Staff

FRAUDSCAPE

Depicting the UK's staff fraud landscape

www.cifas.org.uk | May 2010

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 265 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, which currently has over 130 Members sharing information on confirmed frauds that have been perpetrated against CIFAS Member organisations. 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 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 2008 and 2009, to ascertain any key differences between the typology of the frauds seen in 2009 compared with 2008. 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.

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

CIFAS

1. Introduction
by Peter Hurst, CIFAS Chief Executive

The majority of staff working for any organisation are hard-working, reliable and honest individuals. There is, however, an immense threat posed by the small proportion of staff who act dishonestly and defraud the organisation that they work for: abusing the trust placed in them by their employer, their colleagues and customers alike. This can range from compromising customer or payroll data to straightforward theft or the submission of inflated expenses; through to falsifying or failing to disclose all 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 from one employer to another unchallenged: exposing the new employer to the risk of further fraud.

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 launch of the CIFAS Staff Fraud Database in 2006 was carried out 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.

A CIFAS Staff Fraud Member organisation accesses 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 on 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.

Over 130 employers currenty share information in this way. 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 protect your organisation. The database is growing every year, is gathering momentum, and - for the first time - trends are emerging. *Staff Fraudscape* analyses the cases of staff fraud filed to the CIFAS Staff Fraud Database by participating organisations in 2008 and 2009. *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.

Questions are raised by *Staff Fraudscape*. For example, the overall increase of 45% in the number of cases filed to the database in 2009, compared with 2008: how much of this is attributable to otherwise honest employees driven to 'no other option' by the economic conditions of the last 24 months? On the other hand, is some of the increase linked to other, sinister and organised frauds? Does the increase in the average length of service of the staff fraudster since 2008 tell us anything significant? Alternatively, can patterns be identified regarding the gender or age of the fraudster and the types of fraud committed? The answers are not always obvious: but conclusions can be drawn.

Staff Fraudscape provides the authoritative insight to the staff frauds identified in 2009, and the trends and methods used to defraud organisations.

2. Staff Fraud Database - general trends

In 2009, nearly 45% more cases of staff fraud were recorded on the CIFAS Staff Fraud Database than in 2008.

Staff Fraud cases recorded by CIFAS Staff Fraud Members

Table 2.1

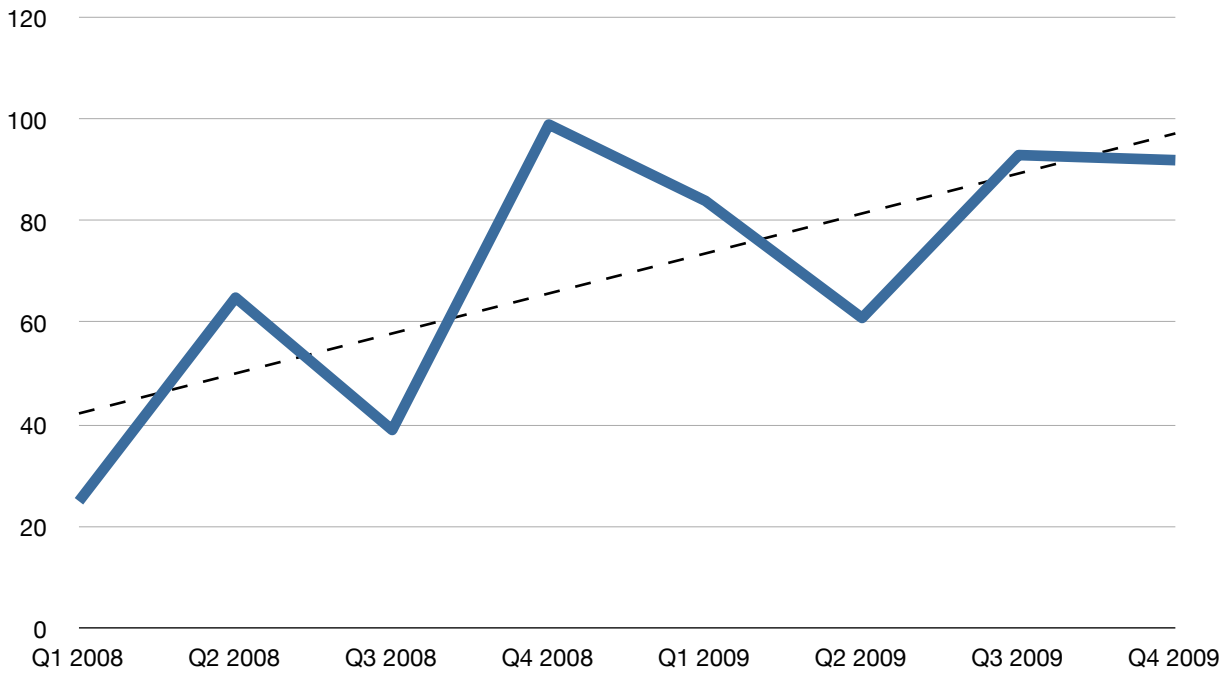
	2008	2009	% increase
Cases recorded	228	330	44.74%

The number of organisations using the CIFAS Staff Fraud Database also increased during 2009. There were 118 organisations participating in the database in 2008 and 128 by the end of 2009. This represents an increase of 8.5%, so the rise in the number of cases recorded on the database is significantly greater than the increase in the number of participating organisations.

Chart 2.1 shows the number of cases recorded in each quarter of 2008 and 2009, together with a trend line to illustrate the behaviour that underpins the figures. This shows that although there was significant quarter on quarter variation, the underlying trend was a steep increase.

Staff fraud cases recorded by quarter

Chart 2.1



The frauds identified are classified into various fraud types as follows (full definitions can be found throughout Section 3 - Specific Offences p 7 - 11):

Number of Staff Fraud types recorded

Table 2.2

	2008		2009		
Staff Fraud type	**Cases**	**% of total**	**Cases**	**% of total**	**% change**
Account fraud	13	5.53%	38	10.83%	192.31%
Dishonest action by staff to obtain a benefit by theft or deception	112	47.66%	215	61.25%	91.96%
Employment application fraud (successful)	10	4.26%	13	3.70%	30.00%
Employment application fraud (unsuccessful)	84	35.74%	50	14.25%	-40.48%
Unlawful obtaining or disclosure of commercial data	1	0.43%	3	0.85%	200.00%
Unlawful obtaining or disclosure of personal data	15	6.38%	32	9.12%	113.33%
Total Frauds	235		351		49.36%

Please note that cases can be filed under more than one fraud type, and (for each fraud type) more than one reason for filing can be recorded. This will explain the apparent discrepancies in numbers that can occasionally be seen, between the different tables, and why the percentage totals do not always add up to 100%.

In both 2008 and 2009, the most prevalent fraud type was 'dishonest action by staff to obtain a benefit by theft or deception', and the number of these cases almost doubled in 2009 compared with 2008. The second most common fraud type was 'unsuccessful employment application fraud' i.e. where the fraud was identified at job application stage. This type of fraud, however, decreased by over 40% in 2009 compared with 2008.

This decrease in the latter can be attributed largely to the economic conditions during the period: where organisations were more likely to be seeking to reduce headcount than increase it. When there are few jobs on offer, so there is less likelihood of employment application fraud. There were more successful employment application frauds identified in 2009 than in 2008, however, indicating that where procedures failed to identify the fraud at application stage, further scrutiny at a later date (possibly after grounds for further scrutiny had been identified) had uncovered the fraud.

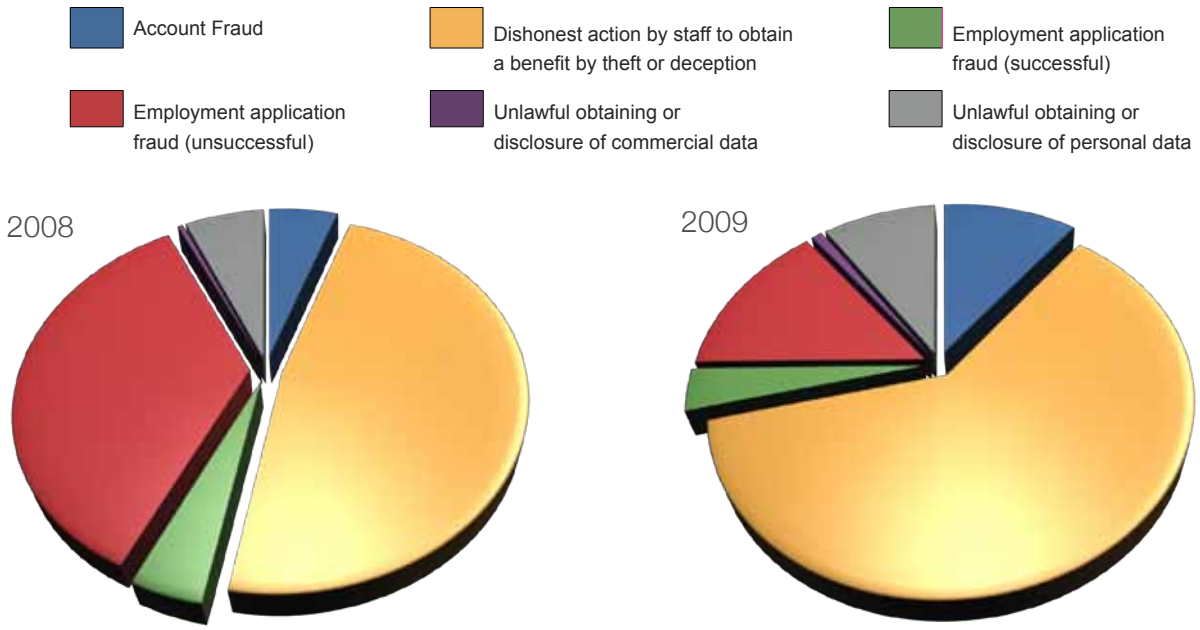
> "Cases of 'dishonest action by staff to obtain a benefit by theft or deception' almost doubled in 2009 compared with 2008."

There were similar increases in the number of instances of 'account fraud' and the 'unlawful obtaining or disclosure of personal data'. Both these types of fraud increased by over 100%, and both involved frauds against the organisation's customers, either through manipulation of their account or the compromise of their personal data.

These changes represent a significant shift in the types of staff fraud identified between 2008 and 2009, as seen in the pie charts overleaf.

Comparison of fraud type distribution between 2008 and 2009

Chart 2.2



3. Specific offences

This section looks more closely at the offences perpetrated by the fraudster, broken down by Staff Fraud type. A case can involve multiple offences (reasons for filing the case).

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 him/herself or others.

Reasons for filing

Table 3.1.1

	2008		2009		
Filing Reason	**Cases**	**% of total**	**Cases**	**% of total**	**% change**
Fraudulent account withdrawal	3	23.08%	22	48.89%	633.33%
Fraudulent account transfer to third party account	5	38.46%	14	31.11%	180.00%
Fraudulent account transfer to employee account	5	38.46%	9	20.00%	80.00%

In 2008, fraudulent account withdrawal was the least frequently identified offence, while in 2009 it was the most frequently identified. Fraudulent transfers (either to a third party account or to the employee's own account) both increased, but not as significantly. This may show that staff fraudsters were more wary of leaving an audit trail that would incriminate themselves or a collusive third party (or both), considering instead that their chances of going undetected would increase if they simply made a straight withdrawal. Equally, it may demonstrate that organisations have tightened controls, thereby identifying more account fraud than before.

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 him/herself and/or others through a dishonest action, and where such conduct would constitute an offence.

Reasons for filing

Table 3.2.1

	2008		2009		
Filing Reason	**Cases**	**% of total**	**Cases**	**% of total**	**% change**
Theft of cash from customer	12	9.60%	80	27.12%	566.67%
Facilitating fraudulent applications	6	4.80%	36	12.20%	500.00%
Manipulation of applications/proposals/ claims	1	0.80%	33	11.19%	3200.00%
Theft of cash from employer	17	13.60%	31	10.51%	82.35%
Manipulation of a third party account	19	15.20%	20	6.78%	5.26%
Manipulation of personal account	7	5.60%	16	5.42%	128.57%
Facilitating transaction fraud	11	8.80%	12	4.07%	9.09%
Removal of charges from personal account	8	6.40%	10	3.39%	25.00%
Removal of charges from third party account	15	12.00%	9	3.05%	-40.00%
Manipulation of bonus/reward scheme	13	10.40%	8	2.71%	-38.46%

In 2008, the most common offence in cases of dishonest actions by staff was the manipulation of third party accounts, but this dropped to only the fifth most commonly identified offence in 2009 (although the actual number of cases still increased). The most commonly identified offence in 2009 was the theft of cash from a customer. This accounted for over 27% of the cases, up from less than 10% in 2008. Some of these cases may have been driven purely by greed, but it is equally probable that some employees were driven to desperate measures to make ends meet in difficult economic times, despite the risk of dismissal if they were discovered. This also applies to the theft of cash from the employer, which almost doubled in 2009 compared with 2008. In times of recession or other economic difficulty - in order to minimise the likelihood of staff commiting fraud, organisations may wish to consider offering support, such as a free debt counselling service.

There were also substantial increases in the number of cases of employees either facilitating fraudulent applications or manipulating applications, proposals or claims. This may indicate an increase in the number of employees who were colluding with other parties in criminal activities. In the prevailing economic environment, credit and services were harder to come by and, therefore, applications may have required some 'help' to ensure their acceptance. For example, where applications are made using identity details derived from data compromised in bulk (which may be incomplete), an organised fraudster will increasingly look to 'insiders' to make sure that sufficient applications are accepted in order to maintain his or her criminal cashflow. Other cases within this fraud type will include employees attempting to assist friends or family making an application.

>

Interestingly, there has actually been a fall in the number of people who have been identified as removing charges from third party accounts or manipulating bonus or reward schemes. This may be due to bonus and reward schemes having been tightened to meet good governance requirements. Equally, this may be because of audit procedures that organisations have put in place to make it difficult for employees to perpetrate such frauds anonymously, and an awareness that being caught will result in disciplinary action, dismissal and being recorded on the Staff Fraud Database.

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.

Reasons for filing

Table 3.3.1

	2008		2009		
Filing Reason	**Cases**	**% of total**	**Cases**	**% of total**	**% change**
Concealed unspent criminal convictions	2	18.18%	7	41.18%	250.00%
Concealed employment history	1	9.09%	2	11.76%	100.00%
False references	1	9.09%	2	11.76%	100.00%
Concealed adverse credit history	3	27.27%	1	5.88%	-66.67%
Concealed employment record	0	0.00%	1	5.88%	-
False documents	1	9.09%	1	5.88%	0.00%
False immigration status	1	9.09%	1	5.88%	0.00%
False qualifications	2	18.18%	1	5.88%	-50.00%
Use of a false identity	0	0.00%	1	5.88%	-

The number of cases of successful employment application fraud is relatively low, so it is difficult to draw meaningful conclusions. It is, however, interesting that the most significant increase is in the number of cases where an employee failed to disclose, in his or her application, unspent criminal convictions. This may be due to employers who are unwilling to wait for the completion of Criminal Records Bureau (CRB) checks before the prospective employee starts in post. Such checks can be delayed by workloads at the CRB, so the employee starts the job before they have been completed, and it is only when the results are returned that the application fraud is discovered. This clearly suggests that, wherever possible, especially in less time sensitive positions, organisations should complete these checks prior to an employee's start date.

3.4 Employment application fraud (unsuccessful)

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

Reasons for filing

Table 3.4.1

	2008		2009		
Filing Reason	**Cases**	**% of total**	**Cases**	**% of total**	**% change**
Concealed adverse credit history	49	58.33%	24	42.86%	-104.17%
Concealed employment record	11	13.10%	12	21.43%	8.33%
Concealed employment history	7	8.33%	8	14.29%	12.50%
False references	4	4.76%	4	7.14%	0.00%
False documents	5	5.95%	4	7.14%	-25.00%
False immigration status	3	3.57%	2	3.57%	-50.00%
Concealed unspent criminal convictions	4	4.76%	1	1.79%	-300.00%
Use of a false identity	1	1.19%	1	1.79%	0.00%

The fall in the number of unsuccessful employment application frauds is likely to be due primarily to the reduction in recruitment. Within this, however, there has actually been an increase in the number of cases of people dishonestly making false statements about the dates that they were previously employed. This may be to make it appear that they have the required experience for a position, or to disguise a period of time when they were out of work, or in a post from which they were dismissed. False statements given in applications also included the circumstances of previous employment (such as candidates claiming that they left their previous employment to travel, when in fact they were dismissed).

These offences together accounted for over 35% of unsuccessful employment application frauds in 2009, compared with 21% in 2008. The most common offence was concealing an adverse credit history (where this is a key consideration for the job), and while the number of these cases halved in 2009, there were still twice as many as the next most common offence – concealed employment record.

> “In cases of unsuccessful employment application fraud, the most common reason for filing in 2009 was concealing an adverse credit history.”

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.

There was only one case of unlawfully obtaining or disclosing commercial data in 2008 and three in 2009. The case in 2008 involved the employee disclosing policies, practices and procedures to a third party, and the cases in 2009 involved two cases of contravention of a systems access policy and another case of disclosing internal practices to a third party. These frauds are rare, but a single case can be *severely* damaging to an organisation, both financially and reputationally. The low incidence of such frauds indicates that organisations have put good controls in place, designed to prevent theft and disclosure of commercial information and intellectual property.

Reasons for filing (personal data)

Table 3.5.1

	2008		2009		
Filing Reason	**Cases**	**% of total**	**Cases**	**% of total**	**% change**
Disclosure of customer data to a third party	11	50.00%	20	55.56%	45.00%
Fraudulent personal use of customer data	6	27.27%	5	13.89%	-20.00%
Contravention of systems access policy	2	9.09%	4	11.11%	50.00%
Contravention of IT security policy	1	4.55%	3	8.33%	66.67%
Unauthorised alterations to customer data	1	4.55%	2	5.56%	50.00%
Contravention of email policy	-	-	1	2.78%	100.00%
Modification of customer payment instructions	1	4.55%	1	2.78%	0.00%

The most significant finding is that the number of times that a member of staff disclosed personal data to a third party has almost doubled. Such cases frequently involve a member of staff being bribed by (or colluding with) organised criminals into revealing customer data. The criminals then use the data either to plunder the accounts of their victims or to make multiple applications in their names. This is serious on a number of fronts. The victims will suffer from having their identities misused, and a victim's identity could also be used for other serious and organised crimes. The organisation may well suffer reputational damage as well as a financial cost if any victims' accounts have been raided by the criminals, and the proceeds of these crimes may well fund other forms of organised crime.

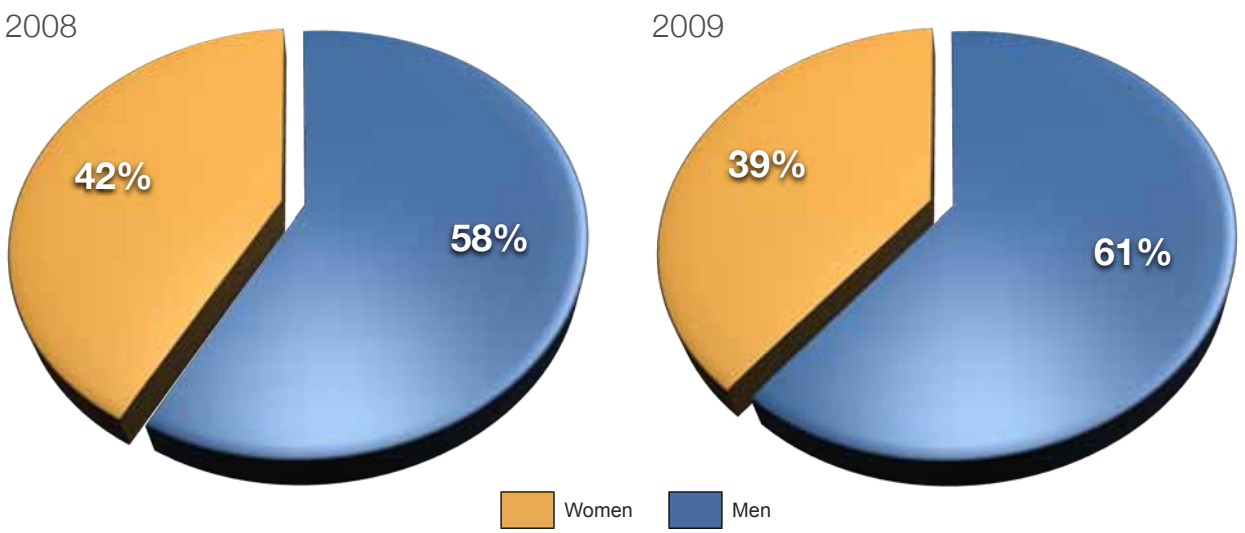
The first step in counteracting such threats is for organisations to put in place reporting mechanisms for staff who are approached by organised criminals. Staff must also be reminded of their responsibilities when processing personal data and the consequences of its misuse. Organisations also need to be aware that staff members may be planted within the workforce with the express intention of compromising data. This threat is real and is continuing to emerge.

4. Gender distribution of staff fraudsters

Chart 4.1 shows that the proportion of men perpetrating staff fraud has increased slightly in 2009 compared with 2008, with men accounting for 61% of staff frauds compared with 58% in 2008.

Gender distribution comparing 2008 and 2009

Chart 4.1



This can be broken down further by looking at the gender distribution by fraud type.

Gender distribution by fraud type

Table 4.1

	2008		2009	
Staff Fraud type	**% Men**	**% Women**	**% Men**	**% Women**
Account fraud	75.00%	25.00%	60.00%	40.00%
Dishonest action by staff to obtain a benefit by theft or deception	53.68%	46.32%	55.21%	44.79%
Employment application fraud (successful)	62.50%	37.50%	80.00%	20.00%
Employment application fraud (unsuccessful)	59.46%	40.54%	76.60%	23.40%
Unlawful obtaining or disclosure of commercial data	100.00%	-	100.00%	-
Unlawful obtaining or disclosure of personal data	64.29%	35.71%	66.67%	33.33%
All Staff Frauds	58.33%	41.67%	61.20%	38.80%

In both 2008 and 2009, men were more likely to commit all types of staff fraud and, with the exception of account fraud, men accounted for a higher proportion of all staff fraud types in 2009 than they did in 2008. This is particularly the case with employment applications.

Table 4.2 shows the distribution across the fraud types of the staff frauds perpetrated by men and women in 2008 and 2009.

Types of Staff Fraud committed by men and women

Table 4.2

	Men			Women		
Staff Fraud type	**2008**	**2009**	**% Change**	**2008**	**2009**	**% Change**
Account fraud	7.56%	10.82%	133.33%	3.53%	11.38%	366.67%
Dishonest action by staff to obtain a benefit by theft or deception	42.86%	54.64%	107.84%	51.76%	69.92%	95.45%
Employment application fraud (successful)	4.20%	4.12%	60.00%	3.53%	1.63%	-33.33%
Employment application fraud (unsuccessful)	36.97%	18.56%	-18.18%	35.29%	8.94%	-63.33%
Unlawful obtaining or disclosure of commercial data	0.84%	1.55%	200.00%	-	-	-
Unlawful obtaining or disclosure of personal data	7.56%	10.31%	122.22%	5.88%	8.13%	100.00%
All Staff Frauds	100.00%	100.00%	63.03%	100.00%	100.00%	44.71%

Table 4.2 shows that a greater proportion of women were involved in theft or deception offences (in both 2008 and 2009) than any other type of staff fraud, and that this trend became more marked in 2009. Just over half of the staff frauds carried out by women in 2008 were 'dishonest actions to obtain a benefit by theft or deception', but this rose to almost 70% in 2009. The proportion of account frauds carried out by women also increased in 2009 to just over 11%. The biggest proportionate decrease was seen in the number of employment application frauds carried out by women. This may be attributable either to the reduction in the number of vacancies (resulting in fewer employment application frauds) or an increase in the number of people 'feeling the pinch' of the economic conditions, remaining with an employer and resorting to the 'cash fraud' type of offences.

> "70% of all Staff Frauds carried out by women were dishonest actions to obtain a benefit by theft or deception."

This change in the distribution across the staff fraud types is echoed in the frauds committed by men, but to a lesser extent. With male staff fraudsters, there is a more even spread across the fraud types. Again, however, the proportion of cases relating to theft or deception and account fraud has increased at the expense of employment application frauds.

>

Dishonest action to obtain a benefit by theft or deception - by gender

Table 4.3

	Men		Women	
Filing Reason	**2008**	**2009**	**2008**	**2009**
Facilitating fraudulent applications	6.67%	18.12%	4.00%	3.45%
Theft of cash from customer	5.00%	18.12%	14.00%	37.07%
Manipulation of applications/proposals/claims	-	15.44%	2.00%	3.45%
Manipulation of a third party account	16.67%	7.38%	16.00%	6.90%
Theft of cash from employer	15.00%	6.71%	12.00%	15.52%
Manipulation of personal account	5.00%	6.04%	6.00%	6.03%
Manipulation of bonus/reward scheme	13.33%	4.70%	6.00%	0.86%
Removal of charges from personal account	5.00%	3.36%	6.00%	4.31%
Manipulation of application systems	-	2.68%	-	-
Perpetrating false insurance claims	1.67%	2.68%	-	2.59%

> “Based on these figures, men were more likely to try and facilitate fraudulent applications or manipulate them but, compared with women, were less likely to steal cash from either their employer or customers.”

It is notable that there is a big discrepancy in the offences committed by men and women when carrying out dishonest actions (see Table 4.3). Based on these figures, men were more likely to try and facilitate fraudulent applications or manipulate them but, compared with women, were less likely to steal cash from either their employer or customers. Theft of cash accounted for over 52% of cases where women were involved during 2009, compared with only 26% in 2008. For men the figures were nearly 25% in 2009 compared with 20% the year before. Fraudulent applications facilitated or manipulated by men in 2009 accounted for almost 34% of cases, compared with almost 7% in 2008. The figures for women were markedly different: only 7% in 2009, up slightly from 6% in 2008.

This does raise a couple of questions: namely, why are women seemingly more likely to try and perpetrate ‘cash frauds’? Or is it that women make up a disproportionate number of the workforce that handles cash? Does this lead to the conclusion that there is a much greater, organised, criminal involvement in the frauds committed by men?

5. Length of service

Average length of service - by gender

Table 5.1

	All		Men		Women	
Average length of service	2008	2009	2008	2009	2008	2009
Years	1.55	4.32	1.30	3.76	2.11	5.42

Table 5.1 shows how long the fraudster was employed before the fraud was identified – although it should be borne in mind that this does not give an indication of the length of time the employee had been committing fraud.

The average length of service for both male and female fraudsters increased significantly between 2008 and 2009, with the staff fraudster (on average) in position for over 4 years before fraud was discovered. This may give credence to the idea that a lot of the frauds discovered were perpetrated by people who had become increasingly desperate in the prevailing economic conditions. It is probable that some of the fraudsters may have been committing fraud against their employer for some period of time prior to discovery. Others, however, are likely to have been previously good employees who had more recently turned to fraud.

Table 5.2 shows the average length of service by the type of fraud committed.

Average length of service by fraud type - in years

Table 5.2

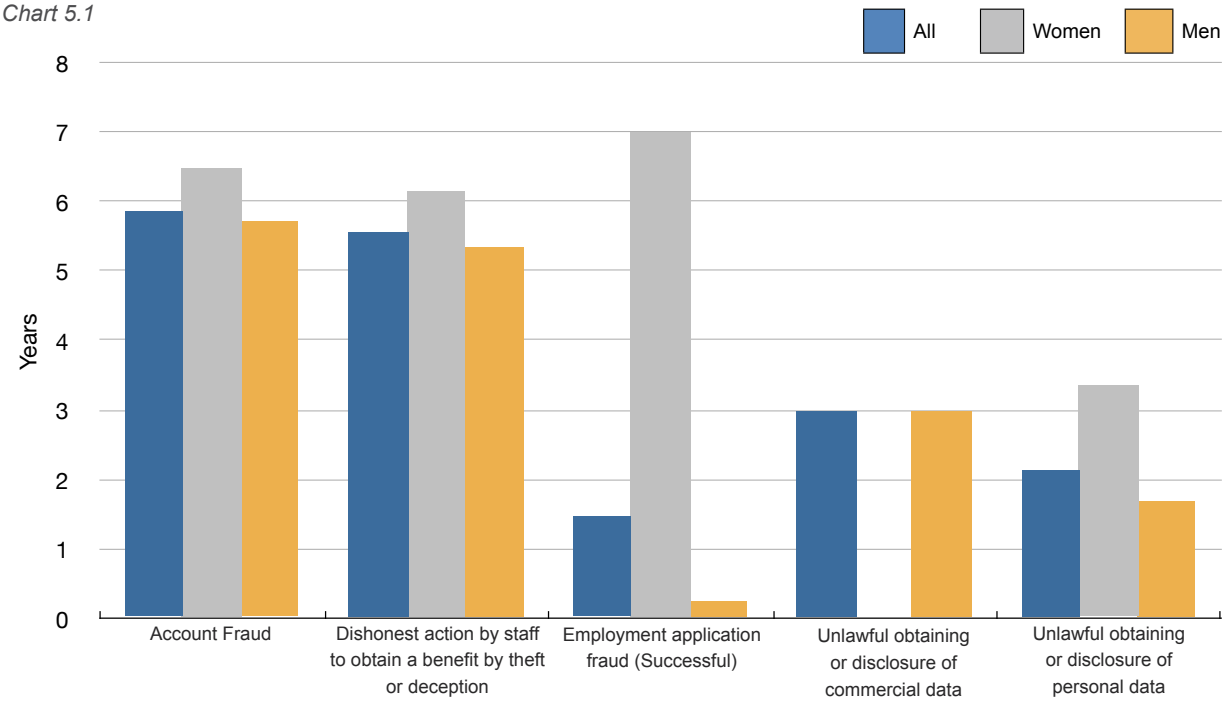
	All		Men		Women	
Staff Fraud type	**2008**	**2009**	**2008**	**2009**	**2008**	**2009**
Account fraud	4.28	5.88	3.47	5.71	6.69	6.48
Dishonest action by staff to obtain a benefit by theft or deception	2.42	5.57	1.90	5.33	3.39	6.14
Employment application fraud (successful)	0.58	1.48	0.92	0.24	0.39	7.00
Unlawful obtaining or disclosure of commercial data	0.17	3.00	0.17	3.00	-	-
Unlawful obtaining or disclosure of personal data	2.09	2.14	2.44	1.69	1.73	3.35

Although there was a general increase in the average length of service before fraud was identified, there does seem to have been a clear gap between the average length of time that people were employed before committing a 'cash fraud' type of offence, and an offence that might be connected to further criminality. People committing 'account fraud' (and theft and deception offences) were employed for roughly twice as long as those found to have unlawfully disclosed commercial or personal information. Again, this adds credence to the idea that the 'cash fraud' offences were committed by the desperate, while the people unlawfully disclosing information (or, at least some of them) were placed specifically to commit fraud by organised criminals.

The very short period of employment for men who successfully committed employment application fraud reinforces the idea that a lot of these cases, where the offence was 'concealed unspent criminal convictions', were instances where the individual had commenced employment before the result of the CRB check was known. Then, when an unfavourable CRB result was returned - usually within the first few months of employment - this resulted in dismissal or termination of the contract. >

Average length of service in 2009

Chart 5.1



6. Age of staff fraudsters

Table 6.1 gives the average age of the staff fraudsters for the different Staff Fraud types.

Average age of staff fraudsters by fraud type

Table 6.1

	All		Men		Women	
Staff Fraud type	**2008**	**2009**	**2008**	**2009**	**2008**	**2009**
Account fraud	31.77	30.00	31.33	31.48	34.33	28.64
Dishonest action by staff to obtain a benefit by theft or deception	27.95	31.35	27.86	31.28	28.41	31.55
Employment application fraud (successful)	29.86	27.54	31.60	24.00	30.00	31.00
Employment application fraud (unsuccessful)	31.49	34.39	31.11	34.66	31.70	33.45
Unlawful obtaining or disclosure of commercial data	40.00	27.00	40.00	27.00	-	-
Unlawful obtaining or disclosure of personal data	26.40	26.21	28.11	26.55	23.20	25.30
All Staff Frauds	29.48	30.96	29.61	31.06	29.56	30.87

The overall trend is that there was little difference between the figures for 2008 compared with 2009. It is of more interest, however, that the increases in average age for the two most commonly identified fraud types - namely 'dishonest action by staff to obtain a benefit by theft or deception' and 'employment application fraud (unsuccessful)' - rose more steeply than the increases across all cases for both men and women. This was especially the case for men, with increases of around 3.5 years for both of these staff fraud types (compared with an increase of just less than 1.5 years for all fraud types). These trends will certainly require further attention over the coming years, to see if this development continues - or whether clear underlying reasons become evident. For instance, will any future change in economic conditions result in further changes to these trends? Will changing demographics in recruitment (e.g. a preference for young, recently graduated, employees or slightly older, experienced, candidates) be reflected through changes to these figures?

26 years

The average age of a staff fraudster involved in 'Unlawful obtaining or disclosure of personal data'

31 years

The average age of a staff fraudster involved in 'Dishonest action by staff to obtain a benefit by theft or deception'.

It must not be overlooked, however, that these figures may also be a further indication that desperation was a motivating factor in 'cash frauds', as those with more responsibilities (mortgage, children etc.) felt that they had no option other than to turn to desperate measures to make ends meet. It is also notable that the sort of fraud that is more likely to be involved in further criminality (e.g. disclosing personal information to an organised criminal) involved somewhat younger fraudsters, suggesting that the young are more susceptible to coercion.

>

Employment application fraud (unsuccessful) age groups in 2008 and 2009

Chart 6.1

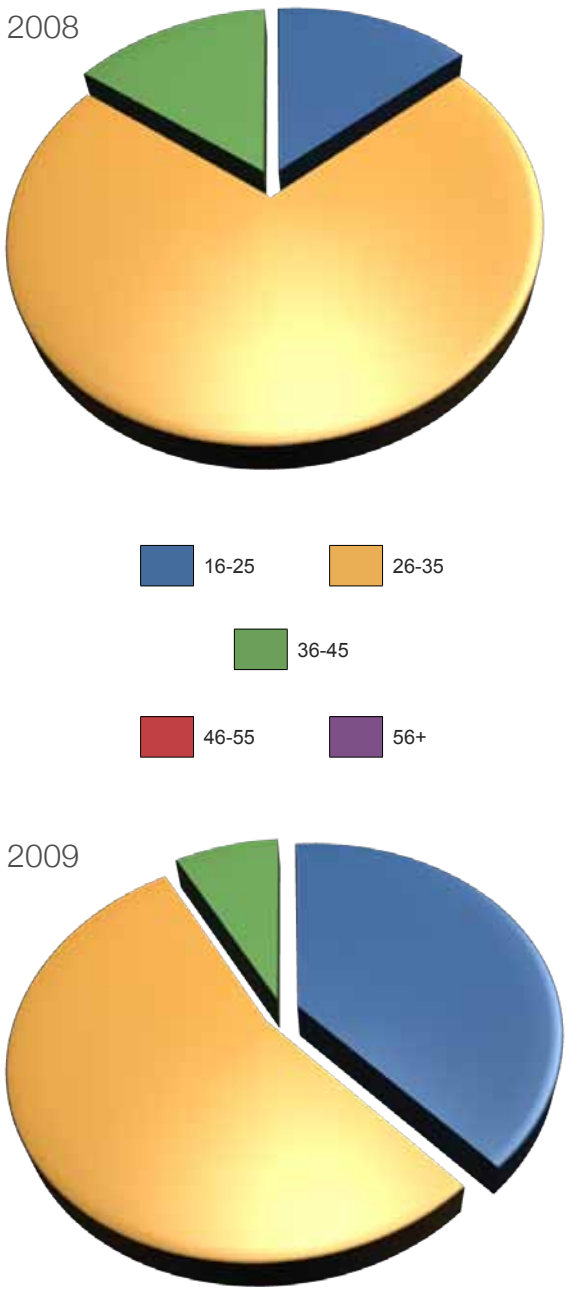


Chart 6.1 clearly shows the increase in the age of those who committed unsuccessful 'employment application fraud' in 2008 and 2009. In 2008, over a quarter of these fraudsters were less than 26 years old and a quarter were 36 or older. In 2009, only 8% were less than 26 and over 40% were 36 or older. The increase in average age of those committing theft and deception offences should also be noted. Over 50% were in the 16-25 age bracket in 2008, but in 2009 this was down to a third.

While the numbers were small (15 in 2008, increasing to 32 in 2009), what is notable is that those cases of 'unlawful obtaining or disclosure of personal data' recorded on the database, were exclusively committed by people (predominantly men) below the age of 46. In both 2008 and 2009, over 90% of the staff fraudsters recorded on the Staff Fraud Database for this offence were between 16 and 35 years of age: with the majority falling into the 16–25 age range (60% in 2008 and 58% in 2009). This obvious slant towards the younger side of the workforce leads to a couple of interesting considerations. First, that organised criminal networks (who, traditionally, are known to exploit staff fraudsters in an attempt to get hold of personal data) may be specifically targeting the younger members of the workforce – deeming them to be more 'susceptible' and less likely to be 'loyal' to an employer due to the short length of service.

Another, perhaps more sobering possibility, is that the criminals of tomorrow could merely be the school leavers of today: and that the younger population's immersion in technology throughout their school lives is beginning to display itself through – in this case – shifts in the criminal patterns being noted, and their knowledge of the value of the data at their fingertips. Sometimes, these staff may view fraud as a victimless crime and be unaware of the consequences, so do not fear detection. Awareness, therefore, is key. Some organisations have implemented a reporting mechanism for staff who have been approached by organised criminals, and these organisations are therefore better geared to preventing fraud of this kind.

7. Area of business

The area of business where the fraudsters were employed can be seen in Table 7.1.

Business area by gender

Table 7.1

	All		Men		Women	
Business Area	**2008**	**2009**	**2008**	**2009**	**2008**	**2009**
Branch/Retail outlet/Store	36.62%	59.00%	31.51%	47.13%	50.00%	76.58%
Customer contact centre	45.77%	24.33%	46.58%	32.48%	36.54%	11.71%
Field unit	10.56%	8.33%	15.07%	12.74%	3.85%	0.90%
Finance department	-	1.00%	-	0.64%	-	1.80%
IT department	0.70%	0.33%	1.37%	0.64%	-	0.00%
Other	2.82%	4.00%	2.74%	3.82%	3.85%	4.50%
Other support services	2.82%	3.00%	2.74%	2.55%	3.85%	4.50%
Staff contact centre	0.70%	-	-	-	1.92%	-

Unsurprisingly, given the increase in the number of offences relating to theft of cash, the proportion of staff frauds perpetrated by someone working in a branch, retail outlet or store has increased to almost 60% of staff fraud cases. For women, who are proportionally more likely to commit the 'cash frauds', this figure is up to over three quarters of cases.

In 2008, a higher proportion of frauds involving men occurred in a customer contact centre (47%) compared with a branch, retail outlet or store (32%). In 2009, these figures have been reversed, with 47% of cases occurring in a branch, retail outlet or store while the proportion that occurred in a customer contact centre dropped to 32%.

8. Geographics

It is important to bear in mind the area of business the fraudsters were employed in (or applying for) when considering the location of the frauds. If, for example, an organisation has one customer contact centre, and that is in Birmingham, then all frauds where the perpetrator was employed in the contact centre will take place in Birmingham, which is not particularly revealing. Therefore, when assessing the location of the frauds and the fraudsters, only offences that took place in a branch, retail outlet or store have been considered. These are likely to be more representative of the UK picture as a whole (although it is acknowledged that some organisations have greater representation in some areas of the country than others).

Top ten postal areas for frauds taking place in branches, retail outlets or stores in 2008

Table 8.1

Postal Area	% of Current Addresses	Postal Area	% of Employment Addresses
East London	21.15%	East London	14.58%
South East London	7.69%	Glasgow	8.33%
Glasgow	5.77%	West London	8.33%
West London	5.77%	Sheffield	6.25%
Wakefield	5.77%	Ipswich	4.17%
Cambridge	3.85%	Leeds	4.17%
Portsmouth	3.85%	Peterborough	4.17%
Bradford	1.92%	Portsmouth	4.17%
Bolton	1.92%	Bradford	2.08%
Brighton	1.92%	Bolton	2.08%

Tables 8.1 and 8.2 show the top ten postal areas for the current address of the fraudster and the employment address in 2008 and 2009. It can be seen that East London was most commonly given as the current address in 2008 and 2009, but the proportion of such addresses that this area accounted for in 2009 was substantially lower. It is of interest that East London did not account for the same proportion of employment addresses as it did current addresses, implying that there were staff fraudsters who lived in East London, but were employed in other areas. The same can be said of South East London – this area appeared in the top ten postal areas for current addresses in 2008 and 2009, but did not appear in the top ten areas for employment address. Conversely, West London appeared very high in the top ten employment address areas in both years, but featured much less in the current address lists. In fact, it was the most common area for employment address in 2009, but didn't feature at all in the current address list. It is interesting that some of the cases of staff fraud in branches, retail outlets or stores in West London were perpetrated by people living as far away as Dartford and Ilford (a longer than reasonable commute for those working in such roles).

Less than **1.2%** of staff fraudsters lived in West London in 2009 - not especially surprising until you consider that **5.2%** were recorded as working in that postal area.

Top ten postal areas for frauds taking place in branches, retail outlets or stores in 2009

Table 8.2

Postal Area	% of Current Addresses	Postal Area	% of Employment Addresses
East London	5.20%	West London	5.20%
North London	4.05%	East London	4.62%
Brighton	3.47%	South West London	4.62%
Romford	3.47%	Brighton	3.47%
South East London	3.47%	East Central London	3.47%
Aberdeen	2.89%	Glasgow	3.47%
Birmingham	2.31%	North London	3.47%
Cardiff	2.31%	Aberdeen	2.89%
Dartford	2.31%	Cardiff	2.89%
Harrow	2.31%	Ipswich	2.31%

9. Reason for leaving

Table 9.1 shows the reason the staff fraudsters left their employer, with the type of offence committed.

Reason for leaving by fraud type

Table 9.1

	Dismissed		Resigned		Resigned during investigation	
Staff Fraud type	**2008**	**2009**	**2008**	**2009**	**2008**	**2009**
Account fraud	62%	72%	-	18%	38%	10%
Dishonest action by staff to obtain a benefit by theft or deception	75%	67%	9%	9%	16%	25%
Employment application fraud (successful)	90%	75%	-	8%	10%	17%
Unlawful obtaining or disclosure of commercial data	100%	100%	-	-	-	-
Unlawful obtaining or disclosure of personal data	87%	73%	7%	9%	7%	18%

Table 9.1 shows that staff fraudsters tend to 'sit it out' until the end of the disciplinary process as opposed to resigning during the process. There was, however, a general increase in the proportion of staff fraudsters who did resign during an investigation in 2009, compared with 2008.

22.5%

Percentage of people that resigned during the initial investigation.

This is most notable in cases of 'dishonest action by staff to obtain a benefit by theft or deception', where the employer is likely to have had sufficient evidence to put the case beyond reasonable doubt, but this may also have been partly due to the gender distribution of this staff fraud type. Women were more likely than men to resign during the investigation in 2009, with over 31% of female perpetrators prepared to walk away, compared with less than 22% of men.

It may be that women were more likely to have committed frauds where there was no possible doubt as to the outcome of the investigation. Or it may be that women were less inclined to put themselves through the disciplinary process while men were more prepared to 'fight their corner'.

More fraudsters who committed account fraud were dismissed in 2009 than in 2008, bucking the trend seen across the other staff fraud types. With this type of fraud, though, a much higher proportion of people actually resigned prior to an investigation - particularly in the case of women, where 25% did so. This would seem to imply two types of behaviour for this type of fraud: those who commit fraud, then leave before their employer discovers it; and those who commit fraud, then dig their heels in and see the disciplinary procedure through to its conclusion. There was a lower percentage of people who, when caught, were prepared to 'cut their losses' and resign.

10. Means of discovery

Table 10.1 shows how the frauds identified in 2008 and 2009 were discovered.

Means of discovery compared by fraudster's gender

Table 10.1

	All		Men		Women	
Means of Discovery	**2008**	**2009**	**2008**	**2009**	**2008**	**2009**
Customer	19.73%	32.45%	17.33%	20.89%	21.82%	44.64%
Internal controls/audit	63.27%	43.38%	65.33%	51.90%	58.18%	33.93%
Law enforcement	2.72%	5.30%	4.00%	6.96%	-	2.68%
Other	2.04%	3.97%	2.67%	5.06%	1.82%	2.68%
Staff	9.52%	11.26%	9.33%	12.03%	12.73%	11.61%
Staff (whistleblowing)	2.72%	3.64%	1.33%	3.16%	5.45%	4.46%

Chart 10.1 (overleaf) clearly shows that between 2008 and 2009, the proportion of cases where the customer reported the fraud increased, while the proportion of cases highlighted by internal controls decreased. In 2009, almost a third of cases of staff fraud were reported by the customer. This shift in the means of discovery may be a reflection of the shift in the type of frauds committed: there were more frauds that directly resulted in the customer losing money in 2009 than there were in 2008, so the chances of the customer being the first person to notice were (reasonably) higher. This is clearly a concern for the employer involved as substantial reputational damage can result if there is a perception by customers that staff working for the organisation cannot be trusted.

> "The increase in the proportion of frauds reported by the customer is clearly a concern for the employer involved as substantial reputational damage can result if there is a perception by customers that staff working for the organisation cannot be trusted."

There was an increase in the number of cases that were brought to the employer's attention by law enforcement (although the numbers were still comparatively small). This could indicate that there was an increase in the number of cases connected to serious organised criminality, warranting a police investigation.

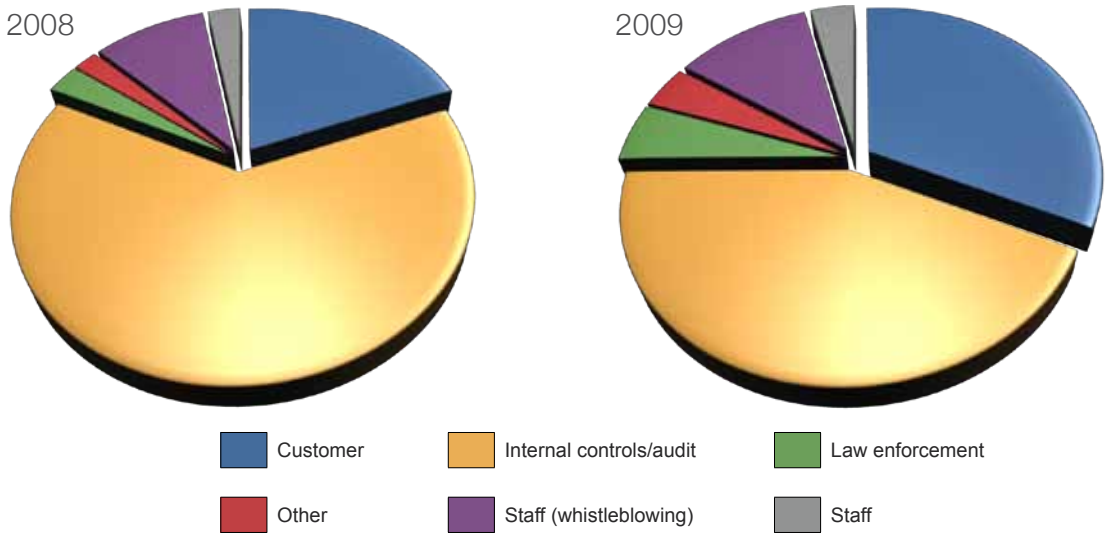
It is curious that the number of cases involving women who were reported by other members of staff decreased in 2009 compared with 2008, but the proportion of men who were reported by their colleagues increased. This may be due to general perceptions of – or preconceptions about – the perpetrators of staff fraud.

Whistleblowing continues to be the least frequent means of discovery. It is, therefore, recommended that organisations have a whistleblowing policy and that this is regularly publicised to staff.

>

Means of discovery comparing 2008 with 2009

Chart 10.1



11. Level of reporting to the police

The majority of staff frauds go unreported to the police, but where the case has been reported, this was almost always by the employer organisation. In 2008, 77.5% of cases were not reported to the police, with 72% going unreported in 2009. While this appears to show an increase in the level of reporting, it is important to consider the types of fraud reported. In 2008 and 2009, there were no instances of unsuccessful employment application frauds being reported to the police, although they are criminal offences. This may be due to a perception that they are not a priority for the police to investigate, as the level of harm that has been caused is a meaasure that the police use in determining whether to investigate a case or not.

Proportion of cases reported to the police in 2008 and 2009

Table 11.1

	Not reported		Reported by Customer		Reported by Organisation		Reported by Other	
Staff Fraud type	**2008**	**2009**	**2008**	**2009**	**2008**	**2009**	**2008**	**2009**
Account fraud	15.38%	51.28%		-	84.62%	43.59%	-	5.13%
Dishonest action by staff to obtain a benefit by theft or deception	72.22%	73.02%		0.47%	27.78%	25.12%	-	1.40%
Employment application fraud (successful)	80.00%	61.54%		-	20.00%	23.08%	-	15.38%
Employment application fraud (unsuccessful)	100.00%	100.00%		-	-	-	-	-
Unlawful obtaining or disclosure of commercial data	100.00%	66.67%		-	-	33.33%	-	-
Unlawful obtaining or disclosure of personal data	46.67%	51.52%		3.03%	46.67%	33.33%	6.67%	12.12%

Table 11.1 shows that there was an increase in the proportion of cases of account fraud, dishonest actions and disclosure of personal data to third parties that were not reported. It could be that employers considered it sufficient for them to dismiss the member of staff and that reporting the case to the police might create unnecessary work for little benefit – especially in times of economic pressure where staff may be under increased workloads.

This finding underlines the fact that employers cannot rely, purely, on CRB checks when vetting staff at application stage. The majority of cases of staff fraud are not reported to the police at all, let alone result in a conviction that will be returned by a CRB check. While it might be argued that the use of references from former employers might reveal such serious frauds, that cannot be guaranteed. The sharing of data about such confirmed frauds - using a shared standard and requirement of proof, is an effective way of preventing fraudsters from moving unchallenged from one organisation to another unsuspecting employer.

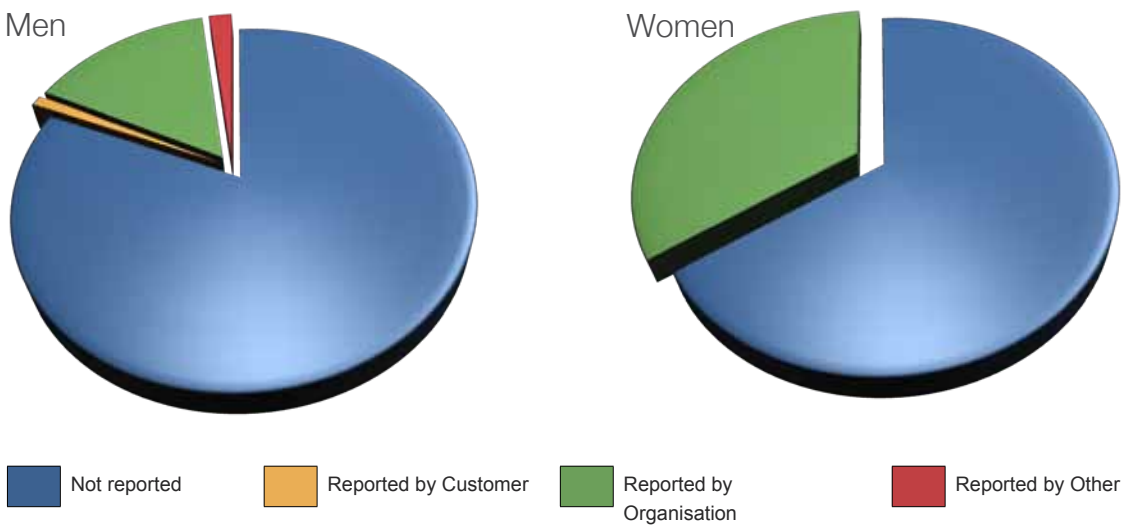
“Employers cannot rely, purely, on CRB checks when vetting staff at application stage. The majority of cases of staff fraud are not reported to the police at all, let alone result in a conviction that will be returned by a CRB check.”

Interestingly, although in cases of account fraud and dishonest actions there was a greater chance of male fraudsters than female fraudsters being reported by their colleagues. This was not the case when it came to being reported to the police, with employers more likely to report female fraudsters than male. This can be seen in Charts 11.1 and 11.2 covering the cases identified in 2009.

This phenomenon, though, did not apply to cases of members of staff disclosing personal data to a third party. Here, men were more likely to be reported to the police than women (70% of women escaped being reported to the police compared with only 40% of men).

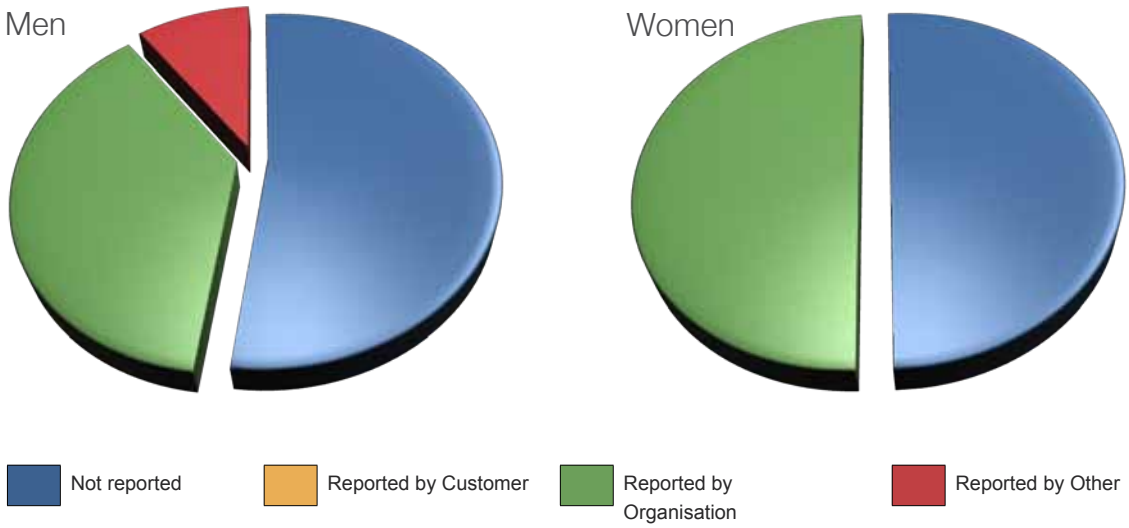
Dishonest actions to obtain a benefit by theft or deception, analysed by gender in 2009

Chart 11.1



Account fraud by gender in 2009

Chart 11.2



12. The fraudscape of the UK: conclusions

2009 saw a substantial rise in the number of cases of staff fraud identified compared with 2008. While the number of organisations participating in the CIFAS Staff Fraud Database grew, the rate of increase in cases recorded on the database was greater.

There was a rise in the amount of 'account fraud' in 2009; much of which involved withdrawals from customer accounts. There was also an increase in 'dishonest actions to obtain a benefit by theft or deception', much of which involved theft of cash from customers or from the employer. These frauds could be considered 'cash frauds', where the employee pockets cash each time they carry out a theft. This might be due to some extent to personal greed, but could equally be fuelled by increasing desperation due to the economic conditions. It is clear that an individual must be truly desperate if he or she is willing to risk dismissal and the loss of income (especially given the downturn in recruitment) if caught for what could be a relatively small sum.

The idea that a lot of the 'cash frauds' were desperation-driven is further reinforced by the fact that the average length of service (prior to the fraud being identified) increased, as did the average age of the perpetrator. This implies that the frauds were increasingly being committed by people who had previously been honest employees, but perhaps had commitments (like children and a mortgage) or lifestyles that they were having increasing difficulty in funding.

Of great concern to employers is the fact that a lot of these frauds only came to light following a complaint from the customer. This could lead to a lack of trust in the organisation involved, and its vetting procedures, damaging its reputation. Such short-term effects can obviously lead to more serious long-term consequences. Establishing an anti-fraud culture that includes the people and policies of an organisation is critical. Combining this with the identification of staff fraudsters and sharing this data to prevent them moving unchallenged to another organisation helps both reputationally and financially.

There was a reduction in the number of unsuccessful employment application frauds, due primarily to the reduction in the amount of recruitment taking place.

The number of successful employment application frauds increased, however. Many of these successful employment application fraudsters, particularly men, failed to declare their unspent criminal convictions. It seems that employers had been allowing successful applicants to start in post prior to receiving the results of a CRB check (indicated by the relatively short length of service before the fraud was discovered). This means that employers effectively allowed criminals access to their organisation, possibly in a position of some trust, for that period. This clearly posed a threat to the organisation, a fact that will require significant human resources attention, and a clearly defined policy, both to address this threat and prevent a recurrence.

A worrying trend was the increase in the number of cases of employees selling personal data. The implication of this finding is that more staff are being approached by organised criminals and bribed to reveal personal customer data. These details could be used to commit financial fraud, or to enable more serious and organised criminality. This might be motivated to a certain extent by tighter economic conditions increasing the sense of desperation, or it could simply be greed. It should also be borne in mind that a number of the employees identified as passing on information in this way may actually have applied for their position with the express aim of obtaining personal information for organised criminals. Especially worrying is that such individuals, and their intentions, may well be entirely unidentifiable when they make their application.

It is apparent that fraud prevention strategies and controls need continually to adapt as the types of frauds clearly changed between 2008 and 2009, as did the motivations of the fraudsters. The continuing reinforcement of an anti-fraud culture is crucial. Staff need to be reminded of the consequences of committing fraud and how it affects victims and their colleagues, while organisations need to ensure that clearly defined, robust procedures are in place to protect the customer, the business and the majority of hard-working, honest staff that they employ.

For further information, please contact our Research Manager and the Communications Team, or our Staff Fraud Adviser.

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

press@cifas.org.uk
staff.fraud@cifas.org.uk

CIFAS

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

www.cifas.org.uk