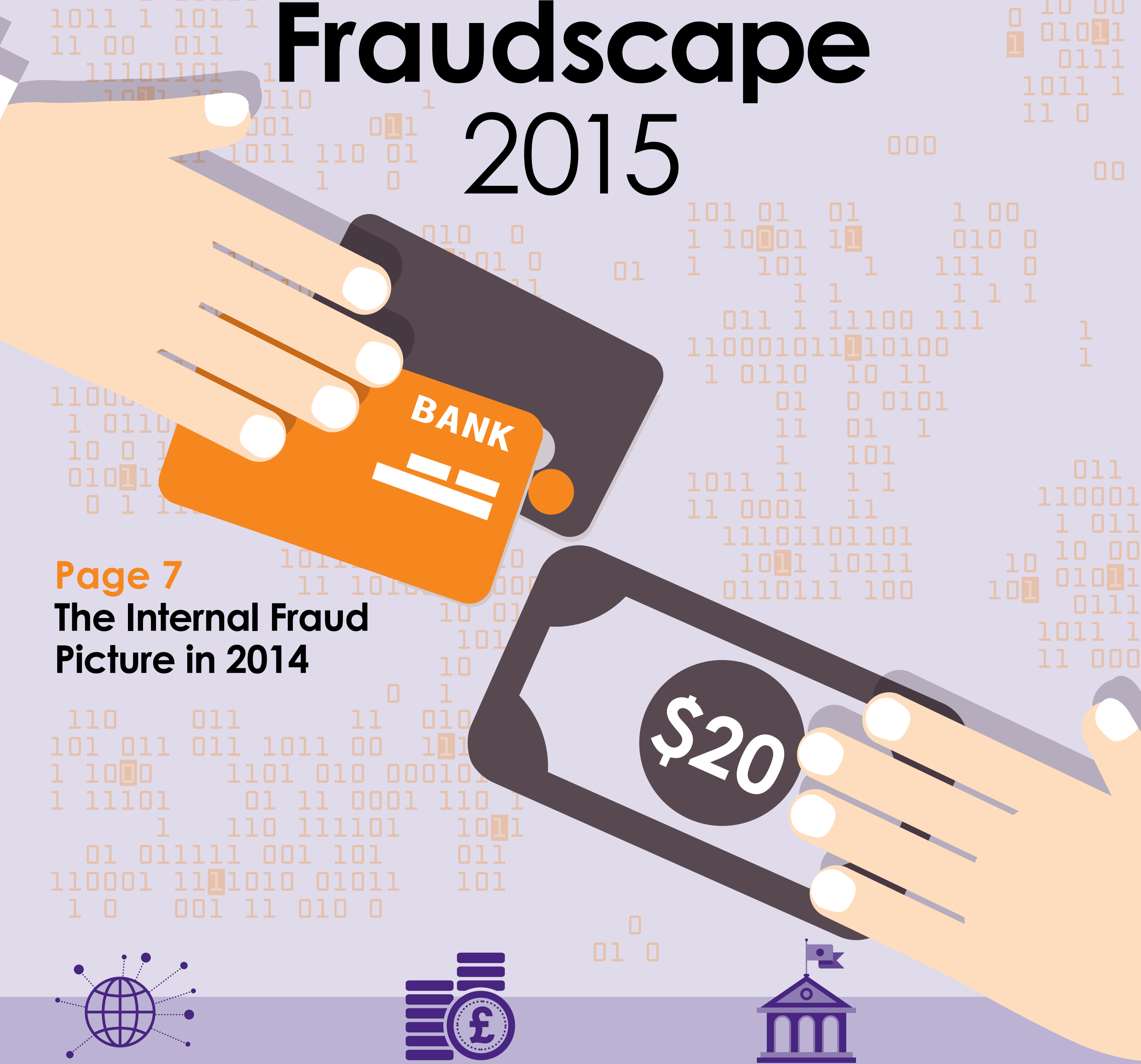
cifas
Leaders in fraud prevention

Employee Fraudscape 2015



CONTENTS

Introduction to Employee Fraudscape

Internal fraud is a reality.

BY **SIMON DUKES**, CIFAS CHIEF EXECUTIVE

PwC's Global Economic Crime Survey 2014 posed the question "who's attacking your company?" before stating that 56% of fraudsters are on the inside[1].

Fraud is not just about being attacked by remote criminals sat at a laptop miles away from an organisation's office. The threat can exist inside the organisation too and it can be wide ranging: from staff claiming to be someone or something that they are not, to the theft of cash or data, to bribery and corruption. All will cause damage to an organisation: not just financially, but in terms of reputation, consumer confidence and damage to the morale of the majority of staff who are honest and trustworthy.

Alongside their reputation and products or services, organisations across all sectors depend and thrive on dedicated staff. It is undoubtedly the case that the majority of these people do not commit fraud. But recognising and admitting that there is a real possibility that some staff or volunteers could be involved in fraud is the first step towards tackling it.

Employers have a duty to protect their organisation and those who work for it from internal fraud. Treating everyone as a suspect cannot be the answer. It would simply result in a culture of fear, and discourage candour. Yet the stakes are too high not to act. Internal fraud is insidious and shakes an organisation to its core, resulting in damage to morale and reputation, as well as finances.

This report examines the insider fraud recorded by organisations who shared data through the Cifas Internal Fraud Database in 2014. It also brings together a range of expert contributors to examine some of the main issues and vulnerabilities that organisations contend with. These range from the vetting of staff to whistleblowing; from identifying what is and what is not fraud to recognising that data – the lifeblood of many organisations – is now an attractive target for fraudsters. We also look at what motivates an individual to commit fraud inside their workplace, and also at calculating the true cost of fraud inside the workplace. This year's report aims to explain insider fraud; not only in terms of what has happened but why it happens and raise questions and challenges about how we can prevent it together.

Internal fraud will always exist in some form. People are just as much part of the solution as they are part of the problem. Staff and volunteers may be the greatest weakness when it comes to insider fraud – but they are also the greatest strength. Well-informed staff, who feel supported to raise concerns, are our, and your, best defence.

> Recognising and admitting that there is a real possibility that some staff or volunteers could be involved in fraud is the first step towards tackling it.

[1] http://www.pwc.com/gx/en/economic-crime-survey/

The data approach to internal fraud:

why sharing information helps combat risk

BY **SOPHIE WAPSHOTT**, CIFAS BUSINESS ENGAGEMENT MANAGER

Employers rightly want to be able to trust their staff but it is only right that they recognise the risk of internal fraud.

By using the Cifas Internal Fraud Database, organisations are able to help each other to counteract the threat of insider fraud through collaborative sharing of information on cases of confirmed fraud, including incidents of bribery and corruption. Having a strong vetting strategy in place is crucial to recruiting and retaining the right people, and key to the success of any organisation.

Throughout this report we stress that the majority of staff are honest and trustworthy. Unfortunately, there will always be individuals who make the decision to commit fraud, either while in employment or during the recruitment process. In order for any organisation to run effectively, staff will need to be placed in positions of trust. If this trust is abused, then the damage to the whole organisation can be devastating; it will almost certainly surpass any financial losses and, in the worst cases, can even lead to the closure of a business.

Organisations gain access to over **90,000** cases of confirmed fraud.

There are some simple ways to mitigate the risk. By using the Cifas Internal Fraud Database, an organisation can broaden its knowledge of an applicant's background by gaining information on whether they are confirmed to have committed a fraud against a previous employer in membership. With police resource often stretched, many fraudulent acts do not lead to prosecution, meaning that confirmed fraud will not always show up on a Disclosure and Barring Service check.

With an additional 28 organisations joining the database in 2014, and the match rate increasing by 25% compared with 2013, the benefits of membership are only growing. Cifas membership is completely cross sector, meaning that there is an opportunity for all employers to benefit from sharing their data. The membership currently includes sectors such as telecoms, call centres, public bodies and financial organisations. The cross sector principle of membership also helps to develop a wider picture of the fraud threats across the UK.

It is not only at application stage that membership of the Cifas Internal Fraud Database can improve defences against internal fraud. With organisations recording their own cases of confirmed internal fraud, there is a clear consequence to the perpetrator and, therefore, an effective deterrent. Serial fraudsters know those organisations in membership and are therefore likely to target others with lower defences.

Beyond the benefits of sharing data on confirmed internal fraud cases, organisations will also gain access to over 90,000 cases of confirmed fraud risks. These will include immigration cases filed by the Home Office, Metropolitan Police data relating to fraudulent documents and Fraudulent Royal Mail Redirections data. These all greatly add to any organisation's defence against unintentionally hiring someone who – for example – does not have the right to be residing in the UK, or who has been involved in other forms of serious criminality.

Cooperation is the key to making data-sharing work, but this is not confined to the use of a database. Organisations who use the Cifas Internal Fraud Database also have the advantage of working collaboratively through working parties, conferences and interest groups; allowing them to share current fraud threats, trends and best practice with one another. By sharing experiences and knowledge, organisations are able to develop a clearer picture of the risks and remedies when building their fraud prevention strategies.

Fraud will always be with us. Dealing with it effectively, without penalising honest employees is a challenge that all organisations must face. Cifas believes that collaboration is the key for organisations to help themselves and each other to reduce the risk.

Understanding the real costs of internal fraud

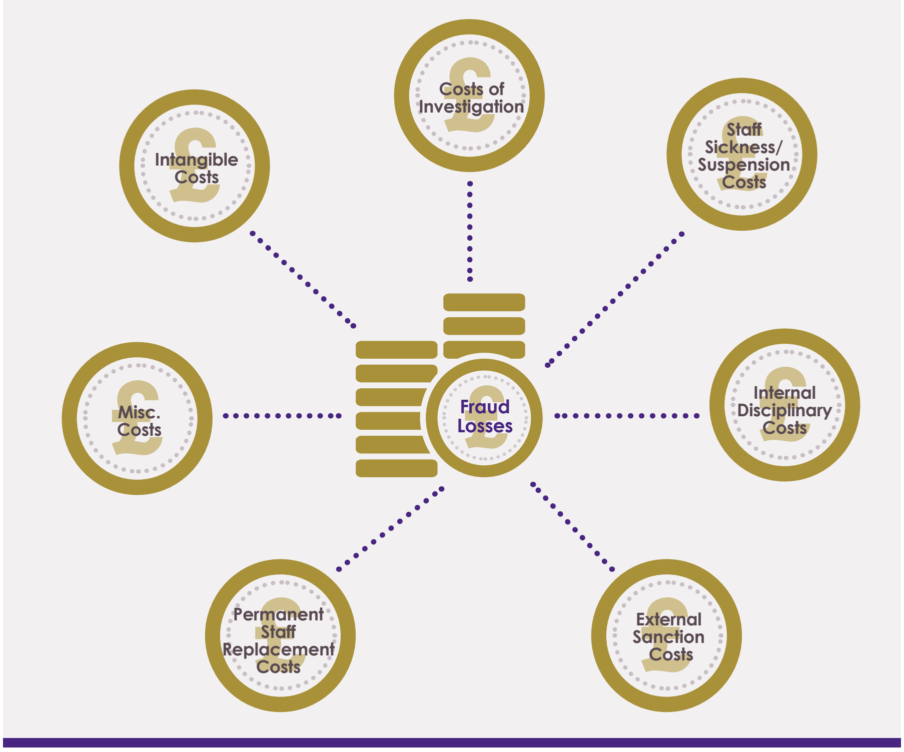
it is more than just a pound sign

BY **LYDIA VYE**, CIFAS RESEARCH ANALYST

Research carried out by the University of Portsmouth on behalf of Cifas discovered that the financial impact of an internal fraud can be several times more that the sum lost to the fraudster in the first place.

The initial losses incurred by an organisation to internal fraud are wholly quantifiable, but there are other costs incurred – which relate to the actions that the organisation takes during the investigation of the fraud. Investigations can be lengthy and costly, especially if the staff member's fraud is complex and the process becomes drawn out. Various staff members may be involved in the investigative procedure, which may mean that the organisation needs to recruit extra staff to cope with workload – another significant cost.

In addition to the costs directly associated with suspension and investigation, there are indirect impacts. Depending on the fraud committed, regulators may impose penalties on the employer. In the case of a data breach, the organisation has a duty to make provisions in order to protect their customers and their personal information from being used fraudulently. While these actions have a clear financial aspect, they also have far reaching impacts which are not just financial, but reputational too.


Costs of Investigation
Intangible Costs
Staff Sickness/ Suspension Costs
Misc. Costs
Fraud Losses
Internal Disciplinary Costs
Permanent Staff Replacement Costs
External Sanction Costs

Consumers place a great deal of trust in businesses who handle their personal finances and data. If consumers do not feel adequately protected, there is every chance that they will take their custom elsewhere. This doesn't mean, however, that the best approach is to sweep internal fraud under the carpet. Where insider fraud does occur, organisations should be open about the measures they take when dealing with it, in order to reassure customers that they take it seriously and are dealing with it appropriately. The deterrent effect of this transparency cannot be underestimated; by showing how seriously they take such frauds, organisations can make some fraudsters think twice before they act.

It is not just the customer who feels the immediate impact of internal fraud. Existing staff will also be acutely aware of the effects; from an increase in workload while investigations take place, to an overall fall in morale as, for example, the business increases its monitoring of the work undertaken by the remaining employees. Colleagues who worked closely with the internal fraudster can be hit the hardest: the resulting lack of trust in fellow employees and a reduction in team cohesion are serious issues. While it is difficult to quantify the financial costs associated with such issues, it is clear that businesses must acknowledge the fact that insider fraud has far greater implications than the single event initially carried out by the fraudster.

For lower level frauds (below £25,000), an average **265%** increase to the initial loss was incurred.

ANALYSIS

The University of Portsmouth's analysis[1] of 45 instances of internal fraud (from the private, public and voluntary sectors) in 2013 revealed the true cost of internal fraud.

- Of the cases examined, an average initial fraud loss of nearly **£424,500** was identified.
- The average total sum lost (after costs were incurred), however, was just over **£483,000**. The net difference (after the recovery of any funds from the fraudster) averaged out at a staggering **£58,696**.
- The true cost of all the frauds analysed was, therefore, **14% higher** than the initial amount lost to the fraudster.
- The smaller the fraud, the greater the proportional increase in the total cost. Frauds under £25,000 incurred costs that represented an average **265% increase** to the initial loss. This means that a £300 fraud loss will incur, on average, a £795 associated cost and a final bill of £1,095; while, a £10,000 fraud could cost over £36,000.
- Of the intangible costs, the impact upon the morale of the fraudster's former colleagues was deemed by research participants to be the greatest threat, while the impact upon the financial strength of an organisation the least threatening.

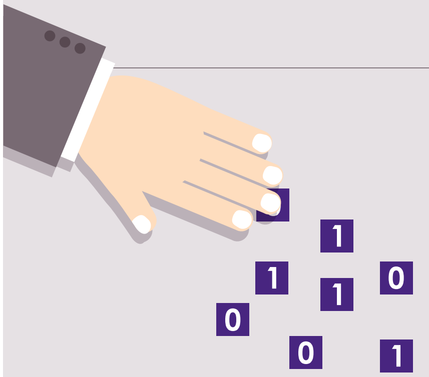
[1] Further information about the true cost of insider fraud can be found in *The True Cost of Insider Fraud* at https://www.cifas.org.uk/research_and_reports

CASE STUDY

Anatomy of a data theft

The following case is a real life example of a fraud which occurred inside one of the organisations that shares data through the Internal Fraud Database.

Please note that the name has been changed.



Eleanor Apple was considered a highly valued employee and was well thought of amongst her peers. Eleanor had been employed with the company for four years before she was found to be stealing customers' personal claims data and passing that information to a claims management company in return for cash.

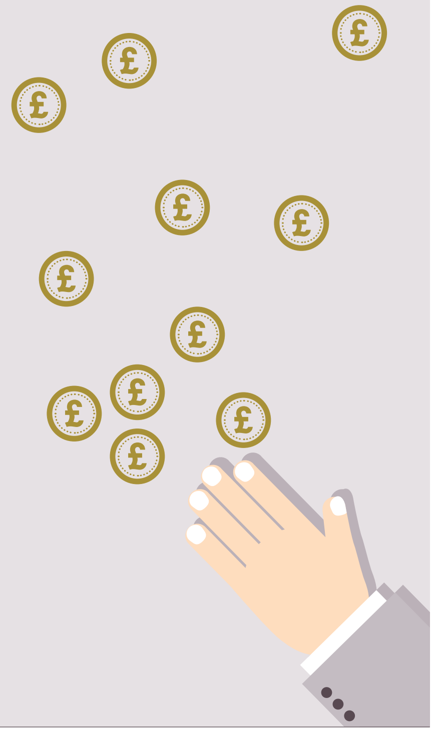
The company was alerted to the theft by a data loss prevention tool. The tool monitored outgoing emails containing customers' valuable personal data. The employee had sent a large number of emails with attachments to her personal email address. Upon investigation, it became evident that she had attempted to conceal customer information by embedding it in a variety of otherwise unrelated documents.

Further investigation revealed that:

- She admitted to stealing the data and receiving payment for it, but attempted to play down the length of time that the theft had gone on for, and the amount of money received;
- In an email to the claims management company, she positioned herself as a valuable player in stealing the data by describing herself as "excellent at her job", and stating she would "do what I can within my remit" and "the offer they had presented was too good to turn down";
- In the short period between the theft and its discovery, Eleanor had received cash payments equal to almost 50% of basic salary (an indication not only of the value of data but the attractiveness of the short term gain);
- Eleanor stated that her motivation was the desire to clear her mounting debts.

Eleanor cooperated with the investigator by giving access to her personal email account and providing bank statements showing receipt of payment from the contact at the claims management company. She was later dismissed and her details recorded to the Cifas Internal Fraud Database for unlawful obtaining and disclosure of personal data.

The case was also referred to law enforcement for investigation and she was subsequently given a suspended sentence at Crown Court.



Compulsion or seduction:

why fraudsters do what they do

BY **DR JANICE GOLDSTRAW-WHITE**, INDEPENDENT CRIMINOLOGIST

For decades people have debated about why individuals commit fraud.

I discovered from interviews with convicted fraudsters that their path to criminality is rarely straightforward. Rather, it consists of multiple reasons, triggered by numerous factors.

From my analysis of their accounts, I was able to identify two main situations that preceded them committing fraud. The first was where individuals felt they had been 'pushed' into crime. The second, where individuals felt they had been 'seduced' into it.

For those who claimed to have been pushed or compelled to behave illegally, this was usually due to pressure that they exerted upon themselves. Individuals described how they felt overwhelmed by the life issues they were facing (particularly financial ones), whether these related to their businesses, families or other pressures they put themselves under. Examples included greed, need, debts, blackmail, gambling, addiction and expectations.

When such pressurised situations occur, individuals tend to become more creative in their daily lives; looking to take advantage of opportunities that exist, turning normally law-abiding individuals into common criminals. Offenders commented about feeling trapped on a rollercoaster they could not get off and becoming so desperate they were not sure what other options there were.

Accounts of seduction, on the other hand, were identified where a person felt they were pulled into crime by other people or systems. When individuals are seduced by systems it is because they usually stumble across loopholes (such as organisational weaknesses, or other poor internal controls) of which they can take advantage. When they find out how easy this is, and get away with it, they often keep repeating the offence.

However, what we see as wrong and illegal, fraudsters may view very differently. For these people, the stigma of being labelled as a criminal is immense. Therefore, they need to try and avoid or minimise this stigmatisation, in order to preserve their power and authority and retain their social standing.

It is only natural, then, that when their characters are attacked and labelled as 'criminal' that they will fight to retain their previous good names. They do this through a mixture of self-presentations and deliberate falsifications, in an attempt to present themselves (and their acts) in a more acceptable way to society. As a result, many of the individuals I interviewed gave accounts which tried in some way to deny, rationalise or justify their behaviour; trying to distance themselves from the tag of being 'a criminal'.

> Fraudsters will always be creative in their attempts to commit crimes, and they will nearly always try and rationalise their acts either before or after the event.

A number of techniques were employed by offenders to try and neutralise their criminality[1]. These included disputing that the act was even an offence at all; distancing themselves from the act by complaining it was someone else; stating that it was no 'big deal' and claiming that those defrauded deserved it and as such, 'had it coming'. In addition, they felt that 'everyone does it' and, given the circumstances they found themselves in, it was the right thing to do. How successful these accounts are, will obviously depend on how they are received by the audience that the individual is talking to.

Fraudsters will always be creative in their attempts to commit crimes, and they will nearly always try and rationalise their acts either before or after the event. The importance of organisations having a sound and secure control environment therefore, cannot be overstated to ensure that they make this as difficult as possible for fraudsters and to minimise the loss from fraud.

*Dr Janice Goldstraw-White (**janice@goldstraw-white.com**) is an independent criminologist and accountant who runs her own management and research consultancy business, GWAssociates (**www.goldstraw-white.com**). She specialises in research relating to white-collar crime offenders and fraud. She has published a number of articles and her own book, White-Collar Crime: Accounts of Offending Behaviour, was published in 2011 by Palgrave.*

[1] As described by Sykes, G. M., & Matza, D. (1957) in Techniques of neutralization: A theory of delinquency. *American sociological review*, 664–670.

THE INTERNAL FRAUD PICTURE IN 2014:

an overview of the insider frauds recorded to the Cifas Internal Fraud Database

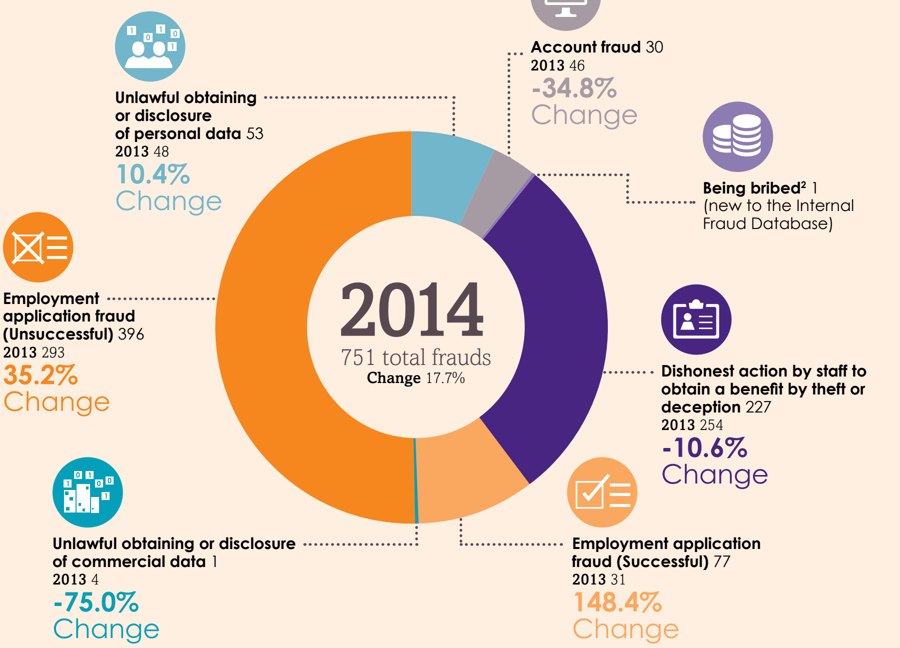
134

organisations used the Cifas Internal Fraud Database in 2014.

The Internal Fraud Database is unique as it is the only cross-sector data sharing system dedicated solely to confirmed cases of insider fraud.

As awareness of internal fraud has increased, so have the resources dedicated to countering the threat, and more organisations have joined the cooperative approach to preventing fraud. As more organisations join the database, and more frauds are filed to the database, the more our understanding of internal fraud will grow. The trends presented in this chapter may not be the whole picture on internal fraud, but they provide an important insight into the threats.

Internal Fraud by Type 2013–2014[1]



Definitions:

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

Being bribed: request, agree to receive or accept, for own or another's benefit, a financial or other advantage intending that a relevant function or activity should be performed improperly by the receiver or another person.

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

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

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

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

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

[1] As it is possible to record a single fraud under multiple fraud types, the sum of the frauds under the various types will exceed the total at the foot of the table.

[2] New to the Internal Fraud Database in 2014.

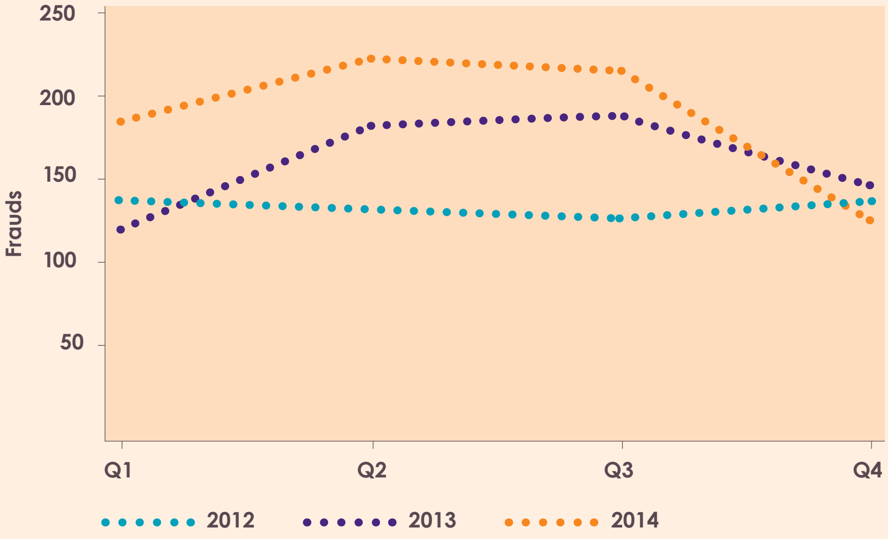
Recorded insider fraud levels increased by

18%

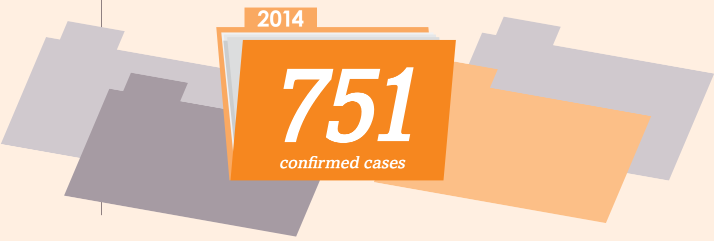
in 2014.

Insider fraud is a growing problem. There were 751 confirmed cases of insider fraud recorded by Cifas Members to the Internal Fraud Database in 2014; an increase of 18% when compared with 2013. The increase is not driven by the rise in the number of organisations sharing data in 2014.

Different fraud types increased at different rates and these trends are explored in this section. In particular the increase in personal data thefts is confirmation of data's value as a commodity for fraudsters.



Total Internal Frauds recorded 2012–2014



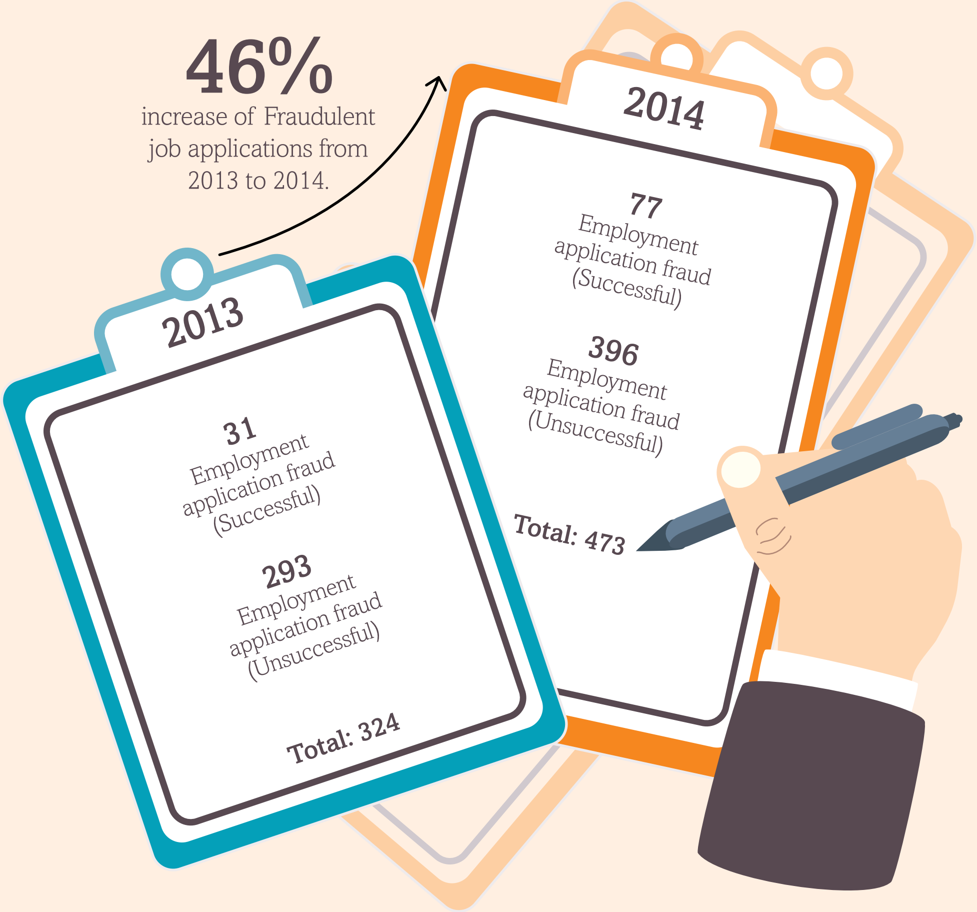
Fraudulent job applications

These are the most prevalent of all the insider frauds. These frauds increased by 46% overall in 2014 and accounted for 63% of all recorded internal frauds.

Employment Application Frauds recorded to the Internal Fraud Database are cases where the individual intentionally deceived their prospective employer, either by providing false details or omitting key information when asked, which would have an effect on whether or not the candidate would be offered the job. These frauds can be recorded as 'successful' (the applicant commenced employment before the fraud was uncovered) and 'unsuccessful' (the fraud was identified before an offer of employment was made).

46%

increase of Fraudulent job applications from 2013 to 2014.


2013
31
Employment application fraud (Successful)
293
Employment application fraud (Unsuccessful)
Total: 324
2014
77
Employment application fraud (Successful)
396
Employment application fraud (Unsuccessful)
Total: 473

Fraudulent job applications accounted for

63%

of all recorded internal frauds.

SIRA Syndicated Intelligence for Risk Avoidance

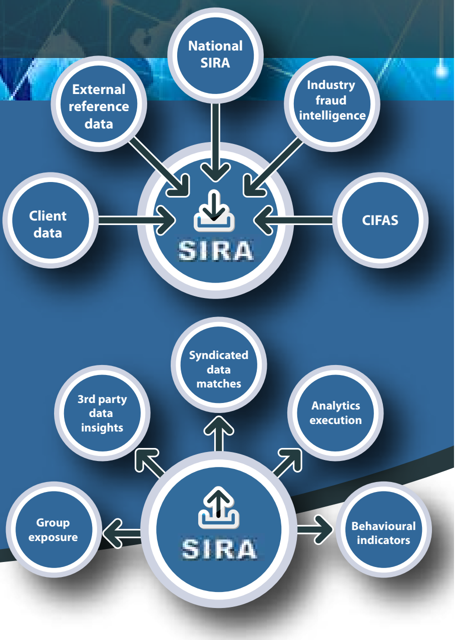
Banking & Finance Sector

SIRA Is The Leading Fraud Prevention And Detection Solution From Synectics Solutions

SIRA provides a single, integrated fraud detection and prevention system to deliver full lifecycle protection. A fully managed, hosted service solution, which eliminates multiple points of referral and streamlines working practices, SIRA places unrivalled flexibility and control in your hands at point of application and for ongoing account and transaction monitoring.

- Full Application & Transaction Lifecycle Protection
- Client Control
- Consolidated Risk
- World Of Data At Your Fingertips
- Enhanced Access
- Enhanced Scoring & Risk Ranking
- Compliance
- Value Added Modules
- Help Is At Hand

Providing A 'One World' Fraud View



Mitigate Your Fraud Risk Today:
01782 664000
sirasales@synectics-solutions.com • www.synectics-solutions.com

Synectics Solutions Ltd • Synectics House • The Brampton • Newcastle-under-Lyme • Staffordshire • ST5 0QY

SYNECTICS SOLUTIONS

Build more secure online customer relationships

Our device intelligence helps you to recognise the device and the individual to support the best service for your customers and protect them from fraudsters.

Deliver a seamless online experience with 41st Parameter, a part of Experian

Learn more:
Experian Identity and Fraud
www.experian.co.uk/41st
0844 481 5893

Experian™
Identity and Fraud

© Experian 2015.

Unsuccessful Application Fraud

There is an important distinction to be made between individuals who have made mistakes, or provided details on an application which are not considered detrimental to a successful application (a recent study estimated over 50% of all applications contained errors[3]), and those who have deceived the employing organisation knowingly. If the candidate claimed to have a particular qualification that was a minimum requirement for the role, any job offer will have been influenced by this fraudulent declaration. It is important to note that errors are not recorded to the Internal Fraud Database: only confirmed cases of fraudulent declarations.

Unsuccessful Employment Application Frauds are identified before an applicant begins a role – and, therefore, before any potential risk to the organisation occurs. These kinds of fraud accounted for 53% of all frauds on the Cifas Internal Fraud Database in 2014; making this type of fraud the most commonly recorded for two years running. The number recorded (396 confirmed cases) also represented a 35% rise from the number recorded in 2013. As organisations have increased their awareness of this issue over recent years, so too have they become better at detecting, preventing and recording such frauds.

88%

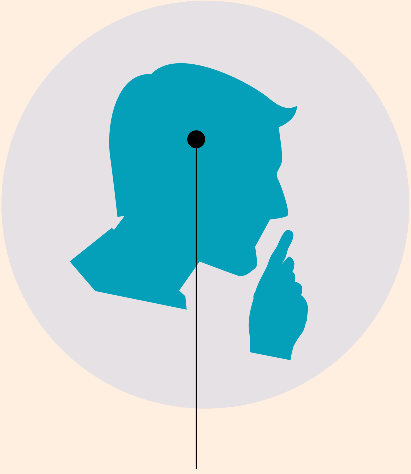
of all Unsuccessful Employment Application Frauds were attempts to conceal adverse credit history.

The driving force behind the increase in Unsuccessful Employment Application Frauds was the attempt to conceal an adverse credit history – which accounted for nearly 88% of all Unsuccessful Employment Application Frauds. Many positions, especially in regulated sectors such as financial services, have a requirement that those in the position have not run up unpaid debts, arrears or incurred county court judgements. Any attempt to conceal this will not only cause an organisation to question the reliability and trustworthiness of an applicant, it also places the organisation in the position of facing possible regulatory sanction. As a result, financial sector organisations take these frauds very seriously – explaining the very high number of frauds recorded for this reason – and also demonstrating how organisations have worked hard over recent years to introduce thorough checks in recruitment processes.

Successful Application Fraud

Although not the greatest increase in terms of absolute numbers, of all the types of internal frauds recorded to the Cifas Internal Fraud Database, Successful Employment Application Frauds increased by the greatest proportion in 2014 (rising by nearly 150%). The obvious cause for alarm here is that these are frauds that were only discovered after the applicant had commenced employment inside an organisation.

The most common reason for recording Successful Employment Application frauds in both 2013 and 2014 was the concealment of unspent criminal convictions. In 2014 these accounted for 66% of all successful employment application frauds, up from 39% in 2013. Other reasons include false references or concealed history.

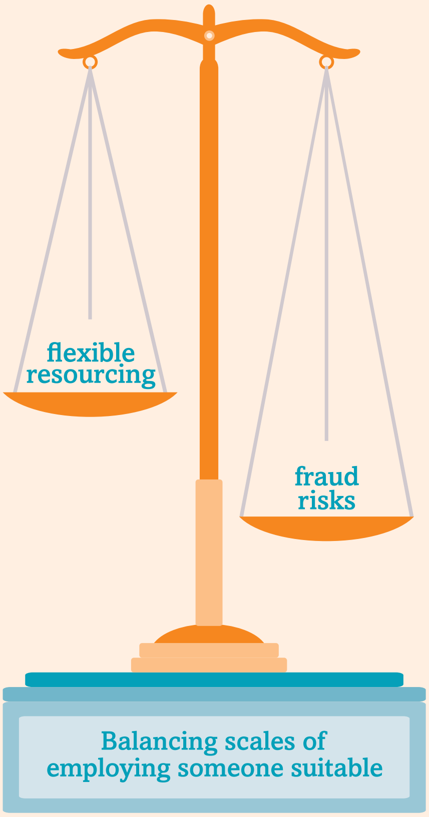


66%

of all successful employment application frauds in 2014 were the concealment of unspent criminal convictions.

If asked, when applying for a job, applicants must disclose any unspent criminal convictions. It is then up to the employer to decide whether or not they continue the application process. Criminal convictions do not mean that an individual will go on to commit insider fraud at their new workplace and should not act as barriers to future employment. Failure to declare such information when asked, however, is fraud. As with undisclosed adverse credit, any attempt to conceal information on an unspent conviction will also call into question the integrity of an applicant. Fundamentally, honesty remains the best policy.

In order to safeguard themselves against the risk of employing someone who has committed application fraud, organisations need to have recruitment process that allow verification checks (such as the Disclosure and Barring Service and Cifas Internal Fraud Database) to be completed before the applicant starts in the role. Analysis of Successful Employment Application Frauds recorded in 2014, however, shows that on average the frauds were uncovered around two months after the applicant had started in the role. This indicates that many positions are being filled before full checks and vetting procedures have been completed. The question for organisations, therefore, is are they happy with the risk they take that they may employ someone whom they later feel is unsuitable? And how can they strike the right balance between flexible resourcing and fraud risks?



[3] http://www.telegraph.co.uk/finance/jobs/11421053/Why-you-should-never-trust-what-you-read-on-a-CV.html

FOCUS ON

Data theft: smaller numbers, bigger danger

There were 54 cases of the unlawful theft or disclosure of data (both personal and commercial) by employees recorded to the Cifas internal fraud database in 2014.

While the number of these frauds is not high, the impact of these thefts upon organisations can be. Illegally stolen data is the main driver behind identity theft. An organisation's IT systems can be hacked, data lifted, sold and re-sold in an industrialised process between many parties. Data is as valuable as cash itself.

Identity fraud depends on compromised personal data.

The theft and disclosure of personal data is a growing and serious issue.

In 2014, the Cifas National Fraud Database – which contains confirmed fraud data – had 114,000 cases of identity fraud (where the fraudster uses personal data to obtain products and services in an innocent victim's name) filed. This is a 5% increase from the number recorded in 2013 and represented 41% of all recorded fraud in 2014. This follows several years where identity fraud levels have constituted the majority of recorded fraud.

The reality

In 2007, the customer data of TX Maxx was subject to a hack by outsiders, which led to the loss of 45 million customer records. Four years later, the Sony Playstation Network was hacked and 77 million accounts affected (Sony is reported to have lost millions, while the site was down for a month). Organisations are increasingly accustomed to protecting themselves against attack from outsiders. But are the vulnerabilities inside an organisation equally understood?

The simple fact is that one case of data theft can involve hundreds, if not thousands, of records. While it is common knowledge that measures such as firewalls, spam filters and anti-virus protection need to be put in place around an organisation's IT infrastructure, what use is it when the inside of an organisation has a less comparable set of defences? What protects the data inside the organisation from an insider determined to steal it? After all, if cash can be stolen by both an external attacker and an insider, then data can also be compromised in the same ways.

> Data is as valuable as cash itself.

The dangers for any organisation

Any organisation that has customer data has it for a reason. There will be people inside the organisation who need to refer to it on a daily basis, so simply blocking access to it is not an option. But – in what ways can data be accessed? Can it be downloaded or extracted from an internal system and saved into a spreadsheet? If so, what is stopping that spreadsheet from being emailed outside the organisation or saved onto a USB stick for onward circulation?

Let's go further: does everyone with access to such data even need it? Are the systems used to access and see data monitored and audited? If not, how will an organisation know whether an individual is accessing systems outside of working hours? Furthermore, the smartphone itself represents a new danger. With many organisations using the 'bring your own device' approach, can this system be abused to access data and pass it on?

1 case of data theft

=

1000s of individuals potentially put at risk

In December 2014, Symantec reported that data on a stolen credit card could sell in online criminal forums for up to $20.

With organised criminals known to target employees in an effort to force them to divulge data, the challenge for every organisation is to make sure that they deploy sophisticated protection against both the internal and external threat.

Personal data theft a growing concern

Although the numbers remain small, theft of personal data increased by 10% last year.

Such frauds may only constitute 7% of all frauds recorded in 2014, but they are likely to have a long lasting and toxic impact; especially considering that the resale of personal data fuels identity fraud.

Of the 53 recorded cases of personal data theft, more than a half involved the disclosure of data to a third party – with one fifth recorded for the employee's fraudulent personal use of customer data.

Criminal gangs have been known to place individuals inside an organisation specifically to obtain and steal data, or they have targeted existing employees and used bribery, threats and coercion to pressurise the staff member into acting as an accomplice (although those that have suffered coercion are not recorded to the Internal Fraud Database).

A handful of individuals were in position for a long time (the highest being 14 years) but over half (61%) were employed for less than three years. Being in position for a long time might help insider fraud threats get a better insight into the policies and workings of an organisation as well as any potential weaknesses that might be exploited. Understanding whether these cases involve a 'previously good employees gone rogue' or a long standing 'planted' associate of an external gang will be crucial to organisations as they tackle this problem.

Dishonest actions

Prior to 2013, Dishonest Actions had been the most common type of internal fraud recorded on the IFD. In 2013, however, it was overtaken by Unsuccessful Employment Application Fraud; a trend that continued into 2014 with Dishonest Actions now accounting for one third of total internal frauds recorded. This suggests that many organisations have implemented better systems to detect fraud.

Despite the fall in volume, there has been little change in the types of Dishonest Actions carried out by employees. Theft of cash is still the most common reason for recording these frauds (theft of cash from customers made up 25% of Dishonest Actions, while theft of cash from employers accounted for slightly less at 18%) but there has certainly been a reduction in the prevalence of these crimes. The figures reported here tie in with the findings of the British Retail Consortium's Retail Crime Survey[5] which reported a fall for the second year running in employee theft in 2014 after a peak in 2010–2011. This signifies quite a substantial change in behaviour; far fewer fraudsters are attempting to defraud their employees by this method and the question is: why? It is clear that both organisations and consumers have been becoming increasingly aware of internal fraud, with many companies becoming more open about the fact that internal fraud exists and that it must be dealt with in an effective manner. Theft of cash is perhaps one of the simplest frauds an employee can commit, but at the same time, one of the least subtle. Many fraudsters might be of the opinion that they are far more likely to get caught thieving cash (either by their employer or the customer) than, for example, manipulating their own personal account.

Theft of cash is perhaps one of the easiest frauds an employee can commit.

Manipulation of personal accounts was the only sub-category of dishonest actions to rise last year (rising by just over 23%). The manipulation of third party accounts and the fraudulent facilitation of transactions also remained relatively high in 2014, highlighting the fact that these types of fraud have not slowed quite as much as the theft of cash. The extent to, and reason for, which an individual will have manipulated their account will vary. A more opportunistic individual might have accidentally incurred a charge on their account and subsequently realised that they have the ability, as an employee, to reverse those charges. Other fraudsters, however, might deliberately go over their overdraft, safe in the knowledge that they can easily remove these charges at a later date.

Reasons for Recording Dishonest Actions in 2013–2014

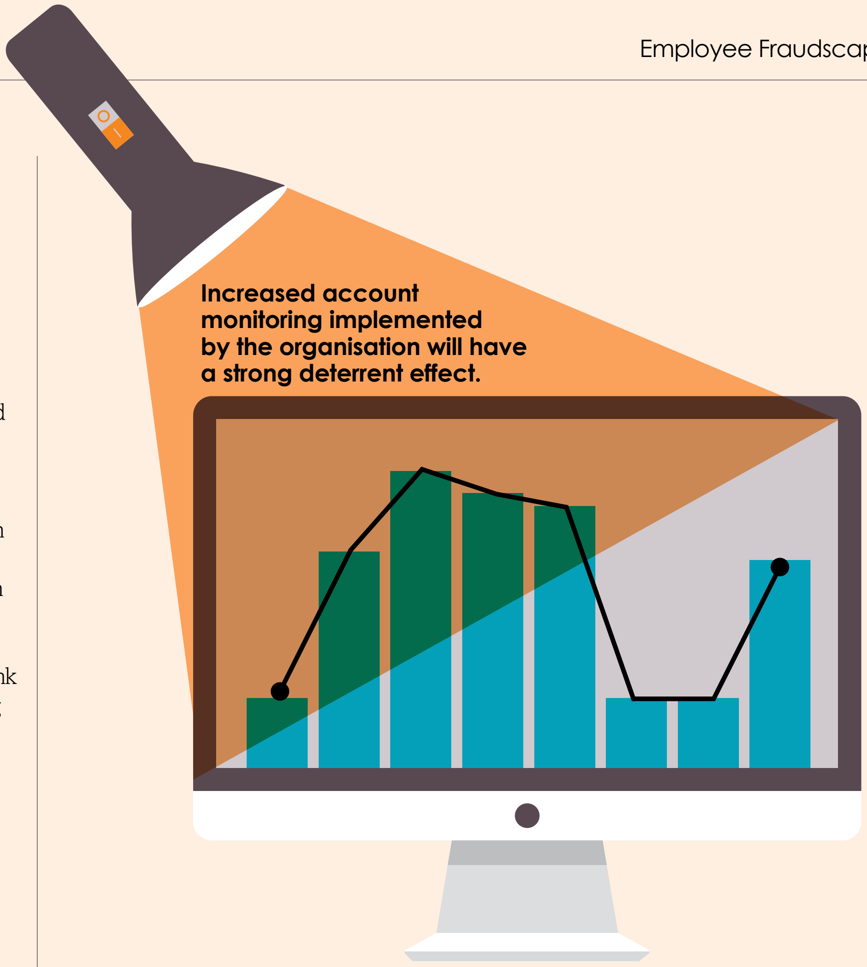
	2013		2014		
REASONS FOR FILING	CASES	% OF TOTAL	CASES	% OF TOTAL	% CHANGE
Theft of cash from customer	86	33.9%	57	25.1%	-33.7%
Theft of cash from employer	57	22.4%	41	18.1%	-28.1%
Manipulation of a third party account	35	13.8%	33	14.5%	-5.7%
Facilitating transaction fraud	30	11.8%	23	10.1%	-23.3%
Manipulation of personal account	17	6.7%	21	9.3%	23.5%
Facilitating fraudulent applications	21	8.3%	19	8.4%	-9.5%
Manipulation of applications/ proposals/claims	14	5.5%	14	6.2%	0.0%
Perpetrating fraudulent applications	15	5.9%	12	5.3%	-20.0%

[5] www.brc.org.uk/brc_policy_content.asp?id=263&iCat=48&iSubCat=646&sPolicy=Retail

Account fraud

There was no single reason for recording account frauds in 2014, with fraudulent account withdrawals, fraudulent account transfers to an employee account and fraudulent account transfers to a third party account making up just over a third of filings each. Tighter controls and increased account monitoring implemented by organisations will have a strong deterrent effect on those considering carrying out an Account Fraud. Also, the increased ease with which consumers can now control activity on their bank accounts (for example, through online banking, mobile banking and text alerts), is likely to discourage insiders from committing blatant internal fraud. If they think that there is any chance of the victim finding out, then they generally will not risk it.

Where Account Fraud was attempted, the targeted individual was often elderly or vulnerable, which is likely to minimise the chances of the fraud being discovered.



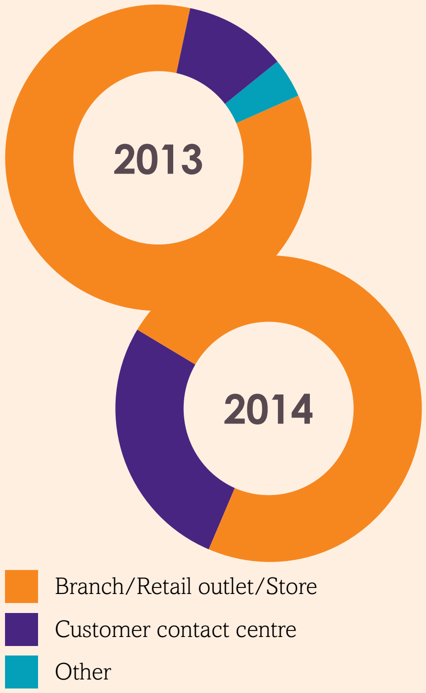
Increased account monitoring implemented by the organisation will have a strong deterrent effect.

In some instances, when challenged, the internal fraudster blamed the victim in some way, often claiming that they 'must be mistaken' or that they 'must have forgotten' about withdrawing their own money.

The average length of service for an internal fraudster committing Account Fraud in 2014 was 5.3 years.

Most people think of the internal fraudster as working in direct contact with customers on a daily basis, for example in a branch or retail environment. This is not always the case, however, as there are many more roles undertaken by staff members who need access to customer data but who work 'behind the scenes'. For many roles in, for example, head office or organisational support roles, the need for staff members to have access to personal customer data is limited, if not non-existent, meaning that access is easily restricted by employers. For employees working in either an organisation's customer contact centre, or an outsourced contact centre, however, there is a business need for access to customer personal data and accounts because, in order to do their job, these employees need this level of access. Wherever these employees have this access, the organisation will be exposed to internal fraud risks. This is illustrated by the fact that in 2014, although Account Fraud decreased, the proportion of Account Frauds carried out from within a customer contact centre actually increased by 27%, highlighting the need for contact centre employees to be subject to just as much scrutiny as branch and office-based employees.

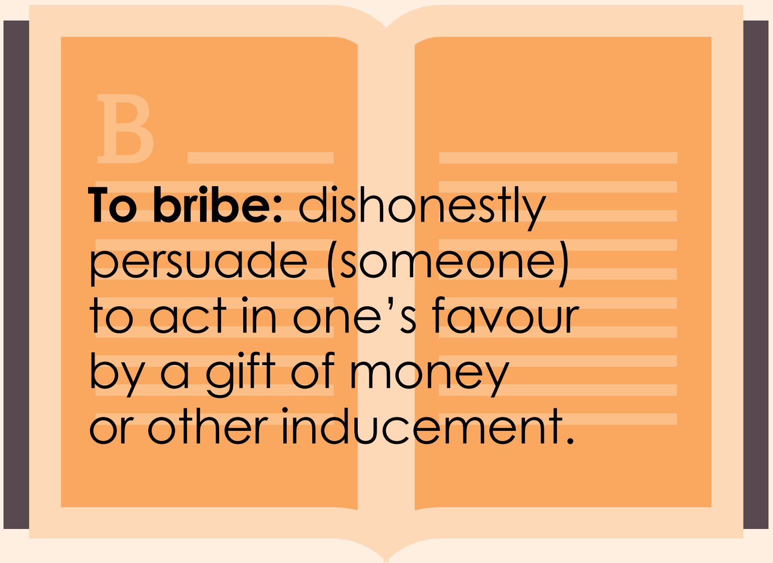
Proportions of Account Frauds by Business Area in 2013–2014



Reasons for Recording Account Fraud in 2013–2014

	2013		2014	
REASONS FOR FILING	CASES	% OF TOTAL	CASES	% OF TOTAL
Fraudulent account withdrawal	23	50.0%	11	36.7%
Fraudulent account transfer to third party account	16	34.8%	11	36.7%
Fraudulent account transfer to employee account	14	30.4%	11	36.7%

Bribery



To bribe: dishonestly persuade (someone) to act in one's favour by a gift of money or other inducement.

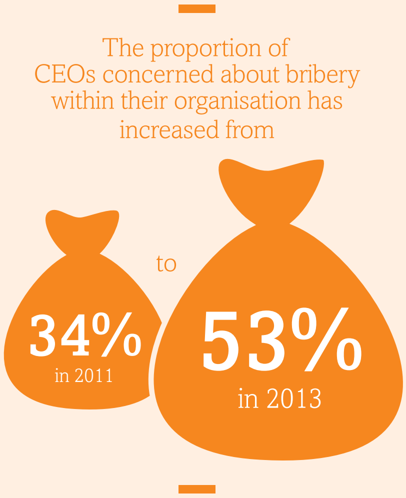
There is one aspect of internal fraud which has not previously been captured on the Internal Fraud Database: bribery. In 2014 this changed with the introduction of three new fraud types: 'Being bribed', 'Bribing another person' and 'Bribery of a foreign public official', and towards the end of 2014, the first case of an individual being bribed was recorded to the database. The fraud types were chosen to reflect the separate crimes detailed under The Bribery Act 2010, which replaced all previous statutory and common law provisions in relation to bribery.

There are still major differences in global attitudes towards bribery and what constitutes an offence, with the giving of gifts or incentives seen as almost a 'normal' part of doing business in some countries. It is this attitude that many organisations are working hard to change; especially now with such serious ramifications for both businesses and individuals should they be found to be engaging in these activities. Organisations have a criminal responsibility to ensure that they implement 'adequate procedures' to stop employees from being involved in bribery and corruption; one such procedure could be to partake in a data sharing scheme designed to detect and prevent bribery, such as the Internal Fraud Database.

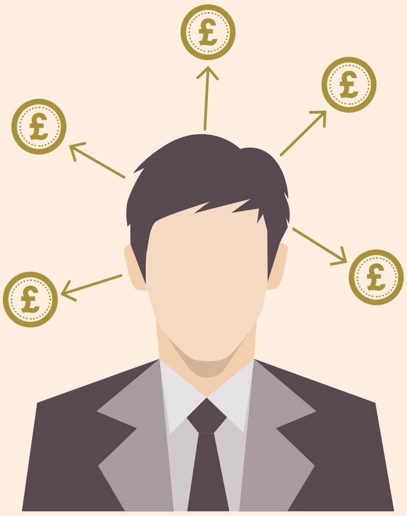
Bribery can affect almost any area of any business and although it is not currently the most highly reported type of internal fraud, it has the potential to cause immense damage (both in a financial or reputation context). This could be the reason behind the rise in concern surrounding bribery and corruption, as reported in the 2014 PWC Global Economic Crime Survey*.

According to respondents from the CEO survey, the proportion of CEOs concerned about bribery within their organisation has increased from 34% in 2011 to 53% in 2013, showing that there is an ever greater senior level focus on these types of fraud. With a greater involvement from CEOs and senior management, organisations have the opportunity to 'lead by example' when tackling bribery and corruption in the workplace. Setting, implementing and promoting clear policies and raising the level of awareness throughout all areas of a business can be exceptionally effective in tackling this type of fraud.

*http://www.pwc.com/gx/en/economic-crime-survey/bribery-corruption.jhtml



Being bribed



Bribing another person

Bribery of a foreign public official

The world of degree fraud

when qualifications are not what they seem to be.

BY **JAYNE ROWLEY**, DIRECTOR OF PROSPECTS AND LEADER OF THE HIGHER EDUCATION DEGREE DATACHECK (HEDD) INITIATIVE

According to a recent report in the Daily Telegraph, graduates earn significantly more in their working lifetime than someone who did not attend university.

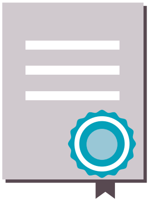
Degrees are clearly a valuable commodity, which may explain why some people are prepared to misrepresent their qualifications. In fact, in a HEDD survey in 2014, one third of students and graduates say they know someone who has lied on their CV, with the qualifications being the most common lie.

There are three broad types of degree fraud: bogus universities and degree mills, fake certificates, and individual fraud.

Bogus universities and degree mills:

Bogus universities and degree mills operate purely to make money – from enrolment fees, premium phone lines, course fees and 'life experience degree' awards. In doing so, they provide a means for fraudsters to obtain authentic-looking degrees and associated documentation from unaccredited institutions.

This type of fraud is becoming more sophisticated, with credible websites and verification services often modelled on their authentic counterparts – including the direct lifting of content and sections of material from genuine university websites.



Fake certificates:

There are also a multitude of websites offering 'novelty' or 'replacement' degree certificates for as little as £30. These websites carry disclaimers about not using the documentation to make fraudulent misrepresentations in order to avoid prosecution. However, they are breaching the copyright and trademarks of the universities whose certificates they are imitating.

Individual fraud:

Individual fraud is when someone falsely creates a certificate or alters a genuine document from a real university – changing the name, subject, qualification, or classification – and presents the documents as real. These are harder to spot, as they are based on real certificates. The only way to verify their authenticity is to check with the issuing institution or HEDD. Presenting this documentation as genuine in job applications constitutes fraud by misrepresentation and can lead to prosecution resulting in a prison sentence of up to ten years.

HEDD is the UK's official degree verification service, protecting UK graduates, universities and employers from degree fraud. Since 2009, HEDD has helped identify more than 180 bogus universities, it has undertaken 55,000 verification checks and 5% have been returned unverified. That's more than 2,700 people submitting incorrect information to would-be employers.

For more information visit **www.hedd.ac.uk**

180

Bogus universities identified

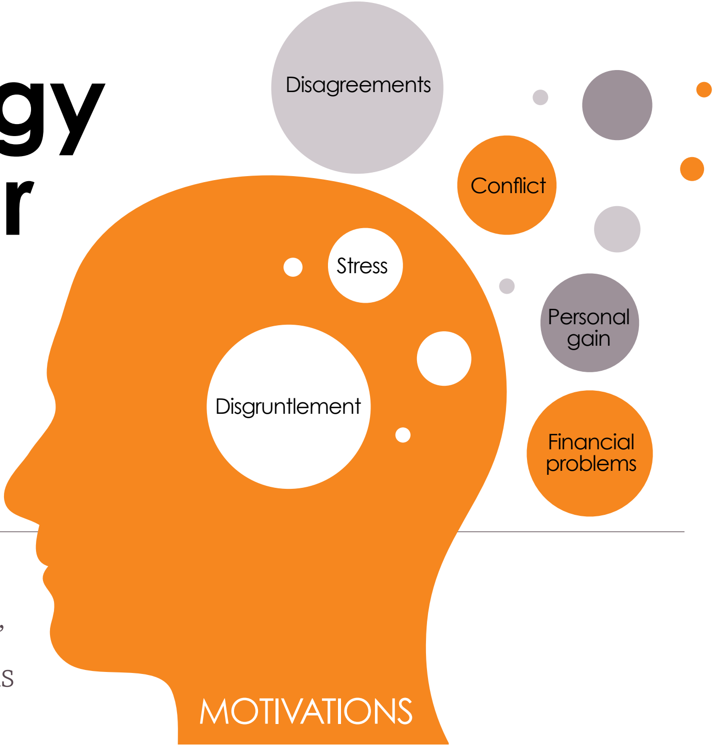
2,700

people found submitting incorrect information

The psychology of the insider

trying to understand it

BY **PROFESSOR MONICA WHITTY**, UNIVERSITY OF LEICESTER



Understanding the human element of the 'insider' problem is crucial if we are to find effective means to detect, deter and prevent this crime.

Very little scholarly work is available on the personality and psychological characteristics of insiders. This brief report provides a summary of the literature in this area and highlights some key points from our own research conducted on insiders. An insider is understood here to be a person or group of people who work for an organisation that deliberately harms that organisation.

In general, researchers have claimed that insiders are typically: risk-taking, impulsive, manipulative, narcissistic, self-deceptive, defensive, emotionally unstable, have low self-esteem, amoral, unethical, prone to fantasising and lack conscientiousness (Turner & Gelles, 2003; CPNI, 2013). The motivations behind an insider attack include: disgruntlement, personal gain, stress, financial problems, disagreements or conflict with co-workers (CPNI, 2013; Moore et al., 2011; Shaw & Stock, 2011). In our own work, which examined 99 case studies of insider attacks (76 of which were frauds), we found similar findings, including:

- Insiders appeared to be narcissistic (i.e. a person who has a sense of entitlement and seeks admiration, attention, prestige and status) and Machiavellian (manipulative, charming and highly ambitious).
- Insiders could be either high or low in terms of conscientiousness. Those who were highly conscientious were more inclined to be motivated because something happened in the organisation that lead to them becoming disgruntled (e.g., missed out on promotion).
- Some insiders were impulsive – especially those who were addicts (drug, alcohol, shopping).
- We also found that many of the insiders, in hindsight, seemed very stressed at the time (some of these experiencing a personal life issue outside of their workplace).

Although case studies where line managers, HR, security, co-workers and the insiders themselves are interviewed are a useful method to tap into the psychology of an insider, they have shortcomings. Observations can be unreliable and fellow co-workers and employers can miss important details. Given this limitation, we carried out a second study where we traced employees' attitudes towards work, counter-productive behaviours and emotional states across time.

In this second study, we followed these people over nine months, asking them to complete survey data at three-month intervals. At the outset of the study, we also obtained their psychological characteristics. Asking the individuals themselves about their personality and their current emotional state and behaviour, can arguably provide more valid and reliable data. Moreover, insiders are known to engage in counter-productive workplace behaviours (some of which are attacks themselves) and so, rather than directly ask participants if they had committed a crime (something they might not have admitted to), we asked them to complete a survey that is commonly used by organisations. This work allowed us to narrow down the list of key personality characteristics to: 'Narcissism', 'Low on Agreeableness (personality trait manifesting itself in characteristics that are perceived as kind, sympathetic, cooperative, warm and considerate)'; highly anxious and less impulsive individuals (i.e., those who scored high on 'Lack of Premeditation'). Notably, stress did not appear to be a predictor. Low impulsivity was contrary to previous findings and theories about insiders. In hindsight, however, this might be explained by the fact that many insider attacks need time and planning if the criminal is to successfully execute the crime (especially for crimes such as internal fraud). We also found that individuals whose exchange commitment (i.e., those who felt their efforts has been recognised by the organisation) changed from high to low were more likely to engage in counter-productive workplace behaviours.

Overall, both these studies revealed some new findings about the psychological make-up of insiders. Importantly, they suggest that they is no easy answer, or simple psychological profile. We need to consider a more complex mix of personality, emotional state, and employees' attitudes towards work, if we are to improve detection, deterrence and prevention methods.

> There is no easy answer, or simple psychological profile.

The importance of being consistent:

vetting and screening high-level staff

BY **DANIEL COOK**, CIFAS INTERNAL FRAUD COMPLIANCE OFFICER

In terms of managing risk and fraud within an organisation, it is important that the board and senior management set both the policy and the example to the rest of the organisation and show that there is a zero tolerance approach.

Fraud prevention and detection

Showing that the very top levels of an organisation are committed to preventing and detecting fraudulent and unethical behaviour, has a trickle-down effect on the rest of the organisation.

Crucially, this means that senior managers, board members and other high-level staff practice the same policies as the rest of the organisation. It should not be forgotten that it is not just call centre workers, branch staff and contractors that have the ability and inclination to commit fraud. It is just as often someone who knows the organisation and its practices inside out, and has the trust to be able to manipulate systems without as much scrutiny.

The Association of Certified Fraud Examiners found (in their 2014 global fraud study, Report to the Nations) that the higher an internal fraudster's level of authority within an organisation, the greater the fraud losses tended to be. Whereas lower level employees might account for a higher percentage of frauds, those committed by executives and other senior level staff caused a median loss of over £300,000; six times greater than the median loss of about £50,000 caused by less senior staff[1]. Similarly worrying is the Foreign Bribery Report (released by the Organisation for Economic Co-operation and Development in 2014). This found that, in the 41 countries involved in the study, senior managers were involved in 41% of the bribery and corruption cases involving foreign public officials with CEOs involved in a further 12%[2].

These reports demonstrate the importance of treating senior staff in the same way as other staff, and recognising that seniority does not mean there is less of a threat. If senior staff are found to be involved in fraud, they must be also be dealt with in a similarly severe way. Organisations must not try to 'sweep the case under the carpet' by dealing with it quickly and quietly, in an effort to avoid the reputational damage that could arise. Such cases need to be treated in line with any policy applied to lower level staff: if a theft from a customer account would be reported to the police, then a case of intellectual property theft or bribery by a senior manager must also be reported to law enforcement. Failure to do so will be counter-productive; staff will see that some are not dismissed or prosecuted, and resentment and temptation can arise.

The equal implementation of preventative measures is also vital. Vetting procedures should be implemented across all levels of an organisation. Having an employee that is found to be involved in dishonest actions is troubling enough, but when it is a Director the consequences can be even higher. These range from detrimental effects on the public image of the organisation to employees feeling disenfranchised by seeing what 'their bosses' have done. It also begs the question: why didn't the organisation feel it was necessary to screen them to a suitably high standard?

The reality is that there no one-size-fits-all profile of an internal fraudster. Having a consistent approach to screening and counter fraud policy is crucial.

Less senior staff
£50,000
Executives and other senior level staff
over £300,000
Executives and other senior level staff generate a loss six times greater than less senior staff.
CEO

[1] http://www.acfe.com/rttn-summary.aspx

[2] http://www.keepeek.com/Digital-Asset-Management/oecd/governance/oecd-foreign-bribery-report_9789264226616-en#page1

Top tips on whistleblowing

When trying to guard against the risk of fraud committed by an insider, organisations must remember that their staff are not just those who might commit fraud. Staff are also the first line of defence.

Whistleblowing is a concept that many recognise is a vital part of any fraud management strategy, and yet is one that is fraught with difficulties. Reports over the last few years have often been accompanied by stories of the whistleblower being harassed, disciplined and even dismissed for raising concerns that were ultimately proved to be correct. In order to make effective use of whistleblowing as a guard against unethical or criminal behaviour, organisations need to take certain points into consideration.

1 Have clear policies and procedures for whistleblowing.

Ensure that the organisation has a framework and policy for dealing with whistleblowing, and that this is written down and accessible by all staff. Ensure that any policy is easy to understand and contains no ambiguities: any such ambiguities will dissuade staff from raising concerns.

2 Publicise and promote the policies and raise awareness.

So you have a policy in place. Are your staff aware of this? If not, then the policy will never work. Ensure that people know that a policy is in place and that it is acceptable to raise legitimate concerns.

3 Make sure that whistleblowers feel supported and accepted.

Nobody will come forward if they lack confidence in either the reporting mechanism or how the report will be dealt with. Neither will they come forward if they instantly feel that they are the ones under suspicion as opposed to those engaged in possibly criminal activity. Treat reports seriously and, most importantly, treat those making a report seriously; don't risk them feeling ostracised.

4 Promote confidentiality over anonymity – lowers the risk of malicious or inaccurate cases.

In order to mitigate against whistleblowing procedures being used maliciously, confidentiality rather than anonymity is key. Anonymous tip offs could cause more harm than good. A confidential one has more chance of being taken forward as the individual can state their case and yet feel protected against potential harassment – as the information will not go beyond the relevant parties.

5 Monitoring: keep your defences under review.

There is a policy, a hotline and a clear set of guidance notes. Have you checked that your staff really are aware? Keep checking: has the message got through? If cases of internal fraud are not reported to a whistleblowing hotline, does this mean that there is a cultural reluctance to report, or does this indicate a problem with the policy as it exists? Equally, if reports were received by a whistleblowing line, what was done with these reports?

Ensure that people know that it is acceptable to raise legitimate concerns.

Staying one step ahead:

instilling an anti-fraud culture

BY **RACHAEL TIFFEN**, HEAD OF CIPFA COUNTER FRAUD CENTRE AND GOVERNANCE

When it comes to corruption, money laundering, asset misappropriation and cyber-crime, keeping one step ahead of the fraudsters is a significant challenge at the best of times.

But in the current, rapidly-changing environment this is even more difficult; especially when faced with challenges from within your own organisation.

In the public sector, recent developments have created a clear skills gap while budget cuts continue to affect counter fraud capabilities; often seen as a back-office function. Tackling fraud is not always a top priority when attempting to protect the services and practices that are more visible to the public.

Creating an anti-fraud culture is therefore vital and begins with establishing the right 'tone from the top'. This means a clear commitment to transparency, led by the Executive Board and including zero tolerance to fraud in your organisation's 'ethical mission statement', or strategy document, reinforcing expected standards in public service.

An anti-fraud culture also comes from making sure that any dedicated counter fraud staff have the right skills and expertise; countering fraud is now a recognised profession and those accredited by the University of Portsmouth's Counter Fraud Professional Accreditation Board are central to creating a robust culture because they share a common 'language', skills and knowledge, methodologies and a commitment to best practice.

> Understanding the fraud and corruption risks faced by your organisation is crucial.

Countering fraud and creating the right culture is everyone's business: from trained counter fraud specialists through to the procurement team, HR personnel, facilities staff and beyond. Ideally counter fraud activity should be embedded into the day-to-day running of your operations and your existing internal communications tools will help to raise awareness of the potential threats and to make sure staff know how to respond to them.

Having the right anti-fraud policies and procedures in place, ones relevant to the size and nature of your organisation, is also important as part of an anti-fraud culture. A general fraud policy that includes guidelines on what to do when suspicions of fraud arise, a response plan, details of gift and hospitality registers and, where appropriate, mandatory declarations of interest is an excellent place to start. A visible and well-articulated whistleblowing policy is also key to creating an anti-fraud culture.

Understanding the fraud and corruption risks faced by your organisation is crucial to creating an anti-fraud culture because these will determine the type of framework you need to put in place. Scanning the horizon for new threats is also necessary. Fraud is constantly changing and evolving and scams often target frontline staff. From vishing to phishing, cyber fraud to mandate fraud, what may seem low risk today may turn into high risk in the future.

ANTI-FRAUD CULTURE

Commitment to transparency

Zero tolerance

Dedicated counter fraud staff

Finally, sharing and publicising the outcomes of successful investigations or incidences where an anti-fraud measure has worked sends a powerful message that fraud doesn't pay. As well as being a deterrent, it can lead to an increase in referrals and whistleblowing, which are indicators that the anti-fraud culture in your organisation is working.

Appendix

As it is possible to record a single fraud under multiple fraud types, and record a fraud for multiple reasons for filing, the sum of the frauds under the various types exceeds the total of 751 frauds recorded.

Internal Fraud by Type 2013–2014

	CASES		
FRAUD TYPE	2013	2014	% CHANGE
Account fraud	46	30	-34.8%
Being bribed*	-	1	-
Dishonest action by staff to obtain a benefit by theft or deception	254	227	-10.6%
Employment application fraud (Successful)	31	77	148.4%
Employment application fraud (Unsuccessful)	293	396	35.2%
Unlawful obtaining or disclosure of commercial data	4	1	-75.0%
Unlawful obtaining or disclosure of personal data	48	53	10.4%
Total Frauds	**638**	**751**	**17.7%**

* New to the Internal Fraud Database in 2014

Reasons for Recording Account Fraud in 2013–2014

	2013		2014		
REASONS FOR FILING	CASES	% OF TOTAL	CASES	% OF TOTAL	% CHANGE
Fraudulent account withdrawal	23	50.0%	11	36.7%	-52.2%
Fraudulent account transfer to third party account	16	34.8%	11	36.7%	-31.3%
Fraudulent account transfer to employee account	14	30.4%	11	36.7%	-21.4%

Reasons for Recording Dishonest Actions in 2013–2014

	2013		2014		
REASONS FOR FILING	CASES	% OF TOTAL	CASES	% OF TOTAL	% CHANGE
Theft of cash from customer	86	33.9%	57	25.1%	-33.7%
Theft of cash from employer	57	22.4%	41	18.1%	-28.1%
Manipulation of a third party account	35	13.8%	33	14.5%	-5.7%
Facilitating transaction fraud	30	11.8%	23	10.1%	-23.3%
Manipulation of personal account	17	6.7%	21	9.3%	23.5%
Facilitating fraudulent applications	21	8.3%	19	8.4%	-9.5%
Manipulation of applications/proposals/claims	14	5.5%	14	6.2%	0.0%
Perpetrating fraudulent applications	15	5.9%	12	5.3%	-20.0%
False expenses submission	7	2.8%	11	4.8%	57.1%
Removal of charges from personal account	4	1.6%	9	4.0%	125.0%

Reasons for Recording Successful Employment Application Fraud in 2013–2014

	2013		2014		
REASON	CASES	% OF TOTAL	CASES	% OF TOTAL	% CHANGE
Concealed unspent criminal convictions	12	38.7%	51	66.2%	325.0%
Concealed employment history	11	35.5%	11	14.3%	0.0%
Concealed employment record	4	12.9%	7	9.1%	75.0%
False references	3	9.7%	4	5.2%	33.3%
False qualifications	2	6.5%	3	3.9%	50.0%
Concealed spent criminal convictions	2	6.5%	2	2.6%	0.0%
Concealed adverse credit history	0	0.0%	2	2.6%	-
False documents	4	12.9%	1	1.3%	-75.0%
Concealed address with adverse	0	0.0%	1	1.3%	-
False immigration status	1	3.2%	0	0.0%	-100.0%

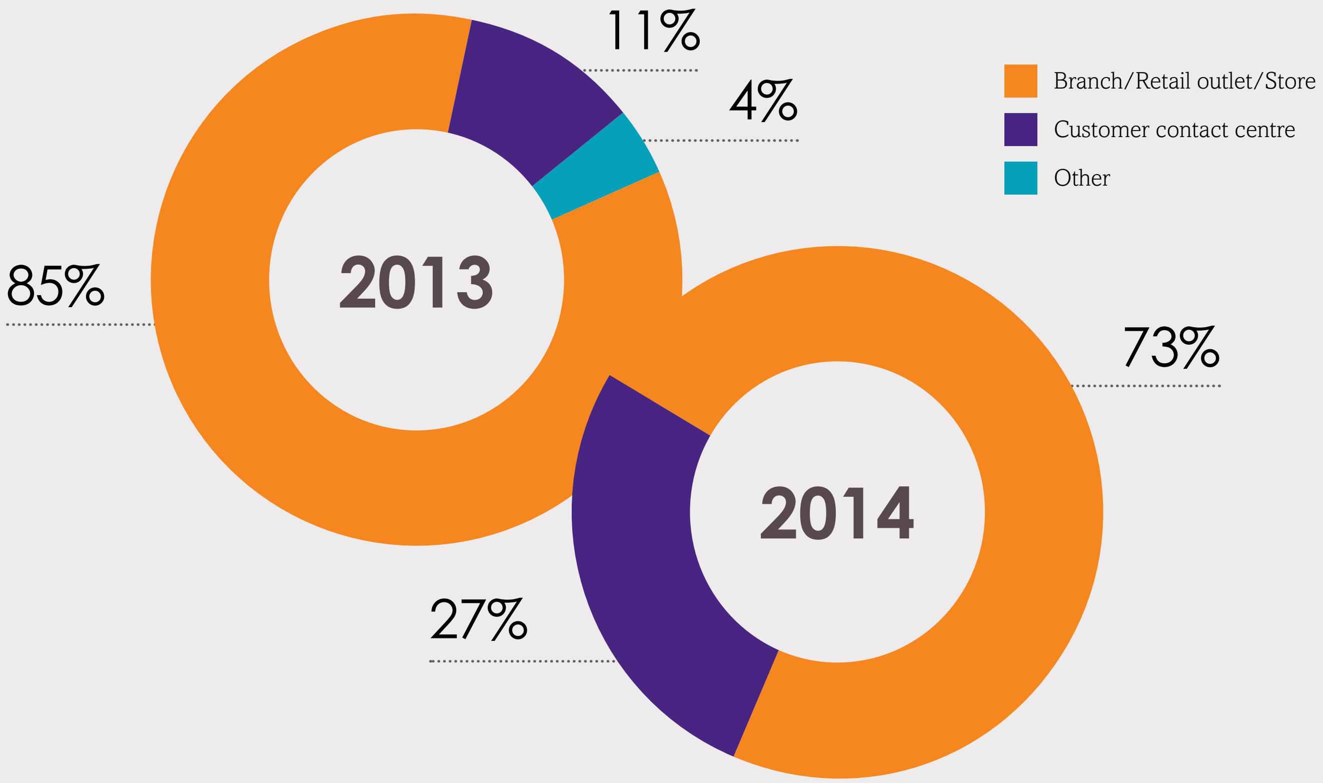
Reasons for Recording Unsuccessful Employment Application Fraud in 2013–2014

	2013		2014		
REASONS FOR FILING	CASES	% OF TOTAL	CASES	% OF TOTAL	% CHANGE
Concealed adverse credit history	253	86.3%	347	87.6%	37.2%
Concealed employment history	15	5.1%	24	6.1%	60.0%
Concealed employment record	18	6.1%	18	4.5%	0.0%
Concealed unspent criminal convictions	11	3.8%	15	3.8%	36.4%
Concealed address with adverse	0	0.0%	12	3.0%	-
False qualifications	0	0.0%	6	1.5%	-
False documents	1	0.3%	5	1.3%	400.0%
False references	1	0.3%	3	0.8%	200.0%
Use of a false identity	1	0.3%	2	0.5%	100.0%

Reasons for Recording Unlawful Disclosure or Obtaining of Personal/ Commercial Data in 2013–2014

	2013		2014		
REASONS FOR FILING	**CASES**	**% OF TOTAL**	**CASES**	**% OF TOTAL**	**% CHANGE**
Disclosure of customer data to a third party	32	61.5%	31	57.4%	-3.1%
Contravention of systems access policy	9	17.3%	14	25.9%	55.6%
Fraudulent personal use of customer data	15	28.8%	11	20.4%	-26.7%
Contravention of IT security policy	11	21.2%	6	11.1%	-45.5%
Unauthorised alterations to customer data	4	7.7%	4	7.4%	0.0%
Contravention of Internet policy	0	0.0%	3	5.6%	-
Contravention of email policy	2	3.8%	0	0.0%	-100.0%
Theft of internal practices	1	1.9%	0	0.0%	-100.0%
Theft of intellectual property	1	1.9%	0	0.0%	-100.0%

Proportions of Account Frauds by Business Area in 2013–2014



Stop fraud in its tracks.

Prevent, detect and investigate fraud with LexisNexis® Risk Solutions.

Offering a global defence in the battle against fraud and financial crime, LexisNexis® Risk Solutions allow you to manage the risk of fraud in a business friendly manner. Our data-driven solutions enable you to confidently verify and authenticate customer identity, screen individuals against international watchlists, conduct systematic fraud investigations and comply with global regulations.

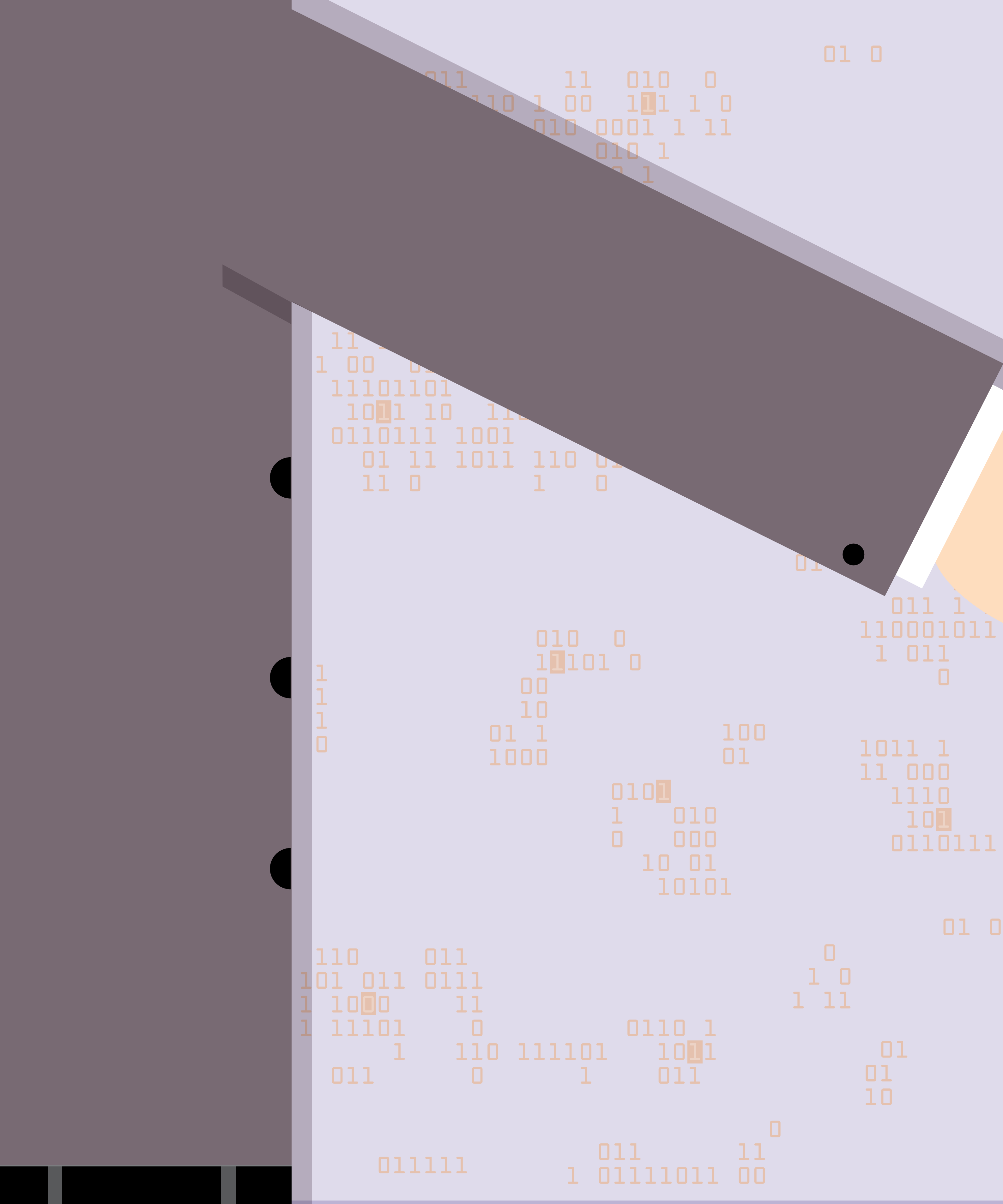
For more information, call 029 2067 8555 or email ukenquiry@lexisnexis.com

lexisnexis.com/risk/tracesmart

LexisNexis®

Risk Solutions

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2015 LexisNexis Risk Solutions. All rights reserved. Tracesmart Ltd is a company registered in England & Wales with company registration number 3827062 and whose registered office is at Global Reach, Dunleavy Drive, Cardiff CF11 0SN. Our data protection number is Z708281X. We are authorised and regulated by the Financial Conduct Authority with consumer credit licence number 565961.



www.cifas.org.uk

Cifas
6th floor, Lynton House
7–12 Tavistock Square
London
WC1H 9LT