



FRAUD DIGEST

March 2016









Welcome to our forth annual Fraud Digest. The purpose of the Digest is to provide a measured assessment of the emerging trends in fraud facing both the public and private sectors. There are no banner headlines derived from extrapolations or similar, but rather our Fraud Intelligence Team's pragmatic assessment based upon their extensive experience. We have included a number of examples of reported frauds to demonstrate that most frauds are not unique to one sector, and consequently awareness of what is happening in other sectors, as set out in this Digest, is of real use and relevance.

For the first time we have also carried out a fraud survey of our clients and the results from this are also summarised. We would like to thank all of our clients who participated in this survey.

Our Digest is not designed to provide sleepless nights, but rather is intended to give practical advice about emerging fraud trends to assist in proactively safeguarding your organisation.

Sector Analysis

TIAA's Fraud Intelligence Team undertook a high level review of fraud, based primarily on open source information available. Data was collated from reported crown court cases relating to internally perpetrated frauds only. It therefore excludes external/third party frauds, such as Housing Benefit fraud in local government. The analysis does not provide a definitive picture of all fraud affecting the United Kingdom in the last two years, but is indicative of risks presented across all sectors. Cases often take a year or more to reach the courts, so there is a built in time lag to the data available. The table opposite analyses the proportion of cases by sector.








Sector	2014	2015	Change
Education	3.2%	5.4%	
Housing	2%	2.1%	
Charities	8.5%	13.6%	
Healthcare	6.1%	6.6%	
Care Homes	11.3%	14%	
Local Government	6.1%	7.4%	
Private Sector	54.8%	49.4%	
Other	8.1%	1.5%	

Issues affecting all sectors

The proportion of reported fraud has increased in some sectors, whilst decreasing considerably in others. The most notable rise in the proportion of reported fraud relates to charities, with an increase of more than 5%. This may simply be due to an increased media profile, creating a greater awareness of such frauds, leading to a higher rate of detection, prosecution and reporting.

According to recent reports, many white collar crimes are not committed by hardened criminals. It is often staff under financial strain, those under severe pressure from their bosses or shareholders, or people who get away with something minor and then try to test their limits. The table below analyses cases by the fraudster's reported motivation or main causal factor. As anticipated in last year's Fraud Digest, increased regulation of payday loans may be starting to level off the steady year on year increase in fraud committed due to inability to service such loans. A rise in fraud committed by staff with gambling problems was identified in last year's Digest, and the figures for 2015 show a further increase which would appear to have some linkage to an increase in on-line gambling.

TIAA's view is that opportunistic and low-scale fraud is more likely to lead to high value fraud over time, therefore constant vigilance must be maintained over seemingly immaterial anomalies and robust action must be taken on wrongdoing.

Factor	2014	2015	Change
None	48.2%	42%	
Debt	15.8%	18.9%	
Gambling	9.7%	13.2%	
Lifestyle	21.9%	15.6%	
Drug / Alcohol Addiction	1.6%	6.2%	
Disgruntled Employee	0.8%	2.1%	
Other	2%	2.1%	

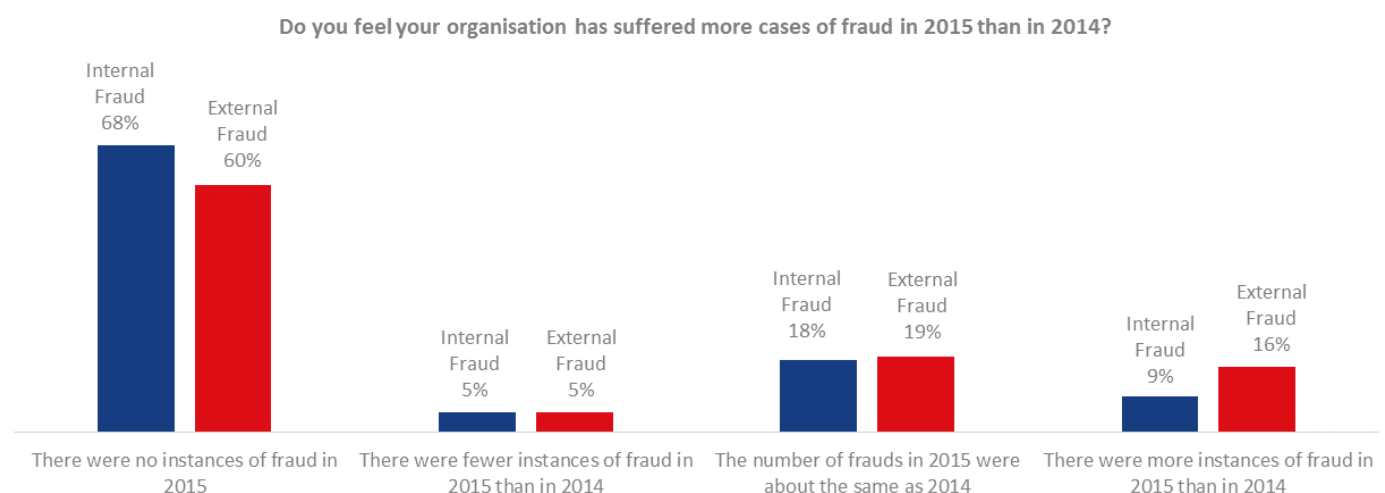
A good corporate human resources function will try to track employee satisfaction, sickness, staff attitudes and culture. This approach is more likely to help prevent fraud, and to identify it when it does occur.

The greatest increase across these fraud indicators relates to those involved in gambling, or who have a debt or drug / alcohol addiction. This is of little surprise and may prove true of all criminality, not only fraud. There has been a marked decrease in the proportion of those committing fraud to fund lavish lifestyles, suggesting that motivational factors go beyond the materialistic in many cases, or that fraudsters are more aware of "flashing the cash".

Key Results of TIAA's Fraud Survey

Instances of reported Fraud

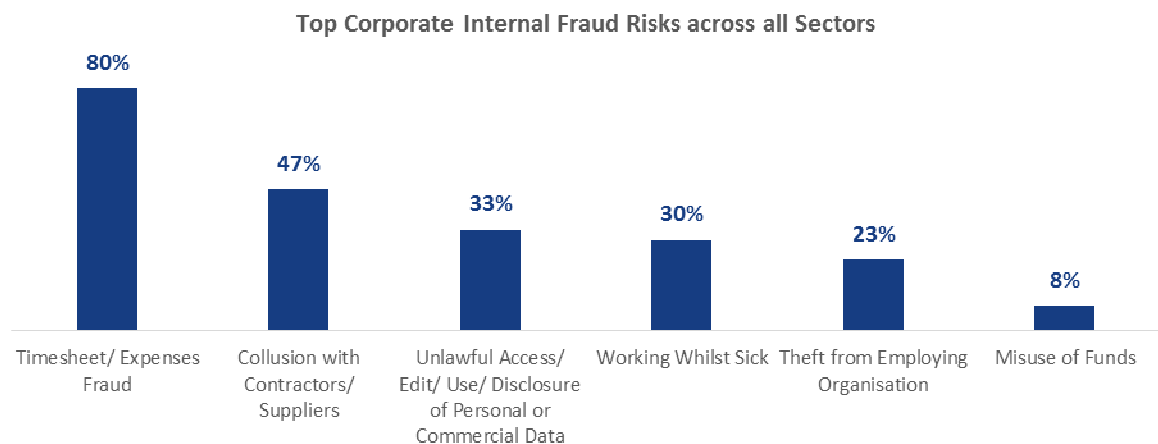
Over half of organisations responding to the survey stated they had encountered no instances of internal fraud (68%) or external fraud (60%) in the last year. Of those organisations which have suffered fraud, most reported similar levels in 2015 compared to 2014. Of those reporting a change in fraud levels, many more reported that fraud had increased rather than reduced compared to the previous year.



When looking at a sector level, all NHS Commissioners stated they had no experience of internal fraud in 2015. Both Education (90%) and Housing (89%) sectors also reported very low levels of internal fraud during 2015. The same three organisation types also reported relatively few instances of external fraud compared to other organisation types. At the opposite end of the scale, all NHS Provider Trusts reported suffering from some internal fraud, and the vast majority of Councils (83%) reported having cases of both internal and external fraud.

Internal Fraud Risks

The highest rated internal fraud risks identified by all respondents are set out below:

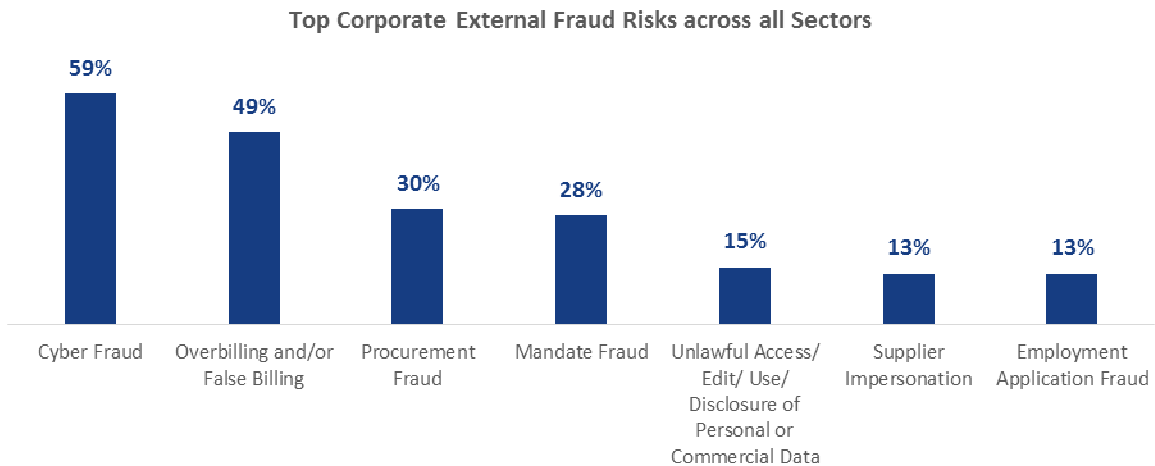


The main variations noted between different sectors was that:

- Unlike all other types of organisation, no NHS Provider raised “Collusion with Contractors/Suppliers” as a top internal fraud risk; and
- Relatively few (less than 12%) of Education and NHS Providers identified “Unlawful Access/Disclosure of Data” as being a top internal fraud risk.

External Fraud Risk

Overall, the highest rated external fraud risks were identified as being:



The main variations in this area noted between different types of organisation were that:

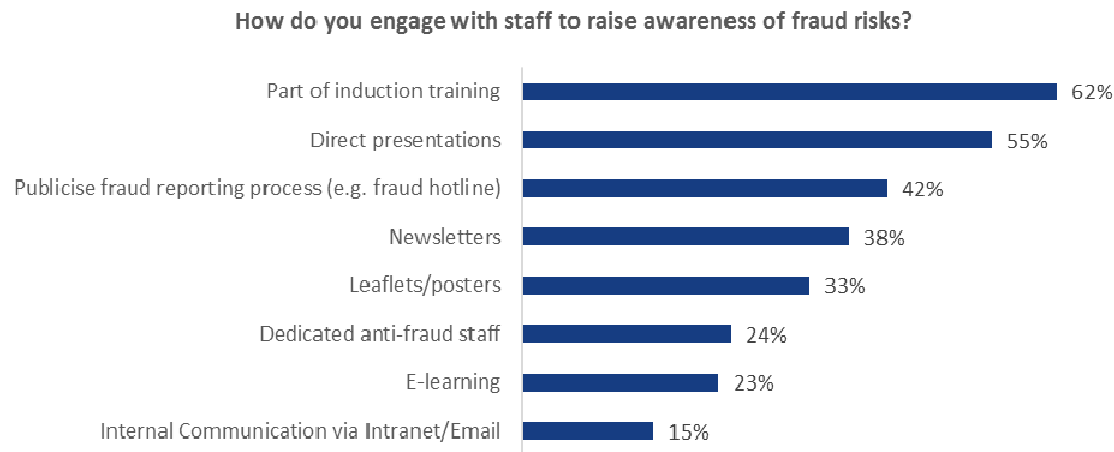
- No Charity raised either Mandate or Procurement Fraud as being a top external fraud risk; and
- None of the Local Government or Charity respondents identified “Overbilling/False Billing” as being one of their top external fraud risks.

All types of organisation cited ‘Cyber Fraud’ as one of their top three corporate external fraud risks.

Anti-Fraud Policy and Whistleblowing Policy

When asked about their policy frameworks, all organisations reported having an agreed Whistleblowing policy in place. Almost all also had an anti-fraud policy, with the exception of one Housing Association and one FE College.

Engaging with Staff to Raise Awareness



Only a small proportion of organisations (5%) stated they did not try to proactively engage with staff to raise awareness of fraud risks. Over 60% of organisations include fraud awareness as part of staff induction training, with 55% providing direct presentations to staff on this area. Other frequently used methods of raising staff awareness included: publicising the fraud reporting process (42%); making use of Newsletters (38%); and Leaflets/Posters (33%).

There were some big differences in the results between sectors for activities in this area. In particular, whilst most NHS organisations and all Councils employ dedicated anti-fraud staff, almost no Housing Associations or Colleges do so. Similarly, whilst half of NHS organisations make use of e-learning to raise staff awareness about fraud, only 17% of Housing Associations and no Councils, Colleges or Charities reported doing so.

Local Government & Housing Sectors

Changes to how local services are delivered have seen major reforms to the welfare system, policing and local government. The change of emphasis from local government being a provider to a commissioner of services changes the risk profile of fraud, as well as the control environment in which risk is managed. Without new safeguards, preventing, detecting and investigating fraud will become more difficult.

All of these changes are happening against a backdrop of depressed economic activity in which the general fraud risk tends to increase. At the same time as unprecedented change to the delivery of local services and increased risk, the counter fraud environment is being fundamentally altered. The abolition of the Audit Commission, the changes to local auditing arrangements and the creation of a single fraud investigation service to tackle benefit fraud has considerably altered current fraud governance arrangements. A positive event during 2015 has been the development of CIPFA's Counter Fraud Centre to provide further tools and training to assist the counter-fraud profession.

Case Study

A senior estates employee was rarely in the office during core working hours and significant periods of their working day could not be accounted for. The employee was responsible for management of the organisation's estates maintenance programme. Investigations confirmed the employee was operating a private business related to property maintenance and had not formally declared this to their employer, as required by their Contract of Employment. It was also established that the employee had:

- Been conducting a significant private business during working hours, and had deliberately manipulated the employer's time recording records so they could claim the time as working on business.
- Used the services of a number of the employer's contractors in a private capacity, over a period of years, and had not formally declared this to their employer.
- Regularly used their employer's computer system and email account to conduct personal work on behalf of their private business, and had done so during normal working hours.
- Regularly used their employer's mobile and landline telephone to conduct personal work on their private business.
- Copied and adapted their employer's documents for use with their private business.

Healthcare Sector

TIAA recently published an Economic Crime Pattern Analysis exercise of NHS Fraud Data for the first six months of 2015/16 and 2014/15 financial year. This found trends broadly similar to those present in recent years, with the most prevalent offences being Working Whilst Sick, Payroll and Timesheet Fraud.

TIAA's NHS clients continue to experience more low level, high incident, low value type offending rather than organised, complex and protracted activity. Many of these end up being dealt with through civil processes, rather than becoming criminal cases. Whilst organisations must remain vigilant to complex attacks, the majority of fraud against TIAA clients is perpetrated by its own staff. Many frauds commence as opportunist crimes, committed by staff who exploit weakness in processes and systems, and maximise any advantage over time. Whilst costly to clients, continued engagement with staff and senior management alike will help ensure that such offences are prevented, deterred, reported and investigated.

Case Study

A senior nurse stole from her hospital's charity and forged numerous timesheets in a fraud totalling £17k. The hospital received an anonymous tip off that the ward sister had paid a cheque from a patient intended for the hospital's Charitable Fund Department into her private bank account. The subsequent investigation revealed she had also manipulated her timesheet on many occasions to fraudulently claim payment for 12-hour shifts when she was not actually at work.

The court heard that despite the nurse earning a £40,000 salary, she was indebted to pay day loans. The judge accepted the nurse had not lived a life of luxury, but had simply been unable to balance the household books. Her actions however had created a potential risk to care of patients for periods when she was rostered to work, and the level of staff required was not being met due to her absence. In all there were around 100 shifts for which fraudulent claims were submitted. The nurse pleaded guilty to fraud and was sentenced to 12 months' imprisonment. Following her conviction, the nurse was also subsequently struck off by the Nursing & Midwifery Council. The NMC disciplinary panel concluded she had put "patients at unwarranted risk of harm, acted dishonestly, breached fundamental tenets of the code and brought the profession into disrepute".

Private Sector

The importance of maintaining robust access controls to computerised systems to help ensure proper segregation of duties over payments and stock cannot be overestimated. Examples of how fraudsters can exploit weaknesses in computer access controls can be found across all sectors, with these sorts of cases often involving large sums.

Case Study

Two large property companies lost over £4m over a five year period as a result of an accountant using colleagues' computer log-in details to transfer funds to family and friends. The employee was gambling massive amounts on a daily basis - losing millions to bookies. The fraud was only identified after the accountant left to join another company.

The fraud involved falsifying receipts for rental income and client payments, and using faked invoices to suppliers. Jailing him for five years, the court heard how the accountant tried to cover his tracks by using colleagues' computer log-in details and by transferring cash to family and friends. The court heard the accountant joined the company with good intentions but soon began syphoning off money. The fraudster was able to access computer systems using colleagues' log-in details, and he also transferred £0.5m to an account of his then-fiancée, telling her the cash was from gambling winnings. The court heard how the accountant made repeated attempts to conceal his behaviour, causing suspicion to fall on ex-colleagues and his ex-partner.

Case Study

An accounts manager at an IT company defrauded their company out of more than £60,000 over a five year period. The employee was responsible for ordering stock and processing it for invoicing. They began stealing laptops and effectively undercutting the company, selling them to customers at a lower price and receiving the funds in their personal account.

When the company detected one of the thefts in 2013, the accounts manager said it was a one-off and promised never to do it again. From that point on they continued offering to sell items at reduced prices, but instead of actually stealing the laptops and carrying them out of the building, they would alter invoices so the company would ship the goods itself. They would then use customer credit card details to pay off small amounts of money to cover their tracks. The court heard the crime was ultimately motivated by greed, and sentenced the manager to a total of 32 months in prison for the offences.

Charity Sector

A charity can fall victim to many different types of fraud, and methods are constantly evolving, supported by rapidly developing technology and increasing use of the internet. The Charity Commission's Compliance Toolkit – Fraud and Financial Crime has a comprehensive – although not exhaustive – list of the types of fraud a charity could fall victim to, as well as tips on how to prevent these types of fraud.

Fraud committed against charities can include:

Internal fraud, involving staff within the charity or responsible for the management of charitable funds – for example:










- Staff intercepting cash or cheque donations
- Staff responsible for managing donations creating false business cases to obtain grants for their own use
- Hijacking charities' identities, and defrauding the public into donating to false causes, e.g. by approaching people on the street with fake raffles
- Misuse of charity credit cards
- Staff claiming false or inappropriate expenses
- Staff setting up their own unregistered/bogus charities that conflict with the official charity

External fraud, where fraud is perpetrated outside the charity/charitable fund, committed by people who are not directly involved - for example:

- False invoices to obtain money from the charity
- Identity fraud e.g. by hijacking a charity's bank account
- Setting up fake accounts for charity pages and similar to defraud the public
- Phishing emails requesting confidential information from the charity which is then used by fraudsters to obtain funds illegally
- Unauthorised fundraising in a charity's name e.g. fraudulent disaster appeal websites

Current and Prevailing Threats

The table below analyses publicly reported court cases of internal fraud by type. This shows a small increase in cases of fake invoice/mandate fraud, which continues to be the most common category.

Type of Fraud	2014	2015	Change
Fake invoices / Bank transfers / Mandate fraud	33%	34%	
Theft of cash from employer	25%	23%	
Theft of cash from service user	13%	15%	
Cheque Fraud	8%	8%	
Payroll Fraud	11%	8%	
Procurement Fraud	5%	9%	
Collusion with suppliers	2%	0%	
Unlawful obtaining or disclosure of commercial data	1%	1%	
Manipulation of applications / proposals / claims	2%	3%	

Our survey indicates that cybercrime is a rapidly increasing fraud risk. The table above indicates the full impact of cybercrime has not yet translated into criminal cases. Our view is that this is due to the time-lag for such frauds to come to court, and also the relatively high number of such attacks where the perpetrator is not identified. The use of electronic means to defraud (in particular bank transfer and mandate fraud) continues to show a year-on-year increase, and from our analysis now accounts for over a third of all external fraud prosecutions (and significantly higher as a percentage of sums defrauded). Many of these electronic frauds circumvent existing traditional internal controls. All organisations need to maintain their vigilance for variations in such scams. See below for some prompts and guidance about how to protect your organisation.

10 Things to help improve your Cyber Resilience

1. Assess your data and business classification, so you know what to guard first.
2. Identify vulnerable information assets and make service based risk assessments
3. Make your IT services and systems secure by design, not by accident.
4. Secure internal networks – it is not just internet hackers, the insider threat is very real.
5. Policies – are they up to date, understood and accessible in a disaster?
6. People – are they trained, and do you have a cyber-security awareness culture?
7. Implement pro-active event logging. Review and detect threats before exploitation.
8. Effective and prompt “Patch Management” is crucial in reducing risks.
9. Control web access – use secured DNS services to block malware sites at source.
10. ...You have got reliable, tested backups haven’t you?

TIAA has developed a comprehensive suite of Cyber Security assessment and support services. These range from Gap Analysis of Cyber resilience, vulnerability assessments, post incident forensic reviews and malware analysis. Our ISO 27001 accredited Digital Forensics service can support evidence gathering, as well as service restoration. Contact us before an incident occurs to find out how we can help.

Mandate Fraud

The recent rise in incidents of on-line mandate fraud mean organisations must have robust checks and controls over all requests to change a bank account or payee details. Emails may have been hacked, meaning that a legitimate email from ANYONE requesting bank account changes needs to be verified. This includes from within your organisation. The TIAA Intelligence Team identified at an early stage the increasing sophistication of fraudsters in this area, and issued a Fraud Alert to protect our clients. Feedback received from a number of clients in response to this alert was that this early warning enabled them to identify and reject attempts at this fraud.

For more information or advice, please contact:



Michael Townsend
Regional Managing Director

T: 01424 776 750

M: 07825 351 654

E: michael.townsend@tiaa.co.uk



Veran Patel
Director

T: 0203 313 2866

M: 07919 595 930

E: veran.patel@tiaa.co.uk

