

# Fraud Survey 2024



IDEAS | PEOPLE | TRUST

**IBDO**

Within the current global context of increasingly complex geopolitical pressures and conflicts, in an economic landscape still recovering from the impacts of the pandemic and grappling with the financial challenges accompanying sustainable development, it is perhaps more important than ever to keep fraud losses at a minimum.



The 2024 BDO Fraud Survey, conducted in partnership with Censuswide, aims to provide insights into the fraud issues experienced by UK corporate entities.

500 directors or business owners at firms with 200 or more employees participated in the survey. The BDO Fraud Survey complements the long running FraudTrack publication, our yearly study of publicly reported fraud, by providing current fraud-related experiences direct from the business community.

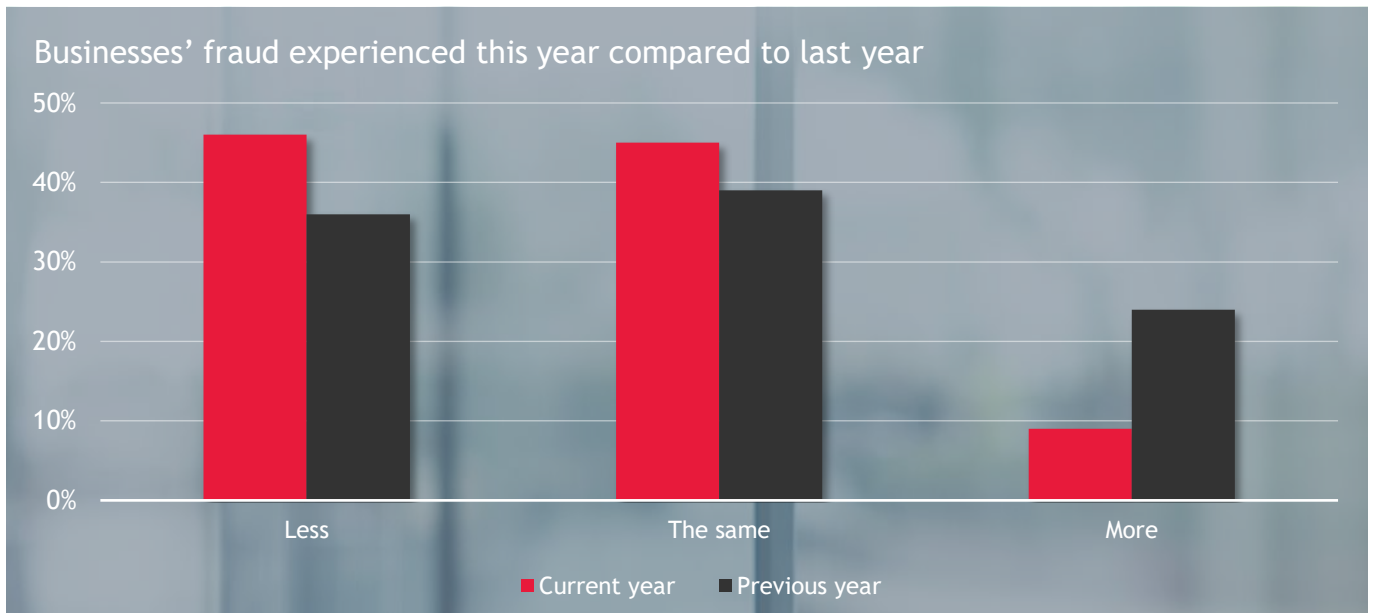
The survey focuses on the assessment by directors and business owners of fraud risks, the impact of fraud and their response to the risks. This includes an evaluation of the impact of the Economic Crime and Corporate Transparency Act ('ECCTA') on businesses' strategic approach to fraud and their fraud outlook for 2025.

---

# Fraud remains a key challenge for UK businesses

The level of fraud suffered by UK businesses remains significant and 42% of businesses surveyed experiencing fraud in the last five years. Whilst this comprises a high proportion it marks an encouraging and somewhat surprising reduction from the previous year figure of 83%.

There were also notably fewer businesses facing multiple fraud incidents, dropping from 49% last year to 15% this year. Consistent with this trend, 46% of businesses reported experiencing less fraud than last year and only 9% saw an increase in fraud incidents over the same period.



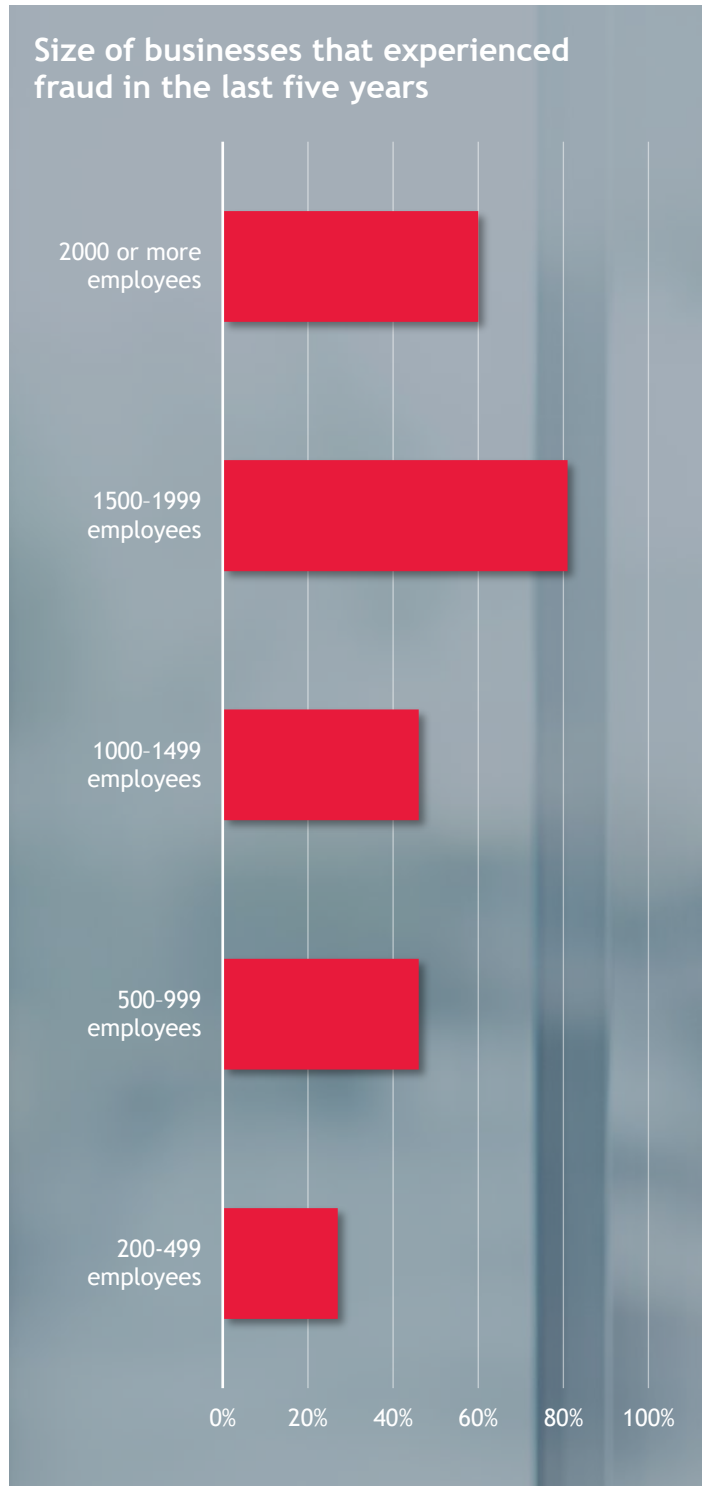
Whilst not all surveyed businesses experienced a decrease in fraud, this general trend of a reduction in reported fraud events this year is an encouraging statistic and may reflect the enhanced fraud prevention and detection mechanisms many businesses have invested in over recent years.



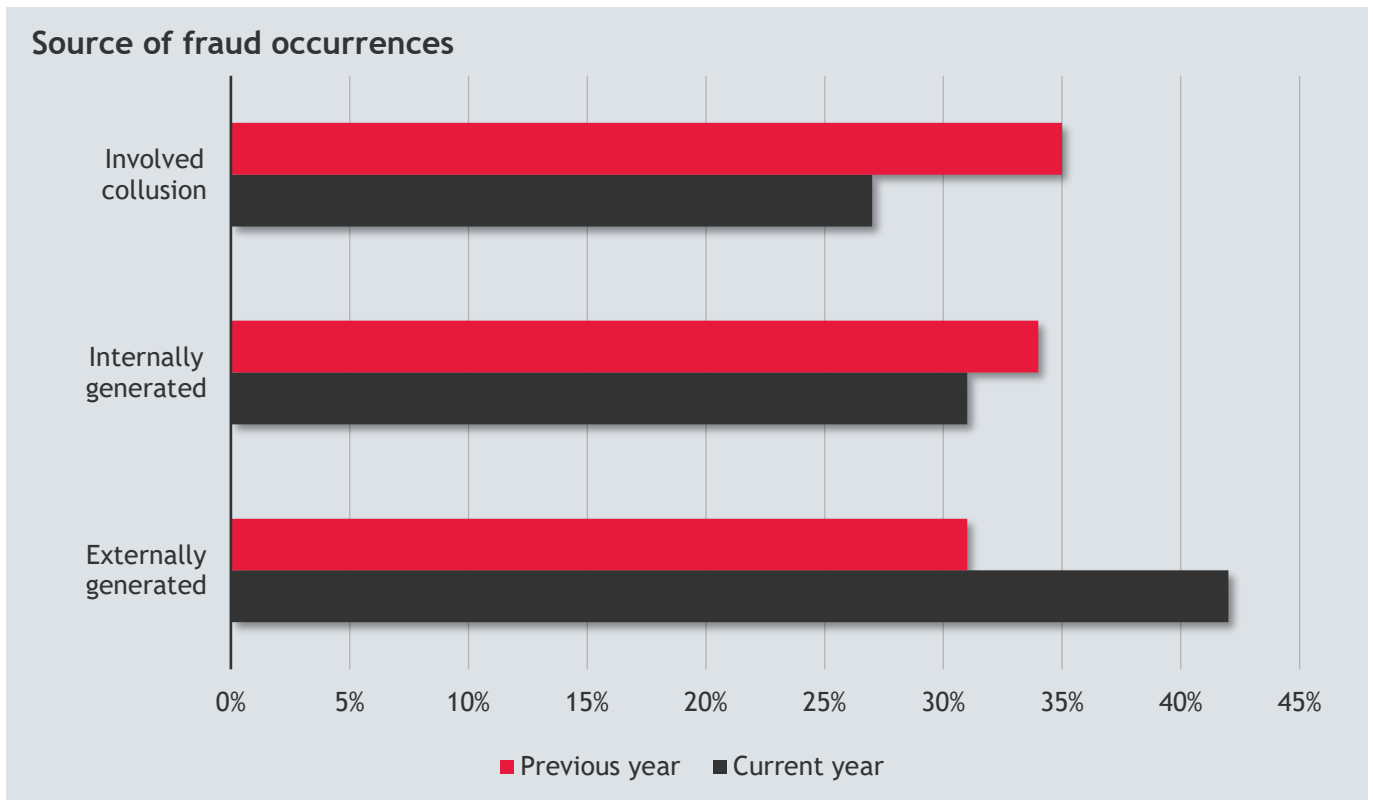
## Smaller businesses experiencing less frauds

Our survey results show a clear pattern in the levels of fraud experienced by different sized businesses in the last five years. Smaller businesses are reporting less fraud occurrences than larger entities. Only 27% of small businesses had suffered fraud in the last five years compared to 81% and 60% respectively for the two largest categories of business.

These figures, suggesting larger businesses are experiencing higher fraud levels, may indicate that fraudsters are targeting the higher potential gains from larger businesses with more potential vulnerabilities and entry points via higher employee numbers and system users. Larger businesses may also have more complex, geographically spread operations and more interaction with third party contractors and suppliers, all potentially contributing to greater fraud risk.



## Increased threat from those external to the business



**Fraud perpetrator trends have shifted this year. The most common perpetrator of frauds suffered by businesses this year was external parties. The proportion of externally generated fraud increased this year to 42% up from 31% last year.**

In contrast, the proportion of fraud that was internally generated or involved collusion decreased by 3% and 8%, respectively.

The rising threat from outside organisations this year is an interesting trend albeit one that is consistent with the ever-evolving cyber threat we see businesses facing every day. The proportionate decrease in internally generated fraud and collusion may be influenced by the trend of more businesses developing their internal anti-fraud culture. Whilst this suggests some entities are getting better at detecting and preventing internal fraud, the figures do underscore the importance of a holistic fraud prevention strategy addressing both internal and external threats.



## The prevalence of financial statement fraud



### Financial statement fraud was the most common type of fraud suffered by surveyed businesses this year (23%).

Financial statement fraud encapsulates a range of accounting actions often involving the manipulation of financial records to present a more favourable picture of a company's financial health. Characteristics can vary and range from overstatement of revenues and bias in accounting judgements to manipulation of journals, provisions and other costs.

Of all the fraud types, financial statement fraud can often have the largest impact. This can be influenced not only by the direct losses from the fraud itself, but also the associated reputational factors, regulatory involvement and the impact on the entity's share price.

The Association of Certified Fraud Examiners (ACFE) 2024 Report on occupational fraud highlights that financial statement fraud has the highest median loss among fraud types.

Our survey shows that corruption and bribery, and money laundering each account for 20% of the fraud suffered by businesses. These activities are often found to

go together, as corrupt practices can facilitate money laundering schemes. Our survey results align with findings from Transparency International's Corruption Perceptions Index and the Financial Action Task Force (FATF) report, which both reflect the prevalence of corruption and money laundering, indicating they are pervasive issues globally.

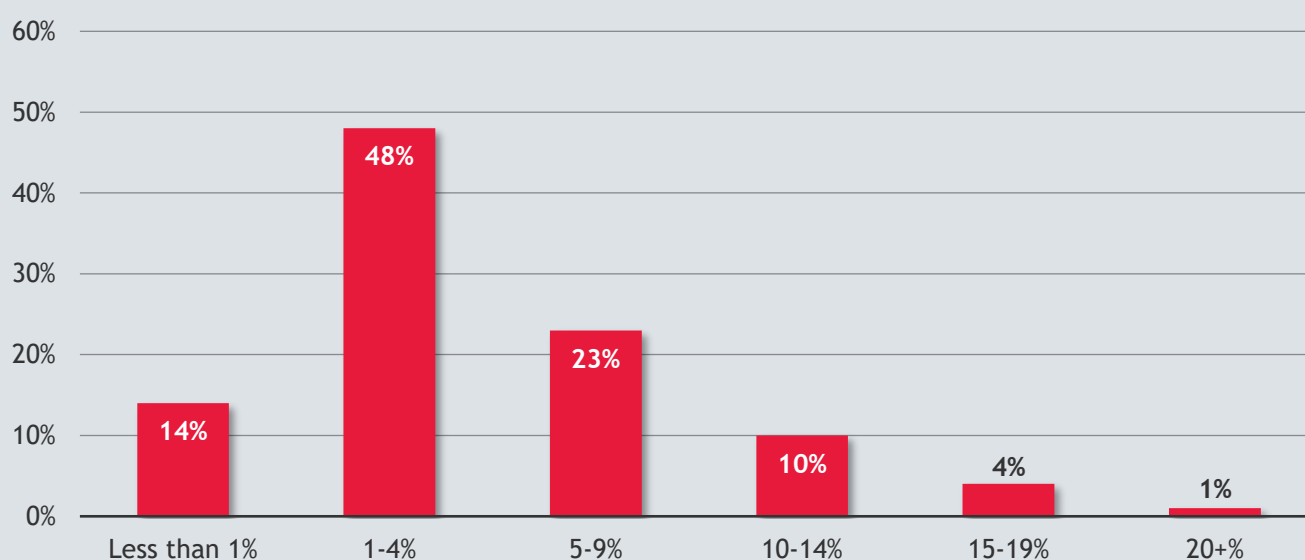
Our survey found that tax fraud was the fourth most common fraud type, accounting for 19% of frauds suffered by businesses. Tax frauds can be linked to several different tax regimes with common examples including VAT frauds and evasion of Corporation Tax or Income Tax through complex offshore arrangements. The introduction of the Corporate Criminal Offences (CCO) for failing to prevent the facilitation of tax evasion may also have had an impact on case numbers.

Accounting for 18% of frauds suffered, asset misappropriation fraud remains an issue for businesses, especially in sectors with valuable stock and liquid assets. Although common, this type of fraud can often be less expensive and is typically easier to detect and prevent, with effective internal controls, compared to some other fraud types. The ACFE's 2024 Report found that asset misappropriation fraud had the lowest median loss.

## How much do businesses lose to fraud each year?

Nearly half (48%) of the respondents reported fraud losses valued between 1-4% of their turnover, making it the most common range. Of even greater concern was that 38% of businesses estimated that their fraud losses were even higher, at 5% or more.

Fraud suffered as a value of annual turnover



The impact of these fraud losses across the UK economy is significant. The latest 2024 FraudTrack publication reported UK fraud losses of £2.3bn last year, a 104% increase on the prior year. Alarming, this is just the publicly reported fraud, so the total value of fraud suffered in the UK will be significantly higher.

At a time when many businesses are finding trading conditions challenging, this really underscores the importance of robust fraud prevention and detection measures.



## Variations in fraud losses across industry sectors

There were some notable variations reported across the different sectors surveyed. Highlights include the following:

**A**

### Charity Sector

Vulnerable to fraud losses

80% of the surveyed businesses in the charity sector reported fraud losses of 5-9% of turnover. This significant loss of resources intended for public good highlights the urgent need for robust internal controls and dedicated fraud awareness programmes to protect charitable funds.

**B**

### Healthcare and Social Assistance Sector

Report high fraud losses

This sector reported significant fraud losses, with 33% of surveyed businesses reporting fraud losses of 10-14% of turnover. Healthcare has long been a sector that is a target for fraudsters and these substantial fraud loss figures underscore that critical vulnerabilities remain at a time the sector can least afford it.

**C**

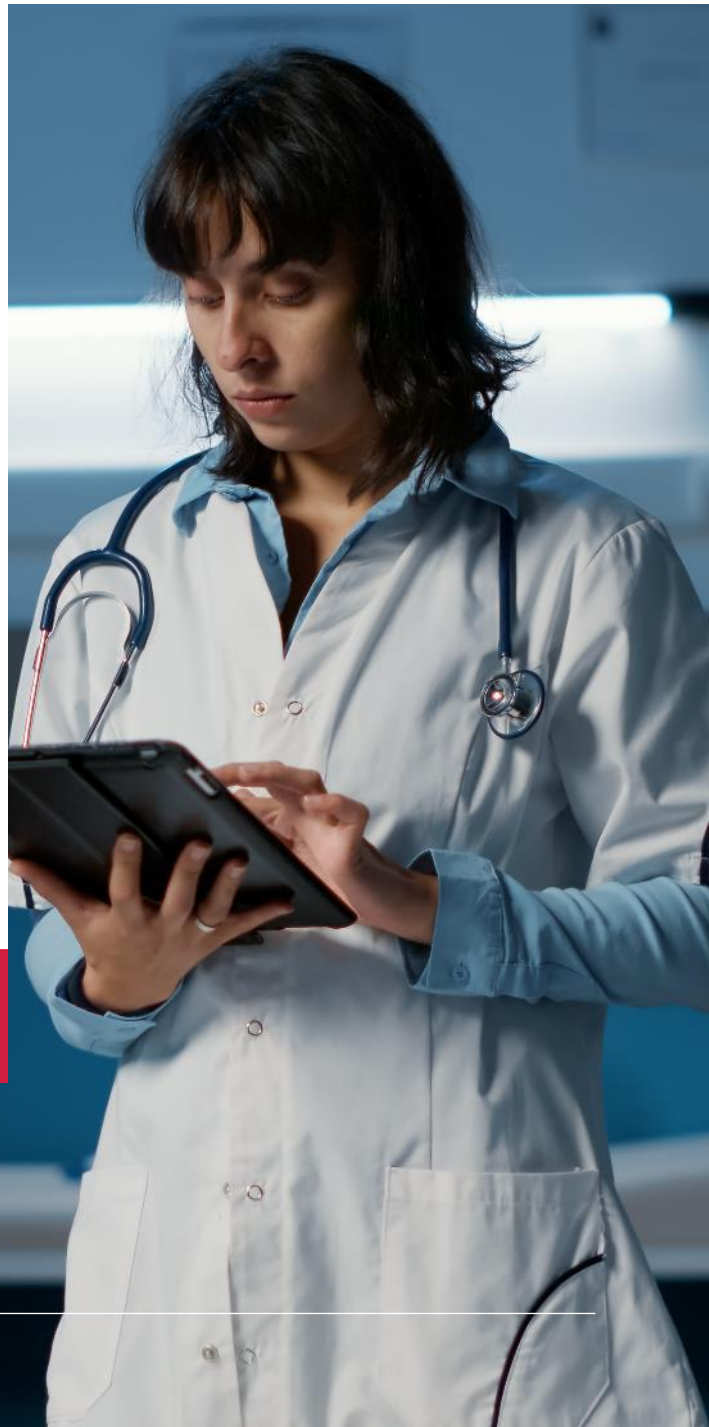
### Professional, Scientific and Technical Services Sector

Report fraud loss spike

This sector showed a diverse spread of fraud losses, with 44% reporting losses of 1-4% of turnover and an alarming 22% in the 20+% turnover range suggesting they would benefit from a robust and tailored fraud prevention program.



Addressing these sector-specific challenges is crucial to safeguarding resources, maintaining trust and protecting the bottom-line.



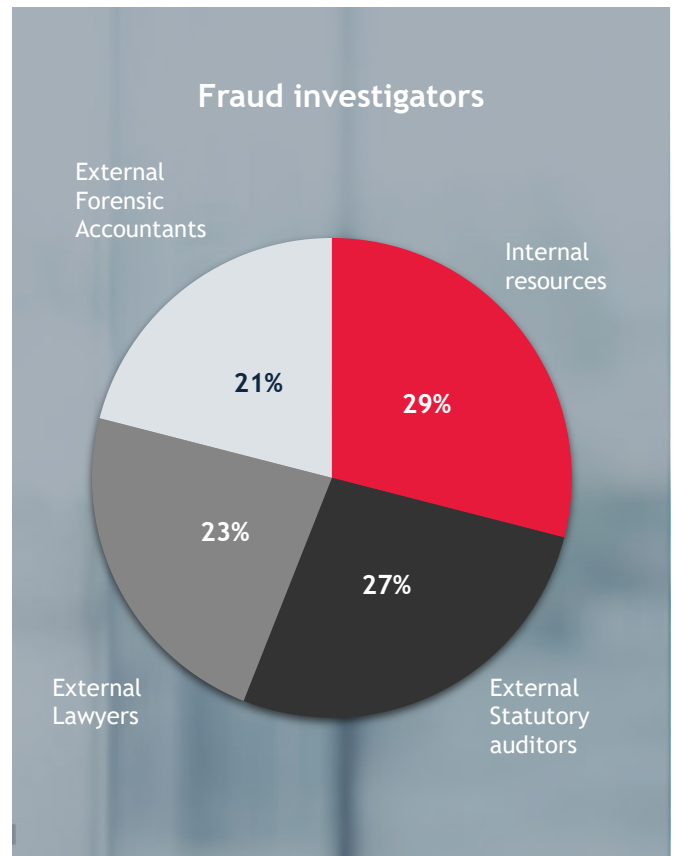


## Who investigates the fraud?

Most businesses used external resources to conduct their fraud investigations, with 71% of businesses reporting they used external lawyers, auditors or forensic accountants to investigate. Only 29% of businesses conducted their investigation using internal resources.



Many frauds, in particular financial statement frauds, can be complex and require specialist expertise to unravel. It is therefore understandable that more businesses are turning to professional resources to investigate fraud.



A specialist external team, familiar with investigating financial crime can be crucial in securing and reviewing evidence. Financial statement frauds can often involve concerns over the actions of members of the internal finance team or senior management. An independent specialist can help businesses establish the facts, so they identify and remove any bad apples.



## Recovering fraud losses is challenging

Our survey shows a consistent theme - recovering a significant amount of fraud losses is challenging.



Whilst some businesses have had success through the courts or claiming on tailored insurance policies, sadly most respondents (58%) expected to recover less than 10% of their fraud losses. Full or near-full recovery was expected by only 2% of the surveyed population.

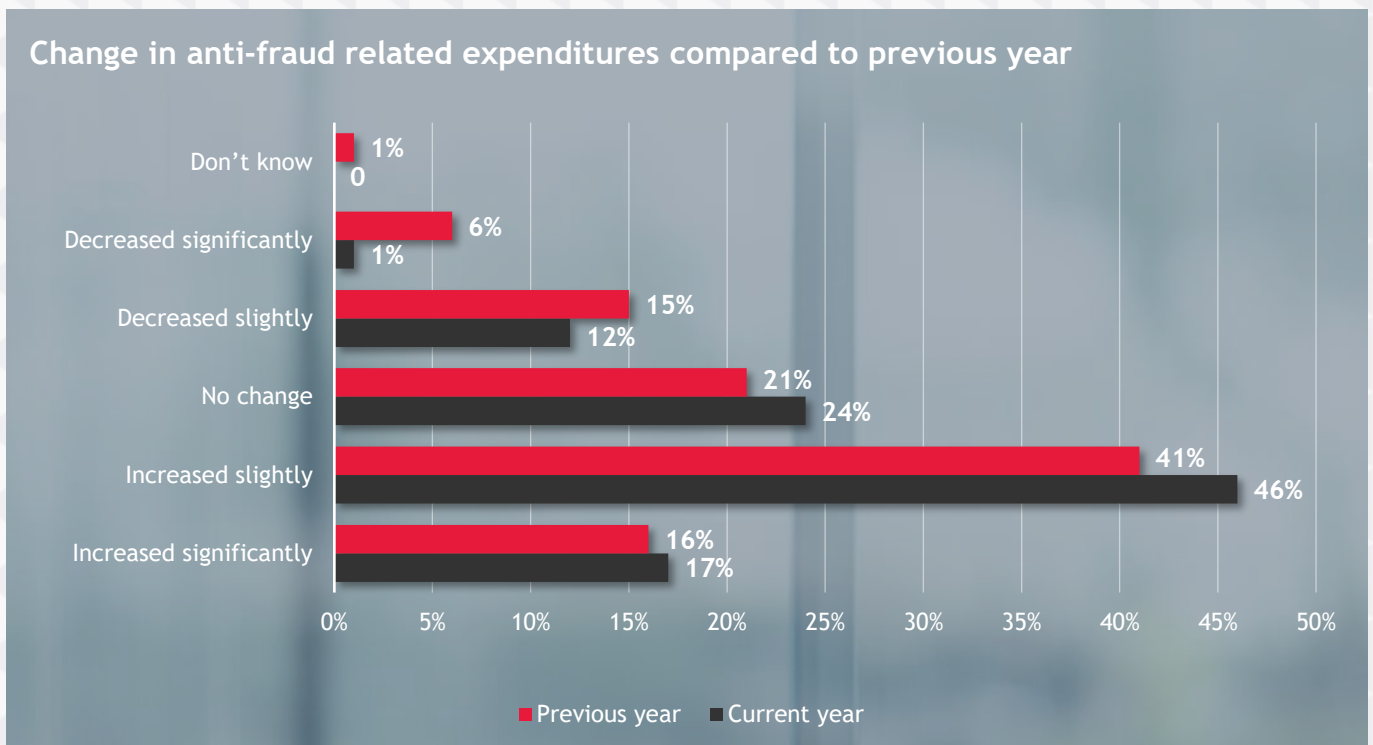
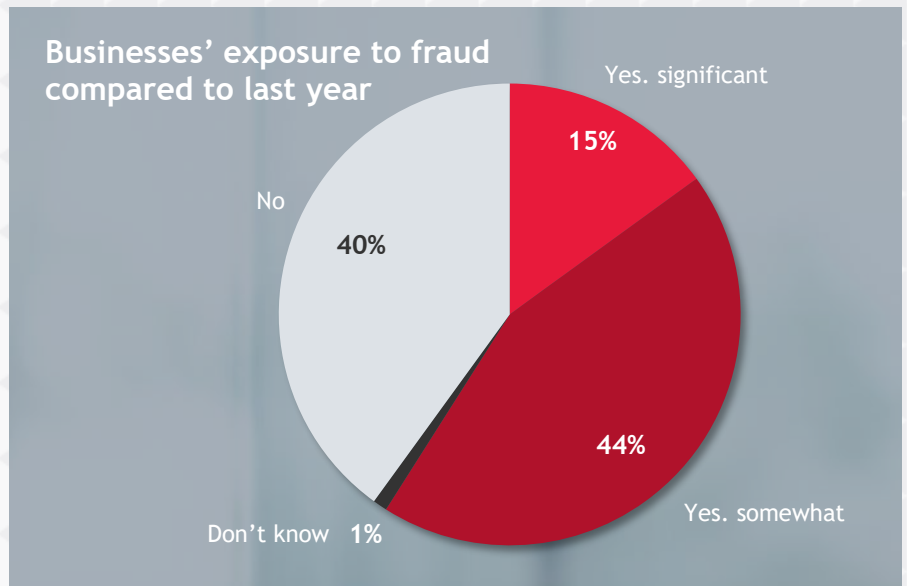
The data reveals the stark reality for many businesses that any form of fraud recovery is an uphill battle. There is therefore a critical need for improved fraud response strategies and engaged professional external support systems to enhance fraud recovery rates.



# Businesses ramp up anti fraud spending in response to rising fraud concerns

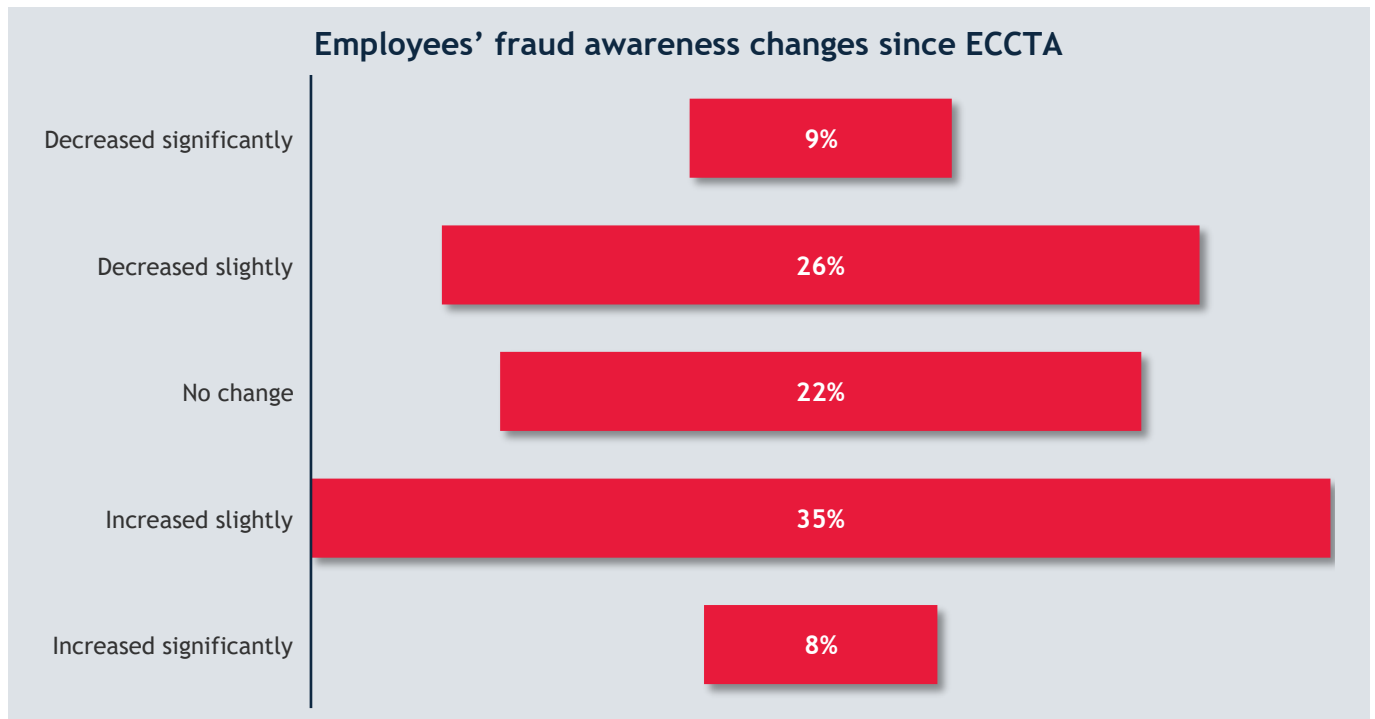
Our survey revealed that 59% of businesses felt more exposed or significantly more exposed to fraud than last year.

It also revealed that 62% are concerned about fraud (up from 44% in the prior year), with nearly two thirds of businesses (63%) recording an increase in anti-fraud related expenditure.



This increased perceived exposure and raised concern about fraud may be linked to the introduction of the new corporate criminal liability legislation which for many has directly influenced the amount spent on anti-fraud measures. These high levels of concern over fraud are also consistent with the landscape of high fraud losses as a percentage of turnover and low expected recovery rates.

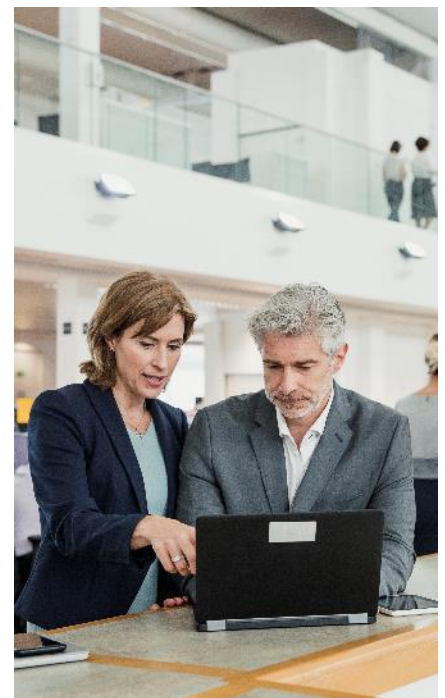
## Fraud awareness increases with the introduction of ECCTA



Some 43% of surveyed businesses reported an increase (slightly and significantly) in fraud awareness among employees since the introduction of ECCTA. This rise likely reflects the refreshed anti-fraud activities many businesses have undertaken since the introduction of ECCTA including employee training and fraud risk assessment. It may also reflect a heightened general exposure to fraud among the UK public with increased media and political attention on fraud regularly highlighting its significant economic impact to us all.

However, fraud awareness is not uniform across businesses. The 35% of businesses reporting a decrease in fraud awareness suggests that many are lagging behind in ensuring their employees are fully engaged in combating financial and economic crime.

Over the next year we would hope to see a further improvement in awareness levels as increased numbers of businesses invest in enhancing their anti-fraud training and communication strategies to ensure that all employees understand the implications of ECCTA and are well-equipped to recognise and prevent fraud. By fostering an anti-fraud culture and greater overall fraud awareness entities can use staff to proactively protect the business more effectively.



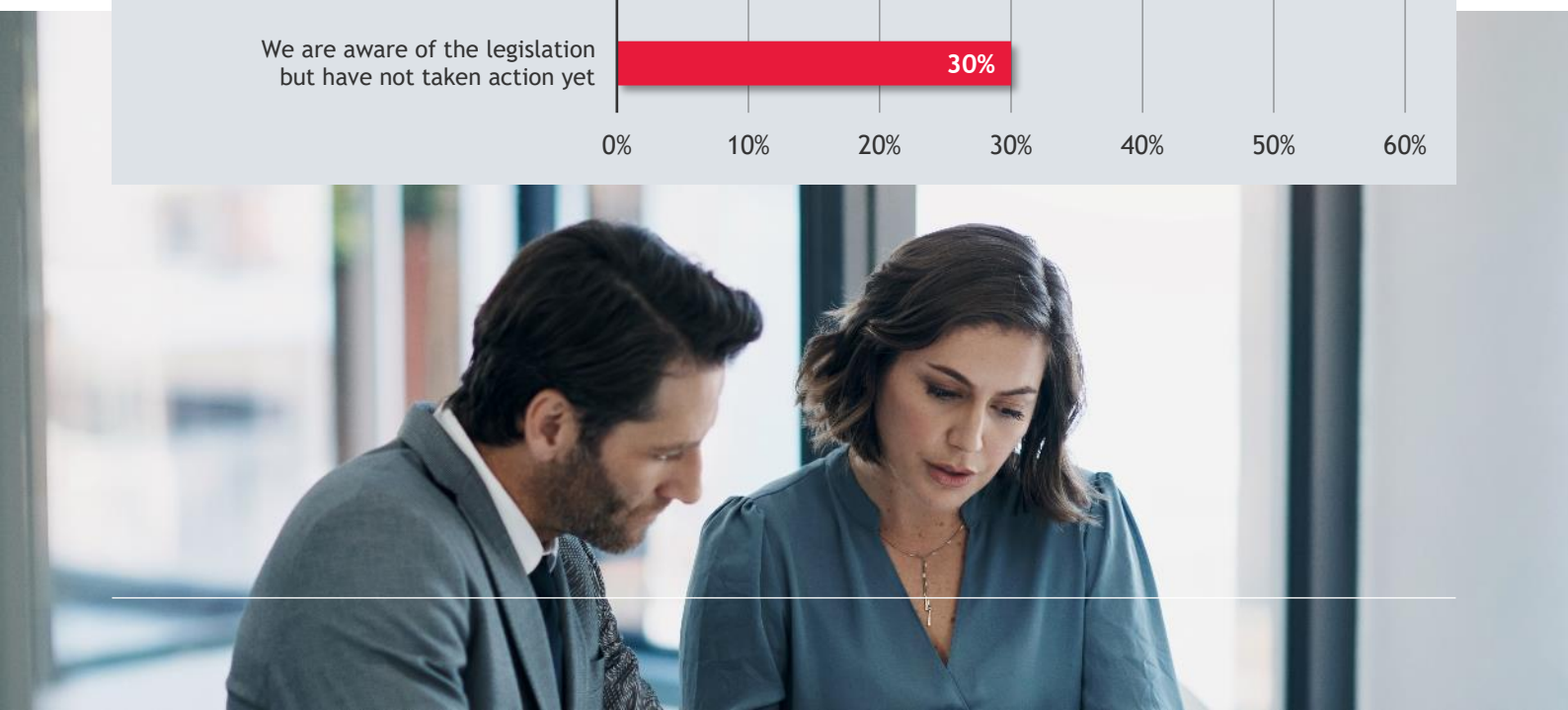
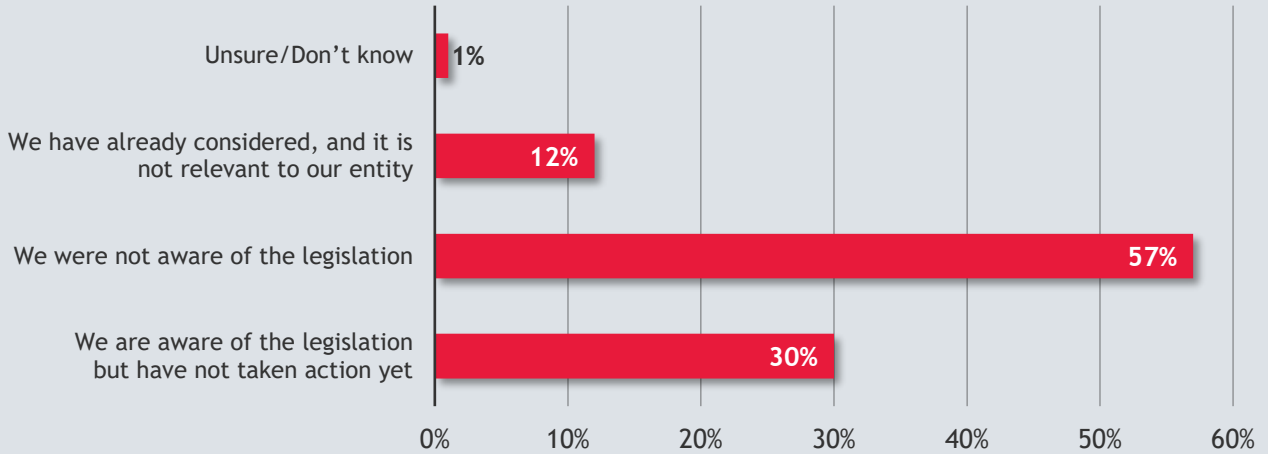
# Most businesses are proactively preparing for ECCTA

With over 78% of our survey respondents reporting that they have begun preparations for the forthcoming 'failure to prevent' fraud legislation within ECCTA, the level of awareness in the business community appears to be generally strong. Most of these organisations (86%) are seeking external expertise to navigate the new fraud legislation.

However, there is still a notable proportion of unprepared entities given that 57% of those that hadn't commenced preparations yet admitted they were not aware of the legislation.



## The reasons why some businesses had not yet prepared for ECCTA





Businesses should carefully consider the implications of ECCTA for their specific entity, review the newly released Government guidance and ensure their anti-fraud programme is documented, communicated and actively followed.

Somewhat surprisingly our survey found that only 19% of businesses conducted a fraud risk assessment in the last year, and just 38% provided fraud awareness training. We expect both figures to rise next year as more entities update their anti-fraud measures in response to ECCTA.

The last time businesses conducted risk assessment and training



# Cybersecurity: a priority for businesses

New cyber threats continue to emerge and 10% of businesses surveyed reported they had been targeted by fraudsters using deepfake clones in the year. Cybersecurity has remained a critical tool for businesses and our survey found that 17% had increased IT security investment and 14% took specific steps to ensure their business data was more secure.

Given the ever-evolving nature of cyberattacks, businesses must ensure their investment in cyber security keeps pace. Deepfake clones, sometimes used over bogus video conferencing calls, are just one of the latest modes of attack faced by businesses this year with technology and AI providing a host of new opportunities for fraudsters. Another common theme we have seen is fraudsters

continuing to target data held by entities, often demanding a ransom to return data or unlock systems and causing long and expensive disruption to operations.

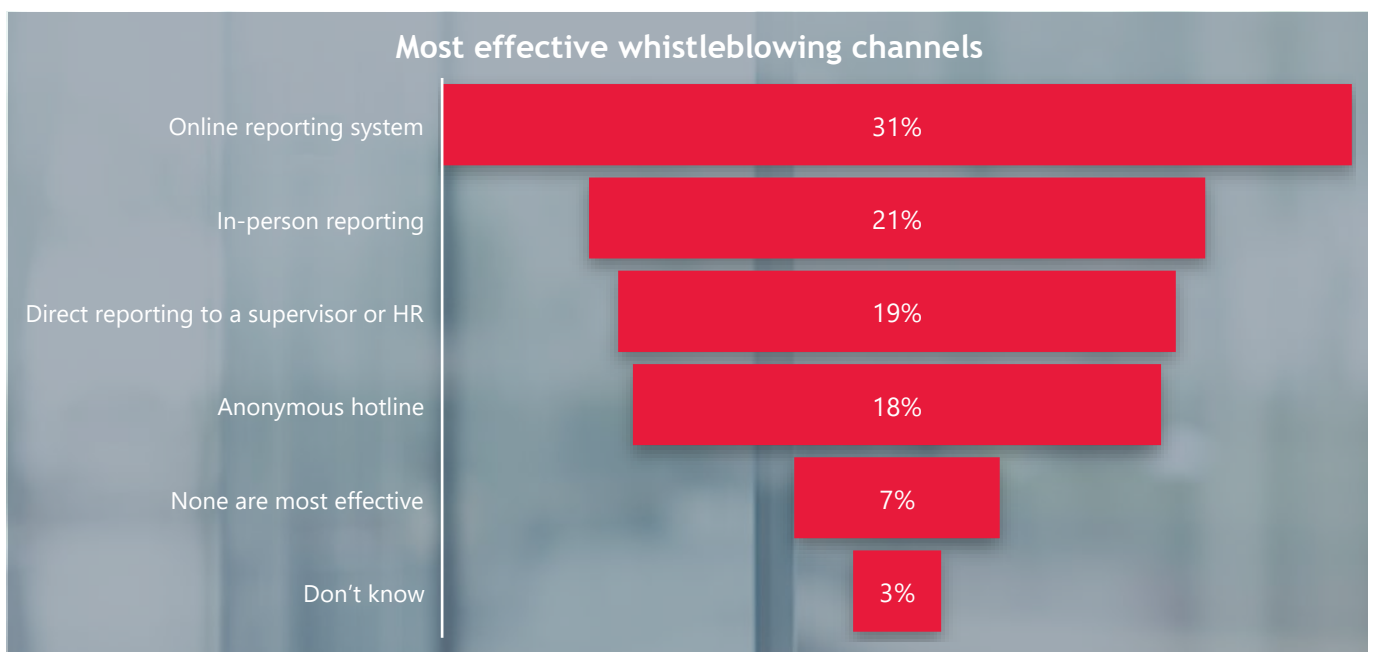
Regularly updating security measures and training staff to recognise and respond to threats should be a priority. Businesses should take a proactive approach to stay ahead of potential threats by:

- 1 Enhancing Cybersecurity measures:** invest in and upgrade cybersecurity infrastructure to reduce the risk of attacks and breaches.
- 2 Increasing investment in fraud detection:** allocate more resources to advanced fraud detection tools, including AI and data analytics, to outpace sophisticated fraud techniques.
- 3 Addressing emerging threats:** develop specific strategies to counter new threats like Deepfake clones, including training and technology investments.

## Whistleblowing leads the way for fraud detection

Whistleblowing remains a key source of fraud detection. Businesses told us that the most common method of fraud detection (19%) was through whistleblowing (the majority of that being internal whistleblowing).

When asked to rank the most effective types of whistleblowing mechanism, 31% of businesses rated online reporting systems highest, with 21% choosing in-person reporting.

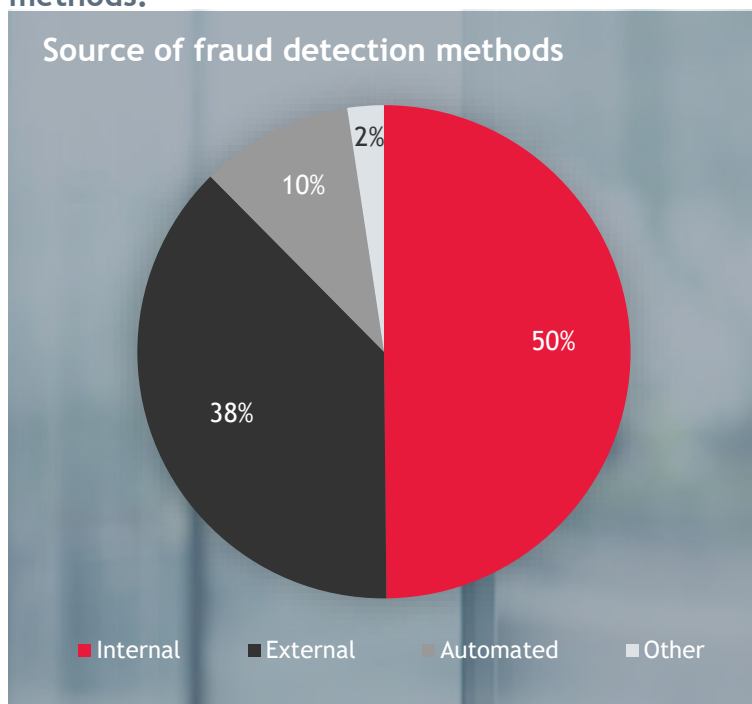


Given the recognised **importance of whistleblowing in fraud detection**, it was surprising that only 9% of businesses reported that they had a formal whistleblowing policy document in place. We would expect to see this figure rise significantly next year as more businesses formalise their antifraud culture and respond to the introduction of the ECCTA.



## The importance of internal detection techniques

Internal detection methods can be a valuable source of information for businesses in helping to highlight bad practices quickly and efficiently. The four core internal fraud detection methods, comprising internal controls, internal auditing, internal fraud teams and internal whistleblowing, accounted for 50% of the detection methods.



This highlights the importance of having robust internal mechanisms and a culture that encourages employees to work diligently and report any wrongdoing or red flags. Dedicated internal audit functions, given free access to internal data, and working on a varied, risk-based test program can be a powerful tool in fraud detection.

### Detection through data

10% of fraud was detected using automated detection techniques or data analytics. It is expected that these techniques will become even more prevalent and influential in future as businesses become more adept at harnessing the anti-fraud capabilities of emerging technology and data analytics.

Given the wide range of antifraud technology now available it was perhaps surprising that only 13% of businesses reported increased spending on fraud detection tools such as AI and data analytics this year. We expect to see this figure rise further in the future years.



## Concluding comments



*“Fraud remains a significant problem for individual businesses and the wider economy. It is noteworthy that over a third of surveyed businesses estimate that their fraud losses are 5% of turnover or higher. These losses directly impact profitability and can therefore have catastrophic knock-on effects. This is consistent with the scale of issues we regularly see when conducting investigations.*

*However, this year there are some definite positive trends within the data. Nearly half of the businesses surveyed experienced less fraud than the previous year, and over three-quarters have started preparing for the new failure to prevent fraud offence.*

*This is encouraging. We hope the coming year will see all businesses enhance their anti-fraud infrastructure, continue the drive to establish more robust preventative regimes, and proactively monitor and respond to new threats as they arise.”*

**Stephen Peters**  
Head of Investigations  
Partner, BDO LLP



FOR MORE INFORMATION:

**Stephen Peters**

Partner

+44(0)7794 243 761  
stephen.peters@bdo.co.uk

**Richard Shave**

Director

+44(0)7711 887 413  
richard.shave@bdo.co.uk

**Karen Edwards**

Director

+44(0)7866 148 363  
karen.edwards@bdo.co.uk

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

Copyright © November 2024 BDO LLP. All rights reserved.  
Published in the UK.

[www.bdo.co.uk](http://www.bdo.co.uk)