by the type of fraud committed and other key criteria.

In this Report . . .

CIFAS is a not-for-profit organisation, concerned solely with the prevention of fraud and funded by subscription. Since February 1991 the membership association has been an independent Company Limited by Guarantee. CIFAS Members are drawn primarily from the UK financial services industry, but also from telecommunications, insurance and other business sectors and the public sector.

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

Introduction
by Peter Hurst, CIFAS Chief Executive

The majority of staff in any organisation work hard and are honest, reliable individuals. What can an organisation do, however, to keep 'bad apples' at bay?

Sadly, this is a question that too few organisations even consider; preferring, instead, to react to situations only when they occur rather than put in place procedures and policies for preventing fraud from the inside.

The CIFAS Staff Fraud Database is a data sharing scheme that enables responsible employers to record, and share with other participants, information on confirmed cases of staff fraud. The CIFAS Staff Fraud Database was launched in 2006 in consultation with the Information Commissioner's Office; the Financial Services Authority; the Confederation of British Industry; the Trades Union Congress and the Chartered Institute for Personnel and Development. Since there is a very low rate of reporting fraud to law enforcement and other authorities, the Staff Fraud Database is a reputable, reliable and legitimate way to report staff fraud and deter staff fraudsters.

Staff Fraud Members covering 205 organisations access the database in order to record data about staff fraud cases, and to check staff fraud cases recorded by other participating organisations. This can be done either to pre-screen applicants or to screen current employees. Before a fraud can be recorded to the Staff Fraud Database, the case must have been investigated, and a burden of proof established (sufficient evidence for it to be reported to the police - even though there is no obligation to do so). Therefore, these frauds are proven. They are not suspicions. They are frauds.

Staff Fraudscape analyses the cases of staff fraud filed to the CIFAS Staff Fraud Database by participating organisations in 2010 and compares them with previous years. *Staff Fraudscape* also includes input from the relationship that CIFAS shares with our Member organisations, and fraud and human resources experts from other prominent organisations. We speak to them about what they identify, the trends that they notice, the *modus operandi* of the fraudsters and the likely areas in which they will strike. The findings presented in *Staff Fraudscape* raise many issues about the steps organisations need to consider, as well as demonstrate the ways that internal frauds have been committed in 2010.

The threat posed by the small proportion of staff who act dishonestly and defraud the organisation that they work for is immense. Not only do such fraudsters abuse the trust placed in them by their employer, their colleagues and customers alike, but they can cause unquantifiable damage to reputation and morale, in addition to the immediate financial impact. Fraudsters' techniques range from compromising customer or payroll data; straightforward theft or the submission of inflated expenses; through to falsifying or failing to disclose significant and pertinent information on an application for employment. Exacerbating this problem is the fact that those staff who have been dismissed for (or who resigned before being identified as involved in) a fraudulent activity, frequently move unchallenged from one employer to another: exposing the new employer to the risk of further fraud. It was to prevent such situations that the CIFAS Staff Fraud Database was established.

Staff Fraudscape provides the authoritative insight to the staff frauds identified in 2010, and the trends and methods used to defraud organisations.

1. Executive Summary

An examination of the staff frauds recorded by Members to the CIFAS Staff Fraud Database in 2010 reveals that:

- Even after taking into account the small 3% decrease in 2010, staff fraud has still increased by over 40% since 2008.
- A 63% increase in instances of staff unlawfully obtaining or disclosing personal data was recorded in 2010, with younger age groups more likely to be involved.
- More established members of staff are committing frauds. The average length of time in employment before the fraud was discovered increased to 5.5 years from 4.3 years in 2009.
- The economic uncertainty of recent years, combined with an ever more competitive job market, has led to more and more people attempting to gain employment fraudulently; the 70% increase in unsuccessful employment application frauds indicates that organisations are increasingly checking applications for fraud before recruitment procedures are completed.
- While instances of staff attempting fraudulently to claim benefits by theft or deception decreased by 29% in 2010 compared with 2009, this was still the most common type of fraud committed by insiders.

The value of data

In an age where the value of personal information is widely known, it is perhaps unsurprising to see an increase in the theft or disclosure of such data. The uncomfortable reality, however, is that this reveals a much bleaker side to the staff fraud problem; with such frauds frequently linked to serious and organised criminal behaviour. Furthermore, an age gap has crystallised in 2010: with 29% of staff fraudsters aged under 21 being guilty of data related staff frauds. This is in stark comparison with only 3% of staff fraudsters aged 41-50 and not a single instance of any fraudster aged over 50 committing such frauds. Does such a stark difference indicate a pronounced shift and evolution in criminal behaviour?

In spite of this, the set of economic and employment difficulties that face the younger members of the workforce in particular mean that the overall profile of staff fraudsters changed in 2010 – with younger people committing more fraud in 2010 than ever before.

Putting checks in place

While overall fraud levels have decreased slightly, organisations' attempts to instil an anti-fraud culture appear to be working, with a marked decrease in attempts to obtain benefits by theft or deception. Any feeling of success, however, must be counterbalanced by the 5% increase in frauds where staff have carried out unauthorised activity on a customer's account (e.g. withdrawing funds). Staff Fraud Database Members' efforts in promoting an awareness of fraud to their employees and customers does mean that more staff have identified fraud in 2010 than in 2009, while customers spotting fraud remained at the 2009 levels.

Such figures pose some questions: are existing anti-fraud controls strong enough? Does the increase in staff fraudsters' average length of service indicate that those fraudsters have gained knowledge of stronger, more complex, controls before bypassing them? Or is the increase in length of service indicative of the economic pinch affecting the widest possible range of staff?

Stopping the fraudsters

The concept of fraud being carried out by a trusted employee, peer or colleague is uncomfortable and, unfortunately, many organisations are more willing to acknowledge the risk of fraud from potential customers. This means that internal fraudsters are often left undetected, and unchallenged when caught. The problem of dealing with an identified fraudster, therefore, remains as challenging as ever.

In 2010, fraudsters increasingly left their employer during an internal investigation and, by doing so, avoided dismissal, while only 27% of staff fraudsters were reported to the police in 2010. This means that nearly three-quarters of staff fraudsters are in a position where they could (under different circumstances) have gone on to obtain successful employment elsewhere. The importance of the Staff Fraud Database, therefore, lies in highlighting fraudsters' previous activities to other participants. This becomes paramount in preventing fraudsters from moving unchecked to a new position with an unsuspecting employer.

All of which demonstrates that as fraud techniques and fraudster characteristics develop, so must the techniques used by organisations to prevent fraud, and to deal with it once it has been identified.

2. CIFAS Staff Fraud Database: Overview

Table 1 shows that a total of 321 cases were recorded to the Staff Fraud Database in 2010, a small decrease of 3% compared with 2009.

Staff Fraud cases recorded 2008-2010

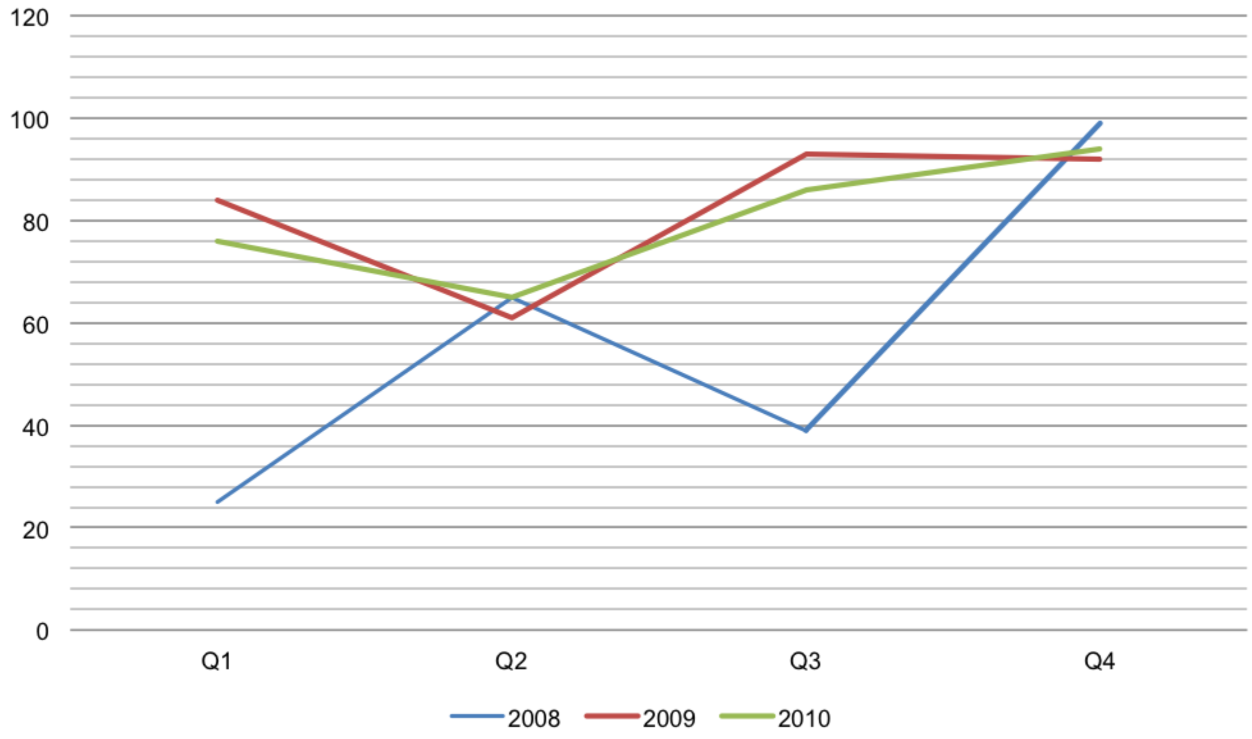
Table 1

Year	**2008**	**2009**	**2010**
Cases Recorded	228	330	**321**
% change	**-**	**45%**	**-3%**

Figure 1 presents the number of staff fraud cases recorded by quarter for the last three years. This shows that the pattern of staff frauds recorded in 2010 closely follows the pattern seen in 2009, with a decrease in quarter two followed by an increase in the second half of the year. It will be interesting to see whether this downward trend in quarter two recurs in 2011 and, if it does, research will need to be undertaken to ascertain the reasons.

Staff Fraud cases recorded by quarter 2008-2010

Figure 1



Frauds are categorised by CIFAS Members when they are recorded to the Staff Fraud Database. Each case can consist of one or more fraud types and, therefore, can be counted in more than one category. *Table 2* (overleaf) presents the numbers and types of fraud case recorded in 2009 and 2010, and the difference between the two years. >

Types of Staff Frauds Recorded 2009-2010

Table 2

Fraud Type	2009	2010	% change
Account Fraud	38	**40**	5%
Dishonest action by staff to obtain a benefit by theft or deception	215	**153**	-29%
Employment application fraud (successful)	13	**14**	8%
Employment application fraud (unsuccessful)	50	**85**	70%
Unlawful obtaining or disclosure of commercial data	3	**1**	-67%
Unlawful obtaining or disclosure of personal data	32	**52**	63%
Total	**351**	**345**	**-2%**

The most notable aspect was the 70% increase in the number of unsuccessful employment application frauds. These were identified at the pre-employment stage. This is where Members have identified frauds in the candidate's employment application before recruitment has been completed: e.g. where a person falsely claims that he or she is professionally qualified where the qualification is a prerequisite. In addition, the number of 'successful' application frauds increased by 8%. These occurred where either initial checks had not identified frauds but later scrutiny revealed them, or when a person commenced employment before the relevant checks were returned.

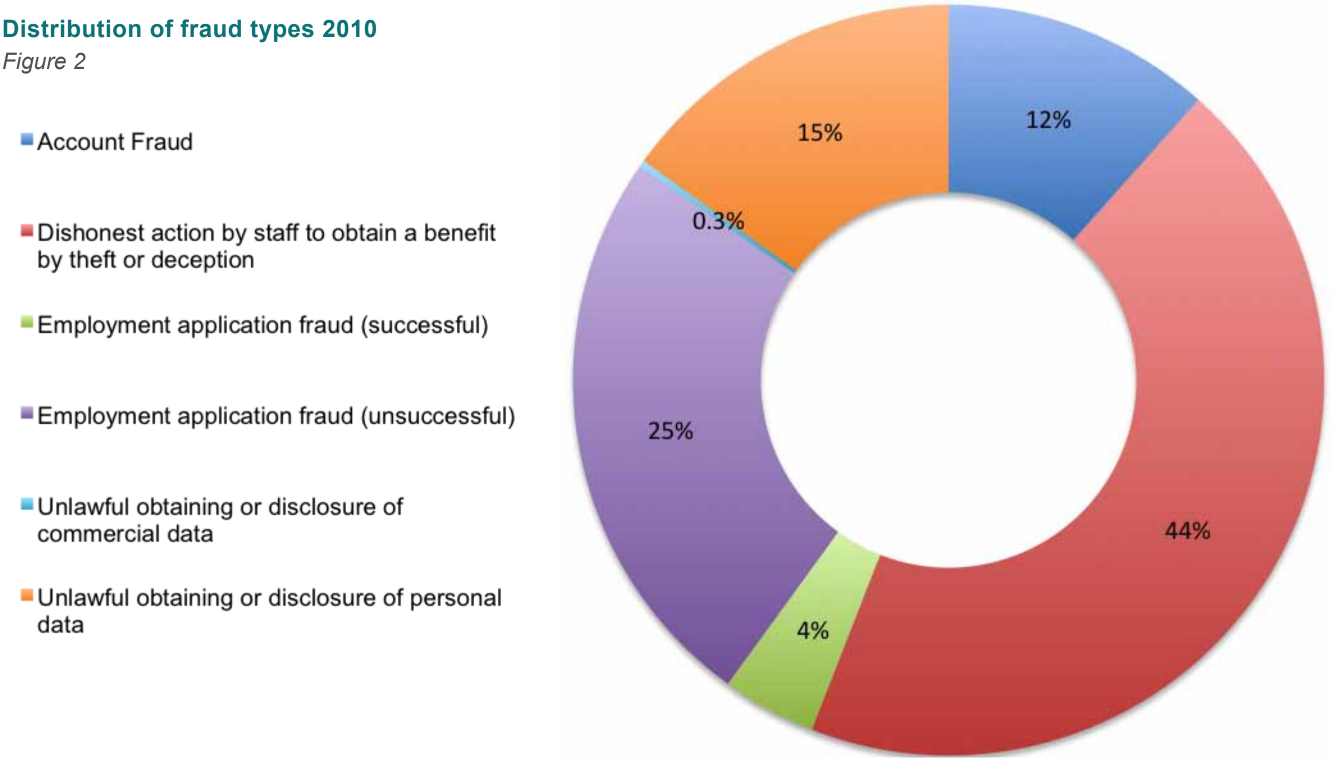
Another substantial increase was in the category 'unlawful obtaining or disclosure of personal data' which showed an increase of 63%. These frauds involve the manipulation of customer accounts, and can often be linked to organised criminal gangs.

The fraud type 'dishonest action by staff to obtain a benefit by theft or deception' (hereafter referred to as 'dishonest action') remained the most common fraud type recorded. However, this category actually decreased by 29% in 2010, when compared with 2009.

Figure 2 shows that while dishonest action remained the most prevalent fraud type, the proportion reduced so that it now accounted for less than a half of all frauds. Unsuccessful employment application fraud accounted for one quarter of all fraud types. ●

Distribution of fraud types 2010

Figure 2



3. 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 number of reasons (called 'Reasons for filing') and these provide a greater insight into the nature of the frauds perpetrated in 2010. 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 *Table 2* (page 6) and the percentage totals in Section 3 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.

Most common reasons for filing Account Frauds 2010

Table 3

	2009		2010		
Reasons for Filing	**Number of Cases**	**% of Total**	**Number of Cases**	**% of Total**	**% change**
Fraudulent account withdrawal	22	49%	**21**	**44%**	-5%
Fraudulent account transfer to third party account	14	31%	**20**	**42%**	43%
Fraudulent account transfer to employee account	9	20%	**7**	**15%**	-22%

Overall, account fraud increased by 5% compared with 2009. *Table 3* shows that fraudulent account withdrawal (where the fraudster stole from a customer's account) was again the most common offence. However this decreased slightly, together with a drop in the proportion of employees identified as transferring money to their own account. Despite these decreases, more of these types of fraud were reported by customers rather than through internal controls (19 cases compared with 12 in 2009).

The number of frauds linked with an account transfer to a third party account increased by 43% and accounted for 20 cases in 2010. Of these, five cases were identified by means of internal controls/audit compared with just one case in 2009. The numbers reported by customers remained static (eight cases).

For all types of account fraud, all fraudsters identified by internal controls were dismissed. For those identified by customers, 57% were dismissed with the remainder resigning either before or during an investigation. Where a fraud is identified by a customer, this indicates that staff fraudsters are gaining knowledge about the internal controls of organisations and are managing to bypass them, or that the internal controls do not exist.

The benefit of data sharing on the Staff Fraud Database means, for example, that the remaining 43% of fraudsters identified by customers, who resigned before dismissal, can be identified at job application stage if they then apply to work for another Staff Fraud Member. ●

3.2 Dishonest action 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.

Most common reasons for filing 'Dishonest Action' Frauds 2010

Table 4

	2009		2010		
Reasons for Filing	**Number of Cases**	**% of Total**	**Number of Cases**	**% of Total**	**% change**
Theft of cash from customer	80	27%	**54**	**28%**	-33%
Theft of cash from employer	31	11%	**37**	**19%**	19%
Facilitating fraudulent applications	36	12%	**16**	**8%**	-56%
Facilitating transaction fraud	12	4%	**15**	**8%**	25%
Manipulation of a third party account	20	7%	**14**	**7%**	-30%
Manipulation of applications/proposals/claims	33	11%	**10**	**5%**	-70%
Manipulation of personal account	16	5%	**7**	**4%**	-56%

The number of dishonest action frauds decreased by 29% in 2010 compared with 2009, suggesting that staff are increasingly of the opinion that such frauds are not worth the risk of losing their jobs. *Table 4* shows that the most common types recorded were theft of cash either from customers or employers. The number recorded as theft from customers was lower than in 2009, although this group still accounted for 28% of cases. These frauds involved an employee stealing cash from a customer. An example would be where a customer deposits £150 cash into an account but the member of staff steals £20 and deposits the rest. Perhaps unsurprisingly, 81% of these frauds were identified by the customer, compared with 74% in 2009.

The number of employees recorded for the theft of cash from their employer increased by 19% in 2010. Offences most commonly involved taking cash from a till float. Interestingly, a lower number were identified by internal controls or audits (15 compared with 20 in 2009), with higher numbers identified by staff and customers (18 combined, compared with nine in 2009). This demonstrates that Staff Fraud Members have implemented good anti-fraud cultures in their organisations within the cash transaction environment (both for staff and customers). Consequently, both customers and staff have identified more fraud and have also been more willing to report it.

> "Dishonest action frauds decreased by 29% in 2010, suggesting that staff are increasingly of the opinion that such frauds are not worth the risk of losing their jobs."

Increases in incidents of theft in 2009 were attributed either to employees being driven to desperate measures to make ends meet during the recession, or simply to greed. This pattern was repeated in 2010 and there is no indication that this will change. In evaluating their investigations, Staff Fraud

>

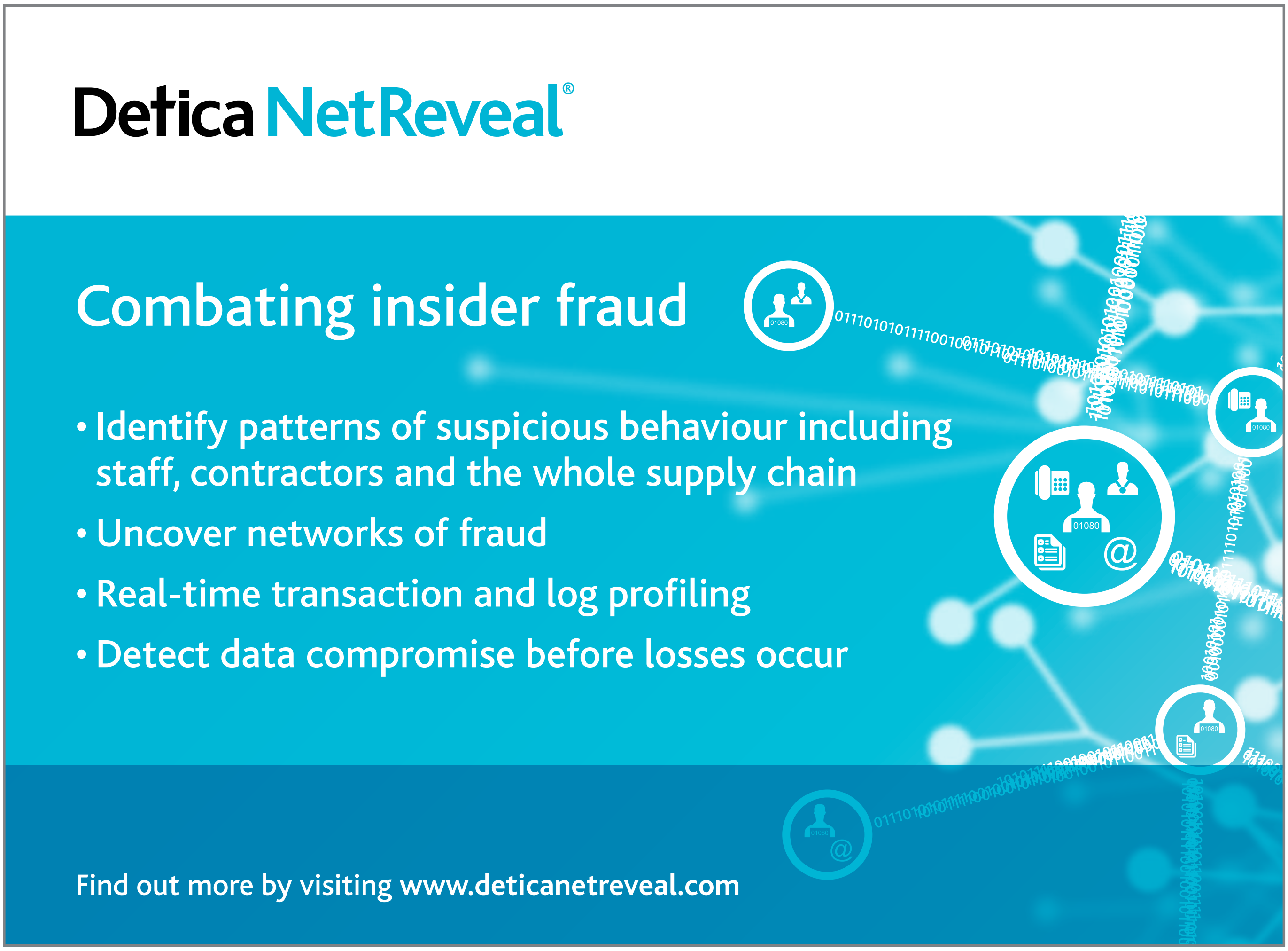
Members have identified that the rising debt of employees can also result from the increased use of online gambling. More cases of theft are therefore likely as online gambling increases.

Another motivation is that, with budget cuts leading to redundancies or potential redundancies, there are more disengaged employees who question not only their own, but also senior management's, commitment to the organisation. Where people fear that they are going to lose their jobs, it might seem that it would make little difference if they were dismissed. They may, therefore, consider that committing fraud would be worth the chance. This is of course counterbalanced by the obverse – those who fear that they won't be able to get another job and that it is not worth the risk.

There were decreases across most instances of manipulating or facilitating fraud on accounts (e.g. a staff member manipulating a process in order to guarantee a successful outcome for a friend). The most notable decrease was in the manipulation of applications/proposals/claims which decreased by 70%, accounting for just 10 frauds in 2010.

However, there was a 25% increase in the number identified as facilitating transaction fraud. Examples of this included a member of staff knowingly accepting false identity documents to support fraudulent transactions and facilitating transactions on stolen/counterfeit cards or altered financial instruments such as cheques.

Following the pattern noted in 2009, there was a continued decrease in the number of people identified as removing charges from a third party account, or manipulating bonus and reward schemes. This represents an improvement and suggests that increasing numbers of checks are being put in place by organisations. The current economic climate, however, remains the most obvious reason for this decrease – due to the lower prevalence of bonuses or reward schemes that are currently paying out and, therefore, being open to potential abuse.



3.3 Employment application fraud (successful)

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.

Most common reasons for filing Successful Employment Application Frauds 2010

Table 5

	2009		2010		
Reasons for Filing	**Number of Cases**	**% of Total**	**Number of Cases**	**% of Total**	**% change**
Concealed employment history	2	12%	**8**	**44%**	300%
Concealed employment record	1	6%	**3**	**17%**	200%
False documents	1	6%	**3**	**17%**	200%
Concealed unspent criminal convictions	7	41 %	**2**	**11%**	-71%

The number of successful employment application frauds was low, increasing by just one fraud in 2010, giving a total of 14 for the year. The low figures make it difficult to provide meaningful analysis when looking at different reasons why such frauds were recorded.

Table 5 shows that these frauds were filed mainly for ‘concealing employment history’ which accounted for eight cases (44%). This marked a difference from the figures in 2009 when this accounted for just two frauds. Conversely, the most common reason in 2009 was the concealment of unspent criminal convictions. By 2010, this was the reason for just two cases.

These changes are indicative of the current competitive job market – with people increasingly willing to try and conceal any fraudulent or other criminal history. This also serves as a further reminder of the necessity for organisations to carry out all possible checks before employment is offered. ●

Box A: DEFINITIONS

Concealed employment history

The identification of an application, either for employment or to provide services, in which the applicant conceals his or her employment history in a way that is considered a serious **material** falsehood (e.g. a period of time in a previous position).

Concealed employment record

The identification of an application, either for employment or to provide services, in which the applicant conceals his or her employment record in a way that is considered a serious **material** falsehood (e.g. claimed resignation when dismissed for fraud).

3.4 Employment application fraud (unsuccessful)

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.

Most common reasons for filing Unsuccessful Employment Application Frauds 2010
Table 6

	2009		2010		
Reasons for Filing	**Number of Cases**	**% of Total**	**Number of Cases**	**% of Total**	**% change**
Concealed adverse credit history	24	43%	**31**	**31%**	29%
Concealed employment history	8	14%	**20**	**20%**	150%
Concealed employment record	12	21%	**20**	**20%**	67%
Concealed unspent criminal convictions	1	2%	**20**	**20%**	1900%
False documents	4	7%	**4**	**4%**	0%

There was a 70% increase in unsuccessful employment application fraud in 2010. This rise is likely to be due to a combination of: (a) more people committing fraud by making false representations or statements on application forms in order to get a job; (b) increased checks carried out by employers prior to employment.[1]

> “Concealed unspent criminal convictions’ increased from just one case in 2009 to 20 cases in 2010.”

Table 6 shows that the most common reason for recording a fraud of this type was that the applicant concealed an adverse credit history (where this was a key consideration for the job). This involved applicants omitting or falsifying previous addresses in order to conceal past address histories. There were also increases in the number who covered up past employment information such as their employment history or employment record (see Box A – page 10 – for definitions of employment histories and records). These tended to be attempts to claim (falsely) that the applicant had the relevant experience for a post, or to conceal a previous dismissal for gross misconduct, for example for fraud. Concealed employment histories and records involved individuals who had been dismissed from previous work and who attempted to cover this either by not mentioning the employment, or by altering the dates during which they claimed to have worked there. There is a perception that fraudsters can be ‘clever’ and are willing to explore different avenues to deceive in order to gain employment. However, one individual actually re-applied to a large organisation from which they had previously been dismissed!

The number of ‘concealed unspent criminal convictions’ increased from just one case in 2009 to 20 cases in 2010. As this cannot be directly attributed to a sudden upsurge in crime (a decrease in crime was reported during 2010[2]), it is likely to be as a result of organisations running checks, such as those through the Criminal Records Bureau (CRB), before the prospective employee started in the post. This is a sign that organisations are increasingly willing to invest in pre-employment checks, including scrutinising applicants for all roles in an organisation where previously only senior roles might have been screened. ●

[1] Powerchex (2010) *The Powerchex annual pre-employment screening survey 2010.*

[2] Home Office (2011) *Crime in England and Wales: Quarterly Update to September 2010*. London: Home Office.

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

Reasons for filing 'Unlawful obtaining or disclosure of personal data' frauds 2010
Table 7

	2009		2010		
Resons for Filing	**Number of Cases**	**% of Total**	**Number of Cases**	**% of Total**	**% change**
Disclosure of customer data to a third party	20	56%	**39**	**56%**	95%
Fraudulent personal use of customer data	5	14%	**17**	**24%**	240%
Modification of customer payment instructions	1	3%	**4**	**6%**	300%
Unauthorised alterations to customer data	2	6%	**4**	**6%**	100%

A 63% increase in frauds relating to the disclosure of personal information took place, with *Table 7* showing increases across the majority of reasons for filing. The disclosure of customer data to a third party has continued to increase (by 95%) following an increase in 2009 compared with 2008. This reason still accounted for over a half of all these frauds, which often involved employees who knowingly assisted external fraudsters by providing them with a number of confidential customer account details. It should be noted that these frauds do not include people who were coerced into committing fraud (for example, by criminal gangs using threats of violence): in each case the fraudsters chose to perpetrate the fraud. Legally, committing an offence under duress is a common law defence, which means that they cannot be prosecuted.

Another noteworthy increase was in the fraudulent personal use of customer data which accounted for nearly one quarter of these types of fraud. Undoubtedly, this is a symptom of individual fraudsters being increasingly aware of the value of personal data and being willing to attempt to use, or sell, the data themselves. ●

Why do fraudsters commit fraud?

Donald R. Cressey, an American criminologist, devised a theory for the triggers that lead employees to commit fraud. The three aspects of pressure, opportunity and rationalisation became known as the 'Fraud Triangle'. CIFAS Staff Fraud Members have actively participated in discussions to share their expertise in how these triggers are seen in the workplace.

The aim of internal controls is to minimise opportunities and remove the incentives from potential fraudsters. Members therefore focused on sharing information on pressures and opportunities (as opposed to rationalisations), as it is those factors on which improved internal controls will have most impact.

Pressure

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

Examples:

- **Personal problems** – a common reason cited for members of staff turning to fraudulent activity. This covers a wide number of issues such as debt, domestic and other financial costs:
    - Debts – (particularly those which could be linked to gambling or drug addiction) may not be covered by the staff member's salary. In addition, if such debts need to be repaid within a strict timescale, this could lead the staff member to consider other ways to obtain the money required.
    - Domestic issues – for example, pressures attributed to divorce or child maintenance payments, or family pressure to bring in a higher income, could be crucial factors.
    - Financial – increasingly high costs of living could also be a major influence. If employees are struggling to pay bills, they may seek to acquire the funds by another means.

- **Greed** – This is, put simply, an employee's desire to fund a lifestyle that he or she is not able to afford. Recent research has indicated that a higher percentage of fraud is committed as a result of greed and to fund lavish lifestyles than any other motive[3].

- **Fear of unemployment** – the current economic climate has led employees to fear that their jobs could be at risk and that it may be difficult to obtain further employment. In addition, increased managerial pressure on individuals to meet targets – and thereby remain employed – can lead to members of staff looking for other ways to achieve them. For example, a mortgage salesman might alter a customer application to show that the customer earns more salary than he or she actually does. This would lead to the customer obtaining a higher mortgage and, in turn, the employee could receive a higher commission. This could also lead them to achieve higher targets than other, more honest members of staff, leading to the fraudster keeping his or her job, whereas others with lower sales lose theirs.

- **Malice/revenge** – disgruntled employees may see committing internal fraud against an employer as a way of getting 'revenge' for low pay or being passed over for promotion. Personal differences with management could also lead to staff wanting to harm or damage the employer deliberately in some way. Another factor in this could be company redundancies. If an employee knows, or believes, that he or she is being made redundant, they may set out deliberately to conduct fraudulent activity; not just to obtain a benefit themselves, but because they want to retaliate by damaging the employer. **>**

[3] *BDO Fraudtrack 7 (April 2010)*. Available online at http://www.bdo.uk.com.

Opportunity

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

Examples:

- **Weak internal controls** – this is a major factor in facilitating fraud. For example, if there is only one staff member who deals with accounts or invoicing, there is more opportunity for embezzlement. Such opportunities would be reduced by implementing dual controls such as having a senior staff member checking and signing off transactions.

- **Lack of clear policy and procedures** – If there is no clear policy in place, then there will be no fear of exposure or reprisal. If there is not a demonstrable standard of what constitutes acceptable behaviour, then a staff member could rationalise that they did not believe that the activities they were undertaking were unacceptable. Clear and concise policies are vital.

- **Poor security** – lack of physical security, e.g. lack of CCTV surveillance or computer passwords, may lead to opportunities for staff to steal. Individuals are more likely to commit fraud if they are confident that they will not be caught.

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

CIFAS
The UK's Fraud Prevention Service
BTG Intelligence
Dealing with
Deception
Thursday 7 July 2011
Visit www.cifas.org.uk/training_services for more information

4. Demographics

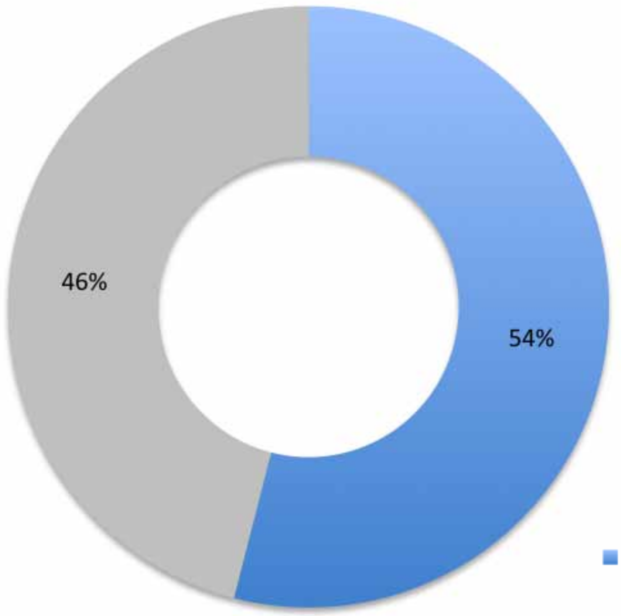
This section provides information about the individuals identified as having perpetrated staff frauds in 2010. When a case is recorded to the Staff Fraud Database, Members can also record demographic information such as gender and date of birth.

4.1 Gender

Figures 3 and *4* show the gender of the working population for the last quarter of 2010[4] compared with of staff fraudsters for 2010. For those whose gender is recorded, the majority of staff fraudsters in 2010 were male (62%), with females accounting for 38%. It is clear that males account for a higher proportion of staff fraud than might be expected, given that the ratio of males to females in the working population is far more even.

Gender of working population October – December 2010

Figure 3



Gender of staff fraudsters 2010

Figure 4

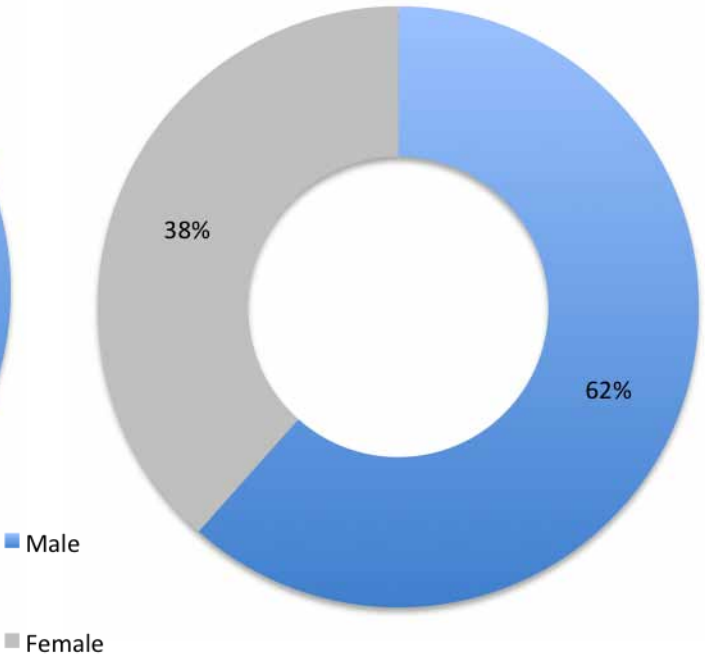


Table 8 (overleaf) presents the proportions of males and females for each fraud type. It shows that while males account for a higher proportion of all fraud types, females account for a higher than average percentage of dishonest action cases and a lower proportion of employment application frauds. >

[4] Working population figures are taken from the report *Office of National Statistics (2011) Labour Market Statistics*, February 2011. Available on http://www.statistics.gov.uk/pdfdir/lmsuk0211.pdf. The figure counts both full time and part time workers.

The breakdown of gender across case types is very similar to 2009. While there are noticeable differences in successful employment application fraud and commercial data-related fraud, the figures in these categories are low. The most notable change is that of personal data disclosure; where females accounted for 43% of frauds in 2010 compared with just 33% in 2009.

Breakdown of fraud type by gender 2009 and 2010

Table 8

	2009		2010	
Fraud Type	**Females**	**Males**	**Females**	**Males**
Account Fraud	40%	60%	39%	61%
Dishonest action by staff to obtain a benefit by theft or deception	45%	55%	45%	55%
Employment application fraud (successful)	20%	80%	30%	70%
Employment application fraud (unsuccessful)	23%	77%	24%	76%
Unlawful obtaining or disclosure of commercial data	0%	100%	100%	0%
Unlawful obtaining or disclosure of personal data	33%	67%	43%	57%
Overall	**38%**	**62%**	**38%**	**62%**

Table 9 presents information on the breakdown of cases by fraud type for each gender.

Gender of fraudsters by fraud type 2010

Table 9

Fraud Type	Females	Males	Overall
Account Fraud	11%	12%	12%
Dishonest action by staff to obtain a benefit by theft or deception	53%	41%	44%
Employment application fraud (successful)	2%	4%	4%
Employment application fraud (unsuccessful)	15%	28%	25%
Unlawful obtaining or disclosure of commercial data	1%	0%	0%
Unlawful obtaining or disclosure of personal data	18%	15%	15%

Over half of the frauds committed by females are attributed to dishonest actions through theft or deception. Moreover, female staff fraudsters have committed a disproportionate percentage of data theft frauds.

A noticeable proportion (41%) of male fraudsters commit dishonest actions through theft or deception. Furthermore, male fraudsters commit more unsuccessful employment application frauds than the overall average. This is a noticeable increase on the 19% seen in 2009.

Compared with 2009, females have committed higher proportions of unsuccessful employment fraud, and frauds related to disclosing personal data. ●

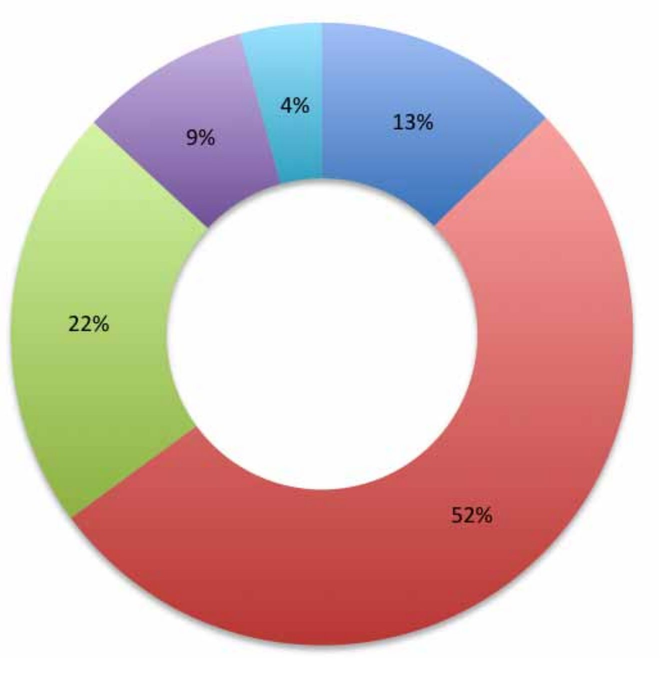
4.2 Age

The average age of a staff fraudster in 2010 was 30 years old. However, the data for 2010 showed a diverse picture, with staff fraudsters across a wide range of age groups.

Figures 5 and *6* show the breakdown of the age group of staff fraudsters for 2009 and 2010. Over half were in the age group ’21-30’ with the next largest group being ’31-40’.

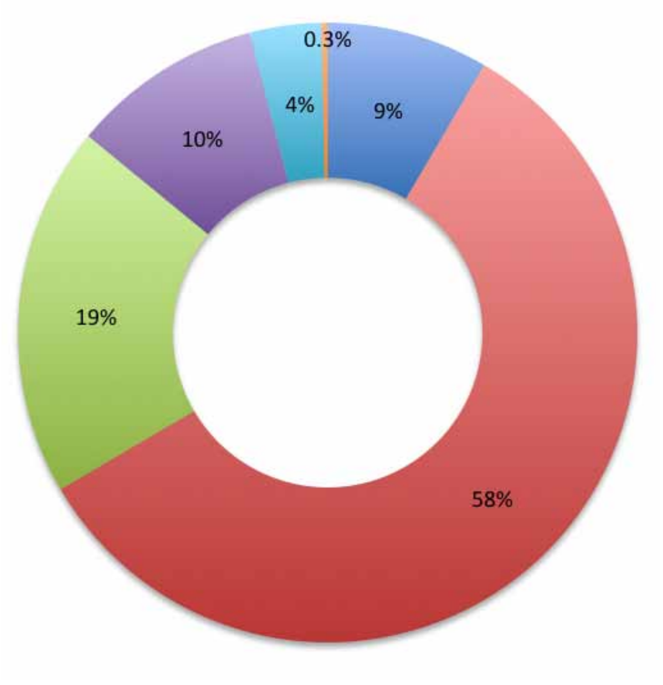
Staff Fraudsters by Age Group 2009

Figure 5



Staff Fraudsters by Age Group 2010

Figure 6



The breakdown is fairly similar to the pattern seen in 2009, with the exceptions being a decrease in the numbers under 21, and an increase in the ’21-30’ age group. It is possible that the move away from the very youngest age group is a reflection of the increase in youth unemployment noted in 2010[5]. *Figure 7* overleaf presents data on the age distribution of fraudsters across the different fraud types (bearing in mind that the age group 60+ had just one person in it). There were some differences in the types of frauds associated with the various age groups. The pattern for the youngest age group of ‘under 21’ was different from older age groups; with disclosing personal data accounting for 29% of all the frauds committed by those under 21; the highest proportion for any age group. Account fraud was also high for this group, at 26% of all the frauds associated with those ‘under 21’. These types of frauds are more likely to >

29% of all frauds committed by those under 21 was for ‘disclosing personal data’; the highest proportion for any age group

[5] ibid http://www.statistics.gov.uk/pdfdir/lmsuk0211.pdf

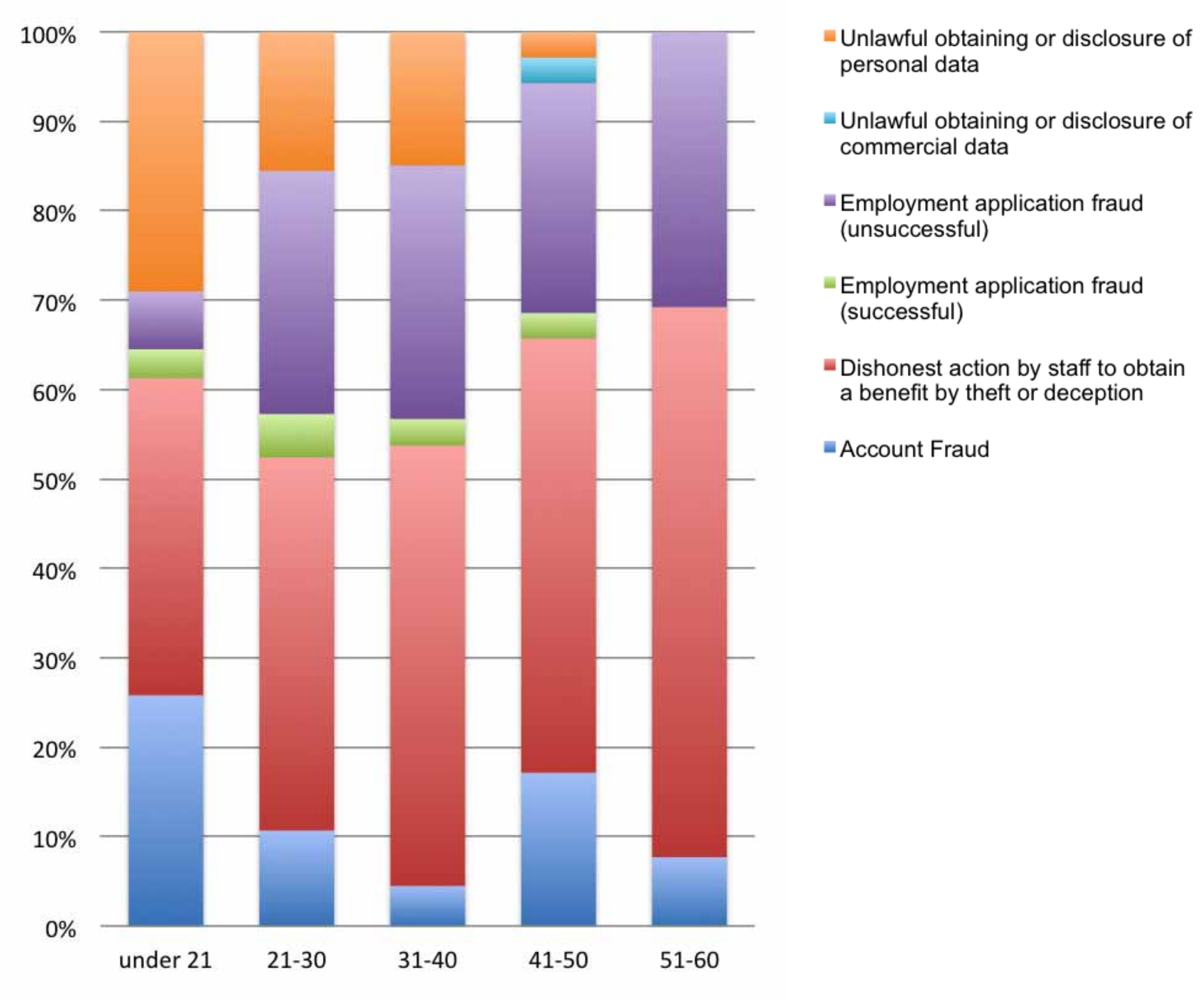
be associated with further criminality and the data suggests that younger people were being targeted more successfully by organised criminals, possibly due to their clean employment history. The younger members of staff may succumb to these approaches because of particular economic pressures affecting this age group, such as worsening employment prospects and lack of salary rises.

For both males and females in the 21-30 age group, approximately one quarter of all frauds were identified as dishonest actions through theft or deception. The proportion of frauds identified as 'dishonest action' tends to increase as the fraudster gets older. This may link to increased financial responsibilities through life, with the need to pay for mortgages, utility bills etc. However, the greed of a fraudster cannot be discounted as a reason for perpetrating fraud. Sometimes the reason is simply greed, no matter what age the person may be.

Figure 8 (opposite) shows that, for the younger age groups, males represent the majority of the fraudsters. However, for the age-groups 41-50 and 51-60 this evens out. Again the age group 60+ has just one staff fraudster in it. ●

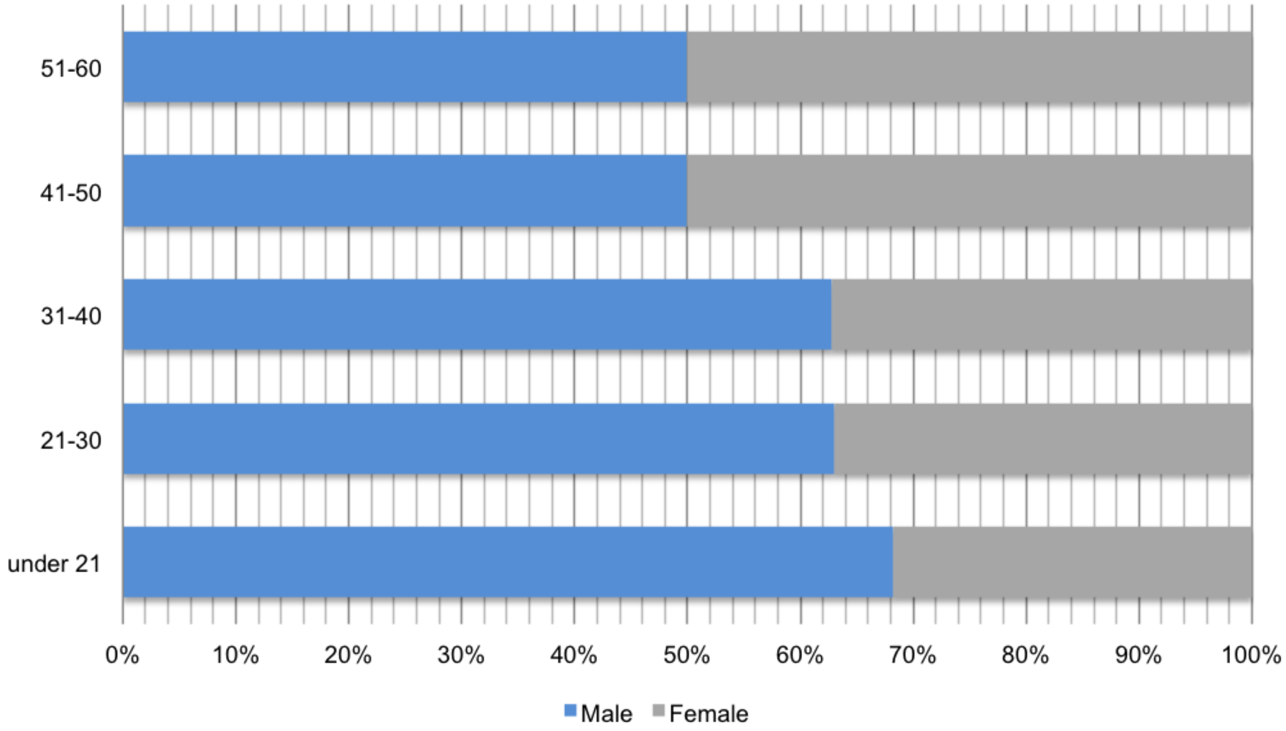
Age Group of staff fraudsters by case type 2010

Figure 7 *The 60+ age group had just one staff fraudster recorded



Age Group of staff fraudsters by gender 2010

Figure 8 *The 60+ age group had just one staff fraudster recorded



5. Employment details

This section provides information on the nature of the workplace where staff frauds were recorded and the length of time that the fraudster had worked for the company before the fraud was identified.

5.1 Business Area

Table 10 shows the business area that the member of staff worked in at the time the fraud was identified.

Business area of staff fraudsters in 2009 and 2010

Table 10

	2009		2010		
Business Area	**Number of Cases**	**% of Total**	**Number of Cases**	**% of Total**	**% change**
Branch/Retail outlet/Store	177	59%	**185**	**72%**	5%
Customer contact centre	73	24%	**49**	**19%**	- 33%
Field unit	25	8%	**9**	**4%**	- 64%
Finance department	3	1%	**0**	**0%**	- 100%
IT department	1	0%	**0**	**0%**	- 100%
Other	12	4%	**6**	**2%**	- 50%
Other support services	9	3%	**5**	**2%**	- 44%
Staff contact centre	0	0%	**2**	**1%**	100%

The number of staff frauds carried out by a person working in a branch/retail outlet or store increased again and represented 72% of all staff fraud cases in 2010. This was unsurprising given that the industries encompassed by this category were likely to involve employees having responsibility both for cash transactions and customer accounts. Much of the increase was in data theft cases recorded in branches, retail outlets or stores: these more than doubled to 40 cases in 2010.

All other areas of business saw a decrease, with customer contact centres dropping to less than one in five of all frauds. While this was (on the surface) encouraging, when looked at in more detail, 14% of the total associated with customer contact centres were successful employee application frauds. This was a relatively high proportion and indicates that these are organisations which are targeted by those who, for some reason, wish to hide an adverse history. Stringent vetting and tightened employment procedures are therefore increasingly important in these areas. In addition, the proportion of frauds identified as being associated with 'field units' (i.e. those who work in non-office based roles, such as regional insurance sales persons) dropped to just 4% of the total recorded. All of these frauds were associated with 'dishonest action', which may indicate that there is a perception by "field" staff that their work faces less scrutiny. ●

5.2 Length of service

Average length of service for a staff fraudster 2008 - 2010

Table 11

	2008	2009	2010
Average length of service (years)	1.6	4.3	5.5

Table 11 shows how long the fraudster was employed before the fraud was discovered. This does not indicate how long the person was committing fraud before discovery, simply the length of time that they worked for the employer.

The table shows that the average length of service for fraudsters was 5.5 years; a continuation of the increase seen in recent years.

To illustrate, there are three possible scenarios:

- Richard worked for Company A with a good employee record for 5.5 years and then committed a single fraud.
- Kate committed several frauds during her 5.5 years of employment at Company B. Recent improved internal controls brought these frauds to light.
- Dean worked for 5.5 years at Company C where the internal controls were well established. It has taken Dean this length of time to circumvent the systems.

Average length of service (in years) by fraud type 2008 - 2010

Table 12

Fraud Type	2008	2009	2010	No. of cases in 2010
Account Fraud	4.2	5.9	**6.4**	40
Dishonest action by staff to obtain a benefit by theft or deception	2.4	5.6	**6.3**	153
Employment application fraud (successful)	0.6	1.5	**0.4**	11
Unlawful obtaining or disclosure of commercial data	0.2	3.0	**8.5**	1
Unlawful obtaining or disclosure of personal data	2.0	2.1	**3.4**	52

While showing a general increase, the data in *Table 12* essentially follows the pattern presented in previous years. Those involved in account frauds and dishonest actions were employed for a longer period of time than those which might be connected to further criminality (such as disclosing personal data). This links to the idea previously proposed that people committing account and theft frauds were in difficult financial situations and committed these offences due to desperation, whereas others were simply greedy, wanting to fund a lavish lifestyle.

While it cannot be discounted that some of these fraudsters may have been committing fraud against their employer for some time before being discovered, some may also have previously been lawfully employed before turning to fraud.

Furthermore, it cannot be discounted that in the second half of 2010, many organisations were looking at restructuring which would lead to redundancies. This may have led to disenchanted employees who, despite no previous offences, thought that they had nothing to lose. It is increasingly important for companies to have good staff support programmes in place to assist those in difficult financial circumstances and those facing redundancy.

Where systematic fraud takes place, Staff Fraud Members acknowledge that this is likely to be perpetrated by those who >

> “Where systematic fraud takes place, Staff Fraud Members acknowledge that this is likely to be perpetrated by those who have been employed for a long time. This is because only those staff will be sufficiently familiar with the internal controls.”

have been employed for a long time. This is because only those staff will be sufficiently familiar with the internal controls.

On the other hand, those who disclosed personal data could have been placed in the post specifically to commit fraud by organised criminals or have been targeted by these criminals once they were in post, with the associated pressure to get ‘results’ by committing frauds within a relatively short period of time.

The reduction in the length of service for those who committed successful employment application fraud is worth remarking upon and was, in a sense, positive. Although the number of cases is low, it shows that even if individuals start work before pre-employment checks were completed, once the fraud was uncovered it was acted upon quickly and decisively, and the person was removed at an earlier stage than in 2009. This reduces the window of opportunity for staff fraudsters to do any damage to their employer. ●

6. Identifying frauds and taking action

This section presents information on the means by which staff frauds were identified, how the fraudster left the organisation and the next steps taken by the CIFAS Staff Fraud Member organisations.

6.1 Means of discovery

Means by which staff frauds were identified 2009 and 2010
Table 13

	2009		2010		
Means of Discovery	**Number of Cases**	**% of Total**	**Number of Cases**	**% of Total**	**% change**
Customer	98	32%	**98**	**38%**	0%
Internal controls/audit	131	43%	**78**	**30%**	- 40%
Staff	34	11%	**38**	**15%**	12%
Other	12	4%	**26**	**10%**	117%
Staff (whistleblowing)	11	4%	**9**	**4%**	- 18%
Law enforcement	16	5%	**8**	**3%**	- 50%

Table 13 shows that the proportion of cases where the customer reported fraud increased in 2010, and accounted for 38% of all frauds identified. More than half of the account frauds recorded were discovered by customers. This was likely to be a continuation of the trend identified in 2009 whereby the increase in account frauds, directly impacting customers, were not surprisingly first reported by the customer; who was, of course, the person most likely to note any discrepancies on their account.

Discovery by internal controls or audit continued to decrease from 63% in 2008, 43% in 2009 and 30% in 2010. Almost two thirds of frauds identified in this way were for 'dishonest action'; demonstrating the importance of monitoring the success of internal controls. For example, implementing controls (such as strengthening the restrictions to computer access levels, segregation of duties, random validation checks and employee monitoring) allows a 'before and after' verification to take place. This type of consistent monitoring enables organisations to adapt their methods and controls constantly in order to counter evolving threats.

A noticeable increase was in the number of frauds identified by 'other' methods (such as members of the public or a regulator) which accounted for 10% of all frauds.

The number reported by staff remained fairly stable with a small increase. This shows that more fraud was identified by chance, e.g. by staff who identified a discrepancy in a colleague's work. This shows the value of the minimum two-week annual leave policy (which is commonplace in many organisations), segregation of duties and job rotation. However, there was a small decrease in the number identified by staff (whistleblowing) e.g. those who notified a fraud anonymously through a whistleblowing hotline. To compare and contrast with figures reported from public sector organisations, 26% of internal and external frauds were identified through whistleblowing[6]. For Staff Fraud Members, who are currently all in the private sector, whistleblowing remains one of the least frequent means of discovery and serves as a reminder for organisations to have a whistleblowing policy that staff are aware of and know how to use. ●

[6] http://www.pwc.co.uk/eng/publications/cutting-costs-and-cutting-fraud.html

6.2 Reason for leaving

Following the reporting or discovery of a suspected fraud within a company, a CIFAS Staff Fraud Member will carry out an internal investigation. On completion of the investigation, if enough evidence is found, the fraudster will be dismissed. An employee, however, can resign at any time, including during an investigation. *Table 14* presents information about how the fraudster left the relevant organisation during the last three years.

How the fraudster left the organisation 2008-2010

Table 14

	Dismissed		Resigned during Investigation		Resigned	
	Number of Cases	% of Total	Number of Cases	% of Total	Number of Cases	% of Total
2008	100	77%	20	15%	10	8%
2009	187	67%	63	23%	30	11%
2010	**141**	**60%**	**77**	**33%**	**16**	**7%**

* in addition, one fraud had a leaving reason of 'redundancy' in 2008

Table 14 shows that, over the last three years, there was a notable increase in the number of fraudsters who resigned while an investigation was continuing. This accounts for one third of all the fraudsters whose means of leaving was identified in 2010. There were corresponding decreases in the proportion of those who were dismissed or resigned. This shows that fraudsters were far less likely to hang around once the investigation had begun than in previous years. Either they were aware that the evidence trail would leave no doubt, or they thought it was more likely that they would secure further employment if there was no dismissal on their employment record.

Presenting information on the associated case types, *Table 15* shows that the higher proportion of those who resigned during an investigation was evident across the majority of case types. The only anomaly was in successful employment application fraud, where the increase in dismissals led to a corresponding decrease in those who resigned during investigations. One reason for this could be that the investigation would be limited as a person could be dismissed if they had started in the post before negative employment checks had been returned. The overall lower figures for those who resigned points to fraudsters being willing to 'tough it out' to some extent, until perhaps the depth of the investigation was known. ●

Reasons for leaving by fraud type 2009 and 2010

Table 15

	Dismissed		Resigned during Investigation		Resigned	
Fraud Type	**2009**	**2010**	**2009**	**2010**	**2009**	**2010**
Account fraud	72%	**60%**	10%	**38%**	18%	**3%**
Dishonest action by staff to obtain a benefit by theft or deception	67%	**58%**	25%	**35%**	9%	**8%**
Employment application fraud (successful)	75%	**82%**	17%	**9%**	8%	**9%**
Unlawful obtaining or disclosure of commercial data	100%	**100%**	-	-	-	-
Unlawful obtaining or disclosure of personal data	73%	**67%**	18%	**27%**	9%	**6%**

6.3 Reported to the police

Frauds reported to the police 2008-2010

Table 16

	Not reported	Reported by Customer	Reported by Member	Reported by Other
2008	82%	0%	18%	0%
2009	68%	1%	28%	3%
2010	**73%**	**1%**	**23%**	**4%**

Table 16 shows that the majority of those committing staff frauds were not reported to the police. However, in 2010 a total of 88 frauds were reported by a variety of means. Where frauds were reported, this was primarily by the Member organisation, with smaller numbers being reported by customers and by other interested parties. The low figures reported to the police reinforces the importance to Members of the Staff Fraud Database. Without this knowledge of fraudsters' previous activities, 73% of those who committed staff fraud in 2010 could be working in another organisation and continuing to commit fraud.

Table 17 presents the breakdown of the types of frauds which were reported in 2010.

Frauds reported to the police by fraud type 2009 and 2010

Table 17

	Not reported		Reported by Customer		Reported by Member		Reported by Other	
Fraud Type	**2009**	**2010**	**2009**	**2010**	**2009**	**2010**	**2009**	**2010**
Account Fraud	51%	**53%**	-	**3%**	44%	**35%**	5%	**10%**
Dishonest action by staff to obtain a benefit by theft or deception	73%	**62%**	-	**1%**	25%	**31%**	1%	**6%**
Employment application fraud (successful)	62%	**93%**	-	-	23%	-	15%	**7%**
Employment application fraud (unsuccessful)	100%	**100%**	-	-	-	-	-	-
Unlawful obtaining or disclosure of commercial data	67%	**100%**	-	-	33%	-	-	-
Unlawful obtaining or disclosure of personal data	52%	**63%**	3%	-	33%	**33%**	12%	**4%**

While, overall, the levels of reporting to the police are falling, there was a different pattern for cases involving dishonest action and account frauds. There were notable increases in the proportions of frauds reported by Members and by others, together with some of these frauds being reported by customers. ●

6.4 Convictions

What is reported in *Staff Fraudscape* is the result of responsible employers fighting fraud for the greater good. Of the cases filed to the database, many (as mentioned in section 6.3) are not reported to the police, but a number of fraud cases are brought to trial each year. These cases can take some time to prepare and so cases in court in 2010 could first have been recorded to the Staff Fraud Database in previous years.

A total of 15 frauds were recorded as resulting in a 'guilty' verdict in 2010. The majority of these cases were 'dishonest action and theft' cases (87%) with a smaller proportion being account fraud (13%).

As of the end of 2010, a further 33 cases were marked as awaiting trial, and 12 of these cases were first recorded in 2010. These cases covered a wider variety of frauds with just fewer than half being dishonest action and theft cases, and approximately a quarter each being account fraud (25%) and disclosing data (26%).

The reality is that, in the meantime, these fraudsters could be working for an organisation that is not a Member of the Staff Fraud Database and, with a case often taking up to 18 months to get to trial, tackling the movement of fraudsters remains a serious issue.

In addition, it cannot be overstated: fraud is a serious crime, as the following real-life examples of cases filed to the Staff Fraud Database that resulted in convictions in 2010 demonstrate.

Example Case 1:
A 53 year old Bank Manager stole £140,000 over a period of three years. She stole the money to help fund her husband's failing landscape gardening business. She had worked for the bank for 30 years. The fraud was discovered by a customer who noticed money was missing from her account. She received a 20 month sentence.

Example Case 2:
A female employee stole £120,000 over four years while working as a customer adviser for a bank. She originally stole money to help pay for her ill mother's mortgage. This then led to her stealing money to fund her greed for holidays abroad, clothes and furniture.

Example Case 3:
A Financial Adviser stole thousands of pounds from customers to help fund his own property development company. He was granted unconditional bail.

Example Case 4:
A former law student stole £65,000 while working at a call centre for a mobile phone company. He was given a two-year jail sentence.

CIFAS Staff Fraud Adviser, Arjun Medhi, concludes: "It goes without saying that the vast majority of employees are trusted and reliable. The damage caused by the few bad apples, however, can cause serious financial consequences and unquantifiable damage to reputation and morale. Responsible actions, careful processes that weed out rogue employees (without punishing the majority of trusted staff) and secure data sharing about confirmed insider frauds are all steps that can be taken by organisations. This will help to uncover those staff fraudsters who – if left unchecked – will damage their organisations, hurt their friends and colleagues and cause further harm to the economy." ●

For further information, please contact our Staff Fraud Adviser and the Communications Team

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

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