Leaders in fraud prevention

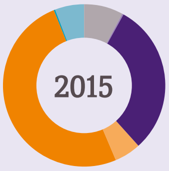
Employee Fraudscape 2016

Insider fraud threats of 2015 and what you can do to protect your workplace

Essential reading for fraud and HR professionals

Page 5
SPECIAL REPORT: Public Concern At Work and Cifas launch joint whistleblowing and fraud research

Page 3
Key internal fraud trends in 2015



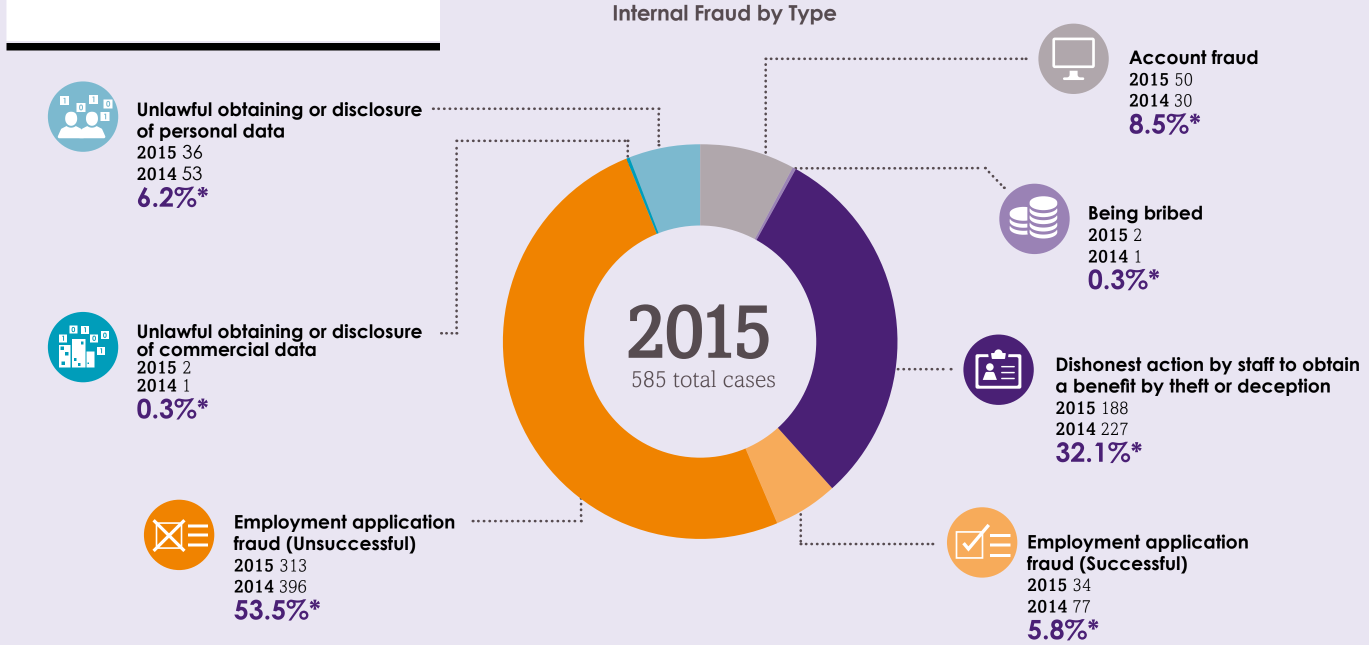
Page 8
Join the UK's largest Fraud Data Sharing Network and protect your organisation from the insider threat

CONTENTS

The insider fraud picture in 2015

In 2015, 153 organisations identified and recorded a total of 585 confirmed insider fraud cases to the Cifas Internal Fraud Database.

Internal Fraud by Type



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.

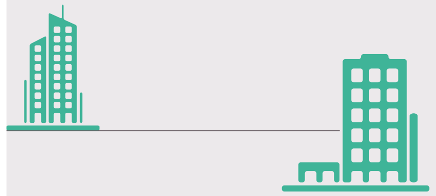
Unlawful obtaining or disclosure of commercial data: the use of commercial/business/company where the data is obtained, disclosed or procured without the consent of the data owner/controller. This includes the use of commercial data for unauthorised purposes that could place any participating organisation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

* Percentages add up to more than 100% – one internal fraud can be recorded under more than one fraud type

INTRODUCTION

Established in 2006, the Cifas Internal Fraud Database is the only cross-sector data sharing system dedicated solely to recording confirmed cases of insider fraud.



With a membership covering a wide range of organisations – including financial services, insurers, call centres, IT businesses and vetting specialists – our cross-sector database helps to prevent organisations from employing someone with a known history of committing fraud, as well as acting as a strong deterrent for existing staff who may be tempted to commit fraud.

Key internal fraud trends in 2015

BY **LYDIA VYE**, CIFAS RESEARCH ANALYST

In 2015, the Cifas Internal Fraud Database membership grew by 14% (compared with 2014); however, the total number of reported frauds fell by 22% (751 recorded in 2014).

The instances of recorded internal fraud have reduced, but not through a drop in the number of organisations reporting. One possible explanation is the deterrent effect of the Internal Fraud Database itself; if an employee knows that they will not only be dismissed from their current role for behaving fraudulently, but also have their chances of gaining future employment affected then they may well think twice before committing the fraud in the first place. Just by being a member of the Internal Fraud Database, organisations are sending a clear message to their staff that any form of internal fraud will be taken seriously and any employees committing fraud will face the consequences of their actions.

Employment application frauds continue to make up the majority of internal frauds, with almost 60% of employment related frauds being committed by prospective employees or new employees who have supplied serious material falsehoods in their applications in order to fraudulently gain employment.

Accounting for 32% of all internal frauds recorded in 2015, the number of dishonest actions - such as cash theft, facilitating fraudulent transactions and manipulating accounts - remains high, but it is actually account fraud which has seen the biggest increase over the 12 month period. Fraudulent account withdrawals by dishonest employees more than doubled in 2015 compared with 2014, with over half of these frauds having been identified by the customer themselves. Evidently, round-the-clock awareness and vigilance on the part of both the customer and the organisation can play a huge part in identifying and dealing with insider fraud at an early stage.

In 2015, there were 38 instances of an employee unlawfully obtaining or disclosing personal or commercial data. As a standalone figure, this doesn't seem high, but when acknowledging the fact that a single stolen dataset could contain the personal details of thousands of customers, the potential damage caused by the crime suddenly becomes much clearer, with the realisation that a large number of innocent people have been put at risk of identity related crime.

Prevention and Protection

According to our database there is no such thing as a 'typical' internal fraudster. Length of service ranges from less than a month to over 30 years and although the overall gender split is 63% male and 37% female, ages recorded in 2015 range from 18 to 67 years.

Therefore prevention continues to be better than the cure, and the best way of dealing with insider fraud is to stop it before it has even happened. This isn't always possible, but there are some measures that organisations can take in order to reduce the risk in the first place. Thorough vetting is the first line of defence. Organisations that are able to run checks against potential and existing employees are better protected by ensuring that they are not unwittingly employing organised criminals or those intending to join the organisation with the sole purpose of committing fraud. One of the simplest ways of reducing internal fraud is to stop the criminals getting through the door in the first place.

> "Fraudulent account withdrawals by dishonest employees more than doubled in 2015 compared with 2014, with over half of these frauds having been identified by the customer themselves."

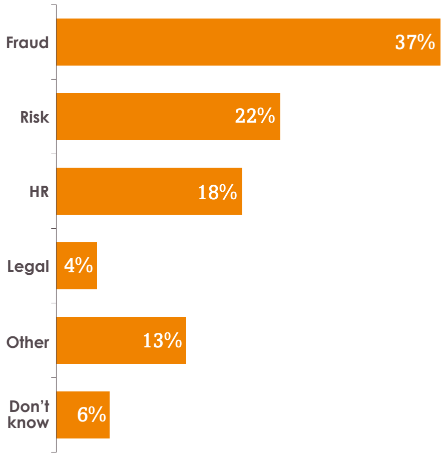
Having a strong anti-fraud culture is key to deterring existing staff from committing fraud. A crucial part of this is making sure staff know how to report concerns and that they will be supported in doing so. Staff can act as the eyes and ears of the organisation and proper training and awareness can teach them what to look out for. If they suspect that one of their colleagues is behaving fraudulently a dedicated whistleblowing line also gives staff the option of reporting fraudulent activity anonymously and it can be a vital source of information where fraudsters have managed to evade internal controls and audits. (See page 5 for our whistleblowing report).

It's also important to note that exposure to fraud might not always come from a deliberate, malicious insider: for example, an unwitting employee could connect to company IT systems over an unsecured public wi-fi, which criminals can hack.

In 2015 we also received reports of the social engineering of staff, where employees are manipulated or deceived into releasing information. We saw cases where seemingly genuine emails, websites, links, pages and attachments designed to be opened by staff actually contained malware intended to attack a company's security systems or convince the recipient to disclose confidential information or security details. Ensuring that staff know the correct procedures and methods to secure their devices and knowing what to look out for in terms of suspicious activity can greatly reduce an organisation's exposure to fraud.

Responsibility for internal fraud prevention and detection continued to be split across many different teams within organisations, with our members reporting the following split in 2015 (Graph below).

Responsibility for internal fraud across teams within organisations



To prevent internal frauds from falling between the various functions involved, it is important that organisations are clear about where this responsibility lies within their own structure. With almost one fifth of members reporting that HR had lead responsibility for internal fraud in 2015, it is imperative that fraud professionals, including Cifas, provide relevant support and guidance to HR professionals.

Future Threats

We asked Cifas members to share what they thought were the biggest internal fraud threats facing their organisations in the future. The key concerns reported were:

- Greater access and use of portable company devices and personal IT such as laptops, tablets and phones leads to an increased chance of loss, theft or personal misuse. If devices aren't adequately encrypted, the danger of data disclosure is a very real possibility.
- Increased use of instant messaging platforms. Some feel that these systems aren't being regulated well enough and that staff can share sensitive information more freely.
- Home working or 'agile working' is becoming more popular among staff who want more flexibility or where office space is at a premium. As well as increased risk of loss or theft of devices, it also increases the chance that other people close by may be able to access or oversee what they are doing (e.g. if using public Wi-Fi in a coffee shop or working in busy communal areas).
- Financial issues faced by some organisations mean that staff pay and bonuses have stagnated or reduced, resulting in increased staff feelings of resentment and indifference towards their employer. Some organisations feel that this could be a trigger for fraudulent activity by some employees who feel that they deserve more or are being overlooked for possible progression.

The above threats don't necessarily stand alone; a combination of two or more scenarios can leave an organisation at risk of internal fraud. For example, an already disgruntled employee may be forced to work away from the office due to lack of desk space, resulting in a heightened motivation to commit fraud alongside an opportunity to do so away from the eyes of their colleagues.

> "Having a strong anti-fraud culture is key to deterring existing staff from committing fraud."

The five main corporate vulnerabilities to fraud

Reducing overheads sometimes leads to reduced supervision and oversight – charities are particularly vulnerable.

More complex and complicated supply networks provides more opportunity for fraud and less clarity for those in supervisory roles.

Ignorance of cyber security principles – knowing what to do when employees receive an email they are unsure of (and what not to do).

Outsourcing and Offshoring work means a reduction in visibility and control and an increase in the vulnerability of systems and processes to fraud.

Churn of staff – the lack of loyalty and greater insecurity in some industries and workplaces can make some employees more susceptible to bribery/corruption/fraud.

SPECIAL REPORT

Whistleblowing and fraud

public concern at work

Support your staff to blow the whistle on fraudulent activity and create an open culture

Recent research by Cifas and Public Concern at Work into whistleblowing and fraud in financial services has found that most staff think reporting wrongdoing is the right thing to do and would report concerns if they had them.

Despite these positive attitudes, the numbers of internal fraud cases attributed to whistleblowing remain low. In 2015, only five per cent of frauds recorded to the Cifas Internal Fraud Database were attributed to whistleblowing, with a further nine per cent from staff reporting through other internal channels. So how can you as an employer or manager tap into the desire from your staff to report fraud and create a culture that will support them to do so when the moment comes?

The majority of those surveyed have a strong preference for internal reporting. They said they want to report via their existing personal relationships, ideally to their own line manager in the first instance. The preferred channels for reporting a concern were:

- My manager
- A specialist department (e.g Compliance/ Fraud control/Audit)
- A corporate/council hotline

The preferred external contacts were:

- An advice service (e.g. PCaW)
- A regulatory body (e.g. the FCA)
- A professional body

ANALYSIS

In our online study, we tested employee reactions to fictional scenarios. Here are some examples below.

Aida works in a bank as a cashier.

When walking to the back office she notices another cashier, Martin, writing down the account number of the customer he is serving. There appears to be a number of other account numbers and balances written on the same piece of paper. She knows this to be against company policy. Aida is immediately worried about this. She decides that she should speak to her branch manager and reports what she has seen.

Would your staff do the same?

Ravi works at an insurance provider selling uplifts to insurance policies.

These include items such as special breakdown cover and increased medical cover. Ravi is concerned as the cost of the special breakdown cover far exceeds its value over a two year insurance term. Ravi believes this is bad value for customers. However his manager tells all staff that they must increase sales of this uplift item by 30% in order to hit their targets.

Ravi is not sure who in senior management has given this instruction, but he is concerned it comes from the top and is another case of mis-selling like the PPI scandal. Ravi decides to tell the Financial Conduct Authority, who regulates this activity, about his concerns.

What would your staff do?

Be open about your investigations policy

Sometimes suspicion is just that: suspicion. We found that staff can be reluctant to report suspicions because they may end up being wrong and do not want to cause problems. This risk of being wrong is one of the key factors in underreporting.

Make sure your employees know that you will investigate every claim and that no one will be treated as 'guilty' unless a full investigation has taken place. Whistleblowing is raising a valid concern – it is then up to the organisation to investigate it.

Be clear on confidentiality

Almost a third of respondents said nothing would stop them from raising a concern, but almost a quarter of staff said that they would be more likely to report if they had clear assurances that their concerns would be kept confidential and they would be protected from reprisal. Follow our recommendations on page 7 to make sure you create a culture where staff have these reassurances and everyone is treated fairly.

Who is a whistleblower?

You're a whistleblower if you're a worker and you report certain types of wrongdoing. This will usually be something you've seen at work – though not always.

The wrongdoing you disclose must be in the public interest. This means it must affect others, such as the general public.

As a whistleblower you're protected by law – you shouldn't be treated unfairly or lose your job because you 'blow the whistle'.

You can raise your concern at any time about an incident that happened in the past, is happening now, or you believe will happen in the near future.

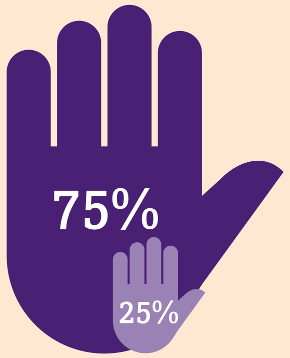
Source – gov.uk

THE WHISTLEBLOWER'S EXPERIENCE

7%

of the respondents said they have witnessed wrongdoing or malpractice in the last three years.

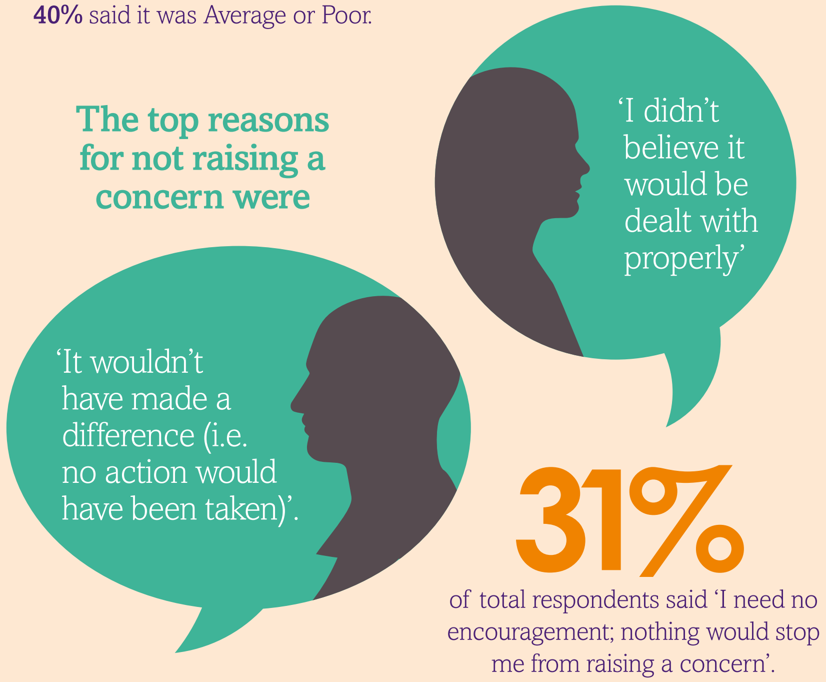
Of those who witnessed wrongdoing, 75% said they raised their concern and 25% did not.



Of those who raised the concern:

60% said the organisation's response to the concern was Good or Excellent, **40%** said it was Average or Poor.

The top reasons for not raising a concern were



'I didn't believe it would be dealt with properly'

'It wouldn't have made a difference (i.e. no action would have been taken)'.

31%

of total respondents said 'I need no encouragement; nothing would stop me from raising a concern'.

WHAT WOULD ENCOURAGE STAFF TO RAISE A CONCERN

13% said 'A commitment from the organisation that they will investigate'.

11% said 'A commitment that the organisation will protect me by ensuring that my job is not affected in any way'.

23% said 'A commitment to my identity and whistleblowing role not being revealed without my consent'.

YOUR WHISTLEBLOWING ARRANGEMENTS CHECKLIST

How can you create an open culture?

- □ Encourage staff to raise a suspicion or concern at the earliest opportunity.
- □ Reassure staff they need not have a wealth of information about the wrongdoing and will not be punished for being wrong.
- □ Promote the role of senior managers in receiving whistleblowing concerns and provide all staff who hold line management responsibilities with appropriate training on receiving and handling concerns.
- □ Ensure that the messaging throughout your arrangements and in training communicates that an appropriate investigation will take place and any action taken in relation to the wrongdoer will be balanced and proportionate.
- □ Identify possible complex wrongdoing that may arise (e.g. mis-selling or procurement fraud) and communicate to staff via training how to identify it and when and how to raise concerns about it effectively.
- □ Identify who has overall responsibility for your arrangements and demonstrate commitment to whistleblowing from the top of your organisation. Include within your arrangements the name and contact details of an identified senior executive and a board member.
- □ Ensure your whistleblowing arrangements highlight sources of independent advice for staff and include a list of external bodies with whom staff can raise concerns (such as regulators)
- □ Try to understand what it is that may still prevent your staff from speaking up (using survey questions, staff engagement forums and feedback from managers, etc.)
- □ Train managers on what constitutes a detriment and sanction those who victimise a whistleblower for raising a concern.

One of my staff has raised a concern, what next?

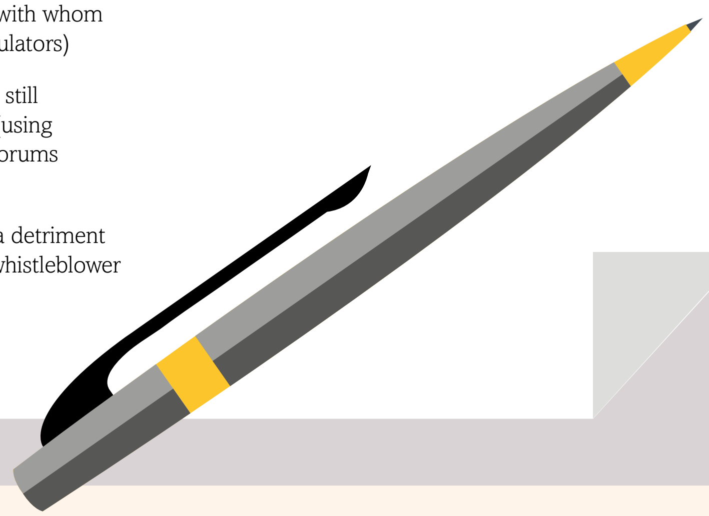
- □ Give assurances to staff that their concerns will be taken seriously and investigated, that their identity will be kept confidential where requested (unless disclosure is required by law) and that they will not suffer detriment for having raised a concern.
- □ Provide progress updates and as much feedback as you can to a whistleblower after they have raised a concern.
- □ Ask those who have used the arrangements for their feedback on the process. Take on board suggestions to improve the experience for those raising concerns in future.

For the full study visit
https://www.cifas.org.uk/research_and_reports

About Public Concern at Work:

Public Concern at Work, the whistleblowing charity, aims to protect society by encouraging workplace whistleblowing. We operate a free, confidential advice line for workers with whistleblowing dilemmas, support organisations with their whistleblowing arrangements, undertake research, inform public policy and campaign for legislative reform.

For further advice and information visit: **www.pcaw.org.uk** or follow us on Twitter - **@WhistleUK**



The Data Approach to Internal Fraud

Join the UK's largest fraud data sharing network

By using the Cifas Internal Fraud Database, organisations are able to help each other counteract the insider threat through collaborative sharing of information on cases of confirmed fraud, including incidences of bribery and corruption.

Established 10 years ago, the cross-sector database has a proven record in helping to prevent organisations employing someone with a known history of committing fraud, as well as acting as a strong deterrent to existing employees. Having a strong vetting and fraud prevention strategy in place is crucial to recruiting and retaining the right people, and key to the success of any organisation.

Cifas membership is completely cross-sector, meaning that there is an opportunity for all employers to benefit from sharing their data. With an additional 26 organisations joining the database in 2015, the benefits of membership continues to grow. The membership currently includes organisations from telecoms, call centres, public sector and financial organisations. As the membership is truly cross-sector it also helps to develop a wider picture of the fraud threats across the UK once the data is analysed.

Beyond the benefits of sharing data on confirmed fraud cases, organisations will also gain access to over 320,000 cases of confirmed fraud risks. These include records of individuals who do not have the right to live in the UK (filed by the Home Office), Metropolitan Police 'Amberhill' data relating to fraudulent identity documents and Fraudulent Royal Mail Redirections data.

Organisations who use the Cifas Internal Fraud Database also have the advantage of working collaboratively through working parties, conferences and open days; allowing them to share current fraud threats, trends and best practice with one another. By sharing experiences and knowledge on top of individual cases, organisations are able to develop a clearer picture of the risks – and the remedies - when building their own fraud prevention strategies.

Fraud will always be with us. Dealing with it effectively, without penalising those who are most important to any organisation, its 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.

Find out more about joining Cifas by emailing **newmembers@cifas.org.uk**

> Cifas is the UK's leading fraud prevention service. We work to make the UK a safer place to do business by enabling organisations in every sector to prevent fraud and protect the public — by sharing data, spreading knowledge and pushing the capabilities of our technology.

www.cifas.org.uk

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