cifas
Leaders in fraud prevention

THE INSIDER FRAUD PICTURE

Why are all organisations at risk of internal fraud?
What does the insider threat look like?
How can you protect your employees and your organisation?

INTRODUCTION

206 organisations use Cifas' Internal Fraud Database to share details of members of staff or applicants for employment whose conduct has been fraudulent. This report looks at the Internal Fraud Database in 2017, and provides insight into the type of internal fraud trends seen by Cifas members.

There were 419 cases recorded to the Internal Fraud Database in 2017- a 2% increase on the number recorded the previous year.

25% of the cases reported in 2017 were reported to law enforcement.

Account fraud
Unauthorised activity on a customer account by a member of staff knowingly, and with intent, to obtain a benefit for themselves or others.

Being bribed
Request, agree to receive or accept, for own or another's benefit, for a financial or another advantage with the intention to improperly performing a function or activity.

Dishonest action by staff to obtain a benefit by theft or deception
Where a person knowingly, or with intent, attempts to gain benefit for themselves or others through dishonest action, and where such contuct constitutes an offense.

Employment application fraud (successful)
A successful application for employment (or to provide services) with serious material falsehoods in the information provided, which includes the presentation of faulse or forged documents.

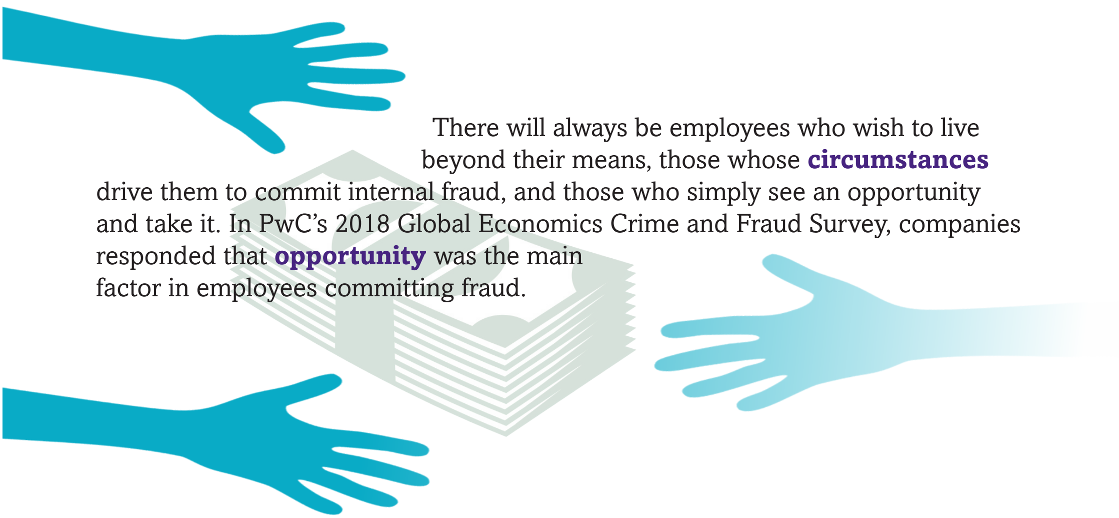
Employment application fraud (unsuccessful)
An unsuccessful application for employment (or to provide services) with serious material falsehoods in the information provided, which includes the presentation of false or forged documents.

Unlawful obtaining or disclosure of commercial data
Where commercial data is obtained, disclosed or procured without the consent of the data owner. This includes using data for unauthorised purposes placing an organisation at a financial or operational risk.

Unlawful obtaining or disclosure of commercial data
Where commercial data is obtained, disclosed or procured without the consent of the data owner. This includes using data for unauthorised purposes placing an organisation at a financial or operational risk.

FRAUD TYPE

Dishonest actions by staff to obtain a benefit by theft or deception was the most common type of internal fraud in both 2017 and 2016. The most common form of dishonest action in 2017 was theft of cash from the employer, which accounted for 24% of cases in 2017 compared with 22% in 2016. The second most common fraud type in 2017 was theft of cash from a customer, accounting for 17% in both 2017 and 2016.



There will always be employees who wish to live beyond their means, those whose **circumstances** drive them to commit internal fraud, and those who simply see an opportunity and take it. In PwC's 2018 Global Economics Crime and Fraud Survey, companies responded that **opportunity** was the main factor in employees committing fraud.

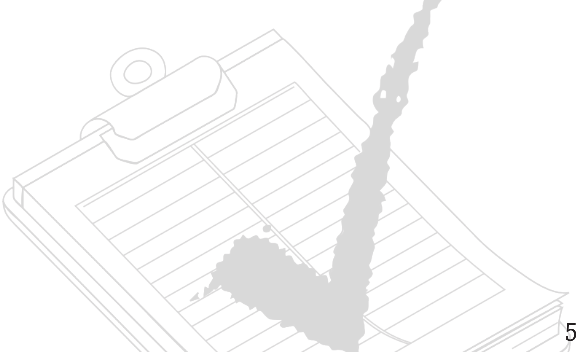
Although **employment application frauds** continue to account for a large proportion of cases filed, there was a reduction in 2017 compared with 2016. Unsuccessful employment application fraud (where an applicant's fraudulent application was detected before an offer of employment) saw a 4% reduction, whereas successful employment application fraud (where a fraudulent application is initially undetected and the individual receives employment) saw a 26% reduction.

The largest number of cases relates to individuals hiding adverse credit information. More interestingly, however, there was an increase in the number of people concealing their employment record (40 individuals in 2017 compared with 27 in 2016). This often relates to individuals hiding the reason for leaving previous employers, so it's always paramount to check references.

CARDHOLDER

Hiding unspent **criminal convictions** remained the most common form of fraudulent conduct where the employment applications fraud was successful, as the individual may have started in employment before the pre-employment checks are completed.

With all types of employment application frauds, **competitiveness for jobs** is likely to be the main motivator. Some individuals will not include certain details on their application in order to improve their chance of employment.



	2017	2016	%
Account fraud	26	31	↓16%
Being bribed	0	1	↓100%
Dishonest action by staff to obtain a benefit by theft or deception	191	172	↑11%
Employment application fraud (successful)	29	39	↓26%
Employment application fraud (unsuccessful)	153	159	↓ 4%
Unlawful obtaining or disclosure of commercial data	7	0	-
Unlawful obtaining or disclosure of personal data	40	31	↑29%

There were 40 individuals recorded to the Internal Fraud Database for unlawfully obtaining, and disclosing personal data in 2017, which is a 29% increase compared with 2016. It's notable that this has occurred alongside unprecedented numbers of impersonations recorded to the National Fraud Database in 2017, with almost 175,000 applications for products or services made in the name of an innocent victim.

Fraudsters rely on a supply of personal data in order to commit these frauds – and employees working in an organisation are ideal targets for coercion or being bribed into acquiring and providing this data, or they may just find themselves in a position where they are tempted by opportunity.

For those whose details have been compromised, particularly if these breached details contain bank account information, this type of data breach increases the risk of becoming a victim of impersonation or having an account taken over. According to the latest *Global Fraud & Risk Report* from Kroll, in 2017 29% of survey respondents believed that their company was highly vulnerable to the theft, loss or attack of information. This is up from 24% in 2016 – the highest level in 10 years of reporting.

WHO COMMITS INTERNAL FRAUD?

Overall, 60% of individuals recorded on the Internal Fraud Database in 2017 were male, which has decreased from 64% in 2016. Traditionally, men have been more closely associated with internal fraud, but it's recognised that women are increasingly involved in this kind of activity. Perhaps some women believe that they are less likely to be suspected as they do not fit the 'traditional' profile of someone who commits internal fraud – someone identifed as 'male, between the ages of 36 and 55, working with the victim organisation for more than six years, and holding an executive position in operations, governance or general management' (taken from KPMG's *Global Profiles of the Fraudster*).

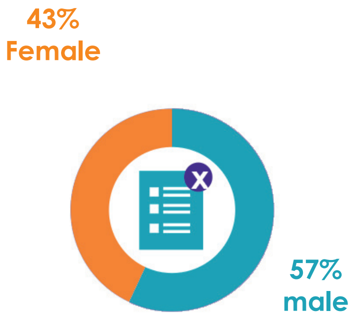
There was a 22% increase in the number of women recorded for dishonest actions by staff to obtain a benefit by theft or deception, compared with just a 9% increase in the number of men. There was a particular increase in the number of women identified as perpetrating fraudulent applications, which rose from 3 in 2016, to 17 in 2017. The proportion of women involved in successful employment application fraud has always been low, and this has decreased further in 2017 – down to 17% from 25% in 2016.

48% of individuals recorded in 2017 are aged between 21 and 30 years old, which is a slightly smaller proportion than in 2016. Counterbalancing this, 42% of individuals recorded in 2017 were aged between 31 and 50, compared to 36% in 2016. 53% of men were aged between 21 and 30 years old compared with 42% of women. Interestingly, there was a higher proportion of women aged between 41 and 50 years old recorded on the database than men. 32% of women aged between 41 and 50 years old were recorded for concealed adverse credit history and 29% were recorded for theft-related conduct such as theft of cash or office equipment.

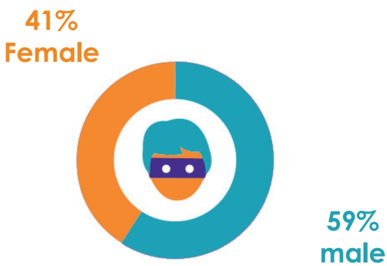
The type of fraudulent conduct that occurs is dependent on what the individual has access to. A large proportion of those individuals recorded on the Internal Fraud Database were working within a branch, retail outlet or customer contact centre – often dealing with personal information on a daily basis, while also having easy access to assets. This presents the 'opportunity' – identifed earlier as a key factor in employees committing fraud.

Account Fraud

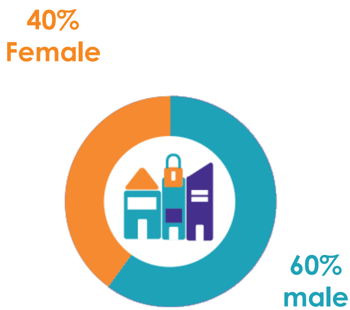
Employment application fraud (unsuccessful)



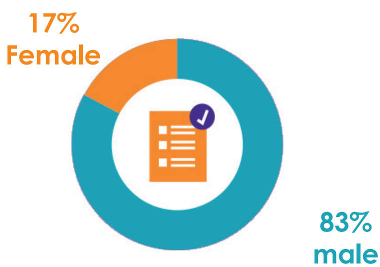
Dishonest by staff to obtain a benefit by theft or deception



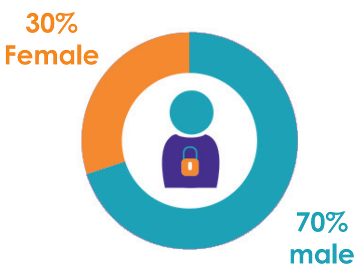
Unlawful obtaining or disclosure of commercial data



Employment application fraud (successful)



Unlawful obtaining or disclosure of personal data



HOW ARE THEY IDENTIFIED?

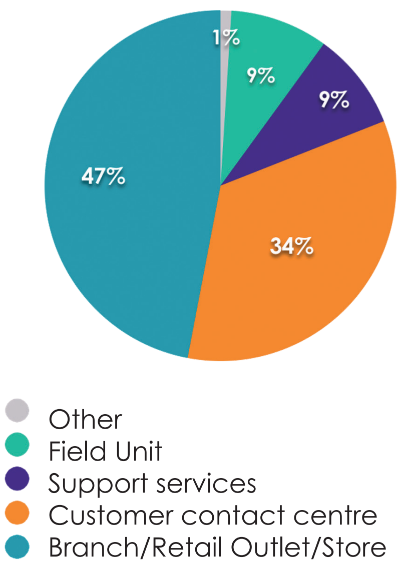
The majority of fraudulent conduct in 2017 was highlighted by internal controls and audit (59%), which is a 47% increase on 2016's figures.

The increased prevalence of internal controls as a means of discovering fraudulent conduct reflects the responses within PwC's Global Economic Crime and Fraud Survey 2018, which highlights that companies are spending more money on combating fraud and economic crime.

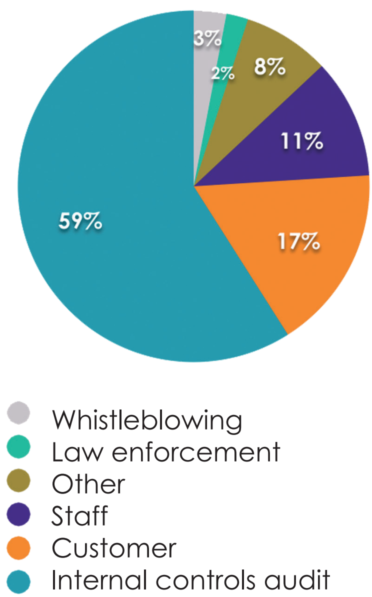
One thing to note is that fraud identified by staff and through whistleblowing channels saw a 15% reduction between 2016 and 2017. This could be because the effectiveness of internal controls has improved, and the reliance upon staff identifcation of fraud has declined.

However, companies should not rely on internal controls alone – there also needs to be an emphasis on trying to reduce the motivation of their staff to commit fraud, establishing an anti- fraud culture in the workplace, and continuing to provide effective and trusted channels to report suspicions of internal fraud.

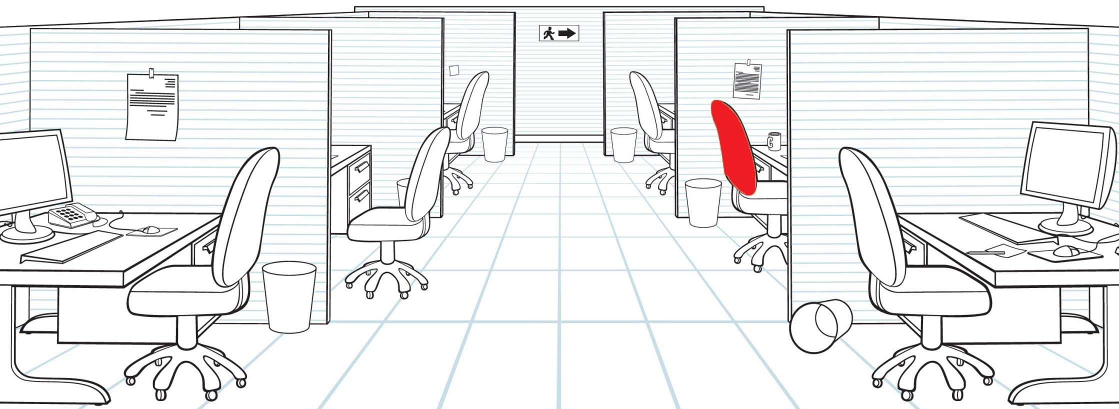
Breakdown of business area



Means of discovery



Leaders in fraud prevention



WWW.CIFAS.ORG.UK