KPMG

Fraud Barometer 2023

A snapshot of fraud in the UK

February 2024

–

kpmg.com/uk

Welcome

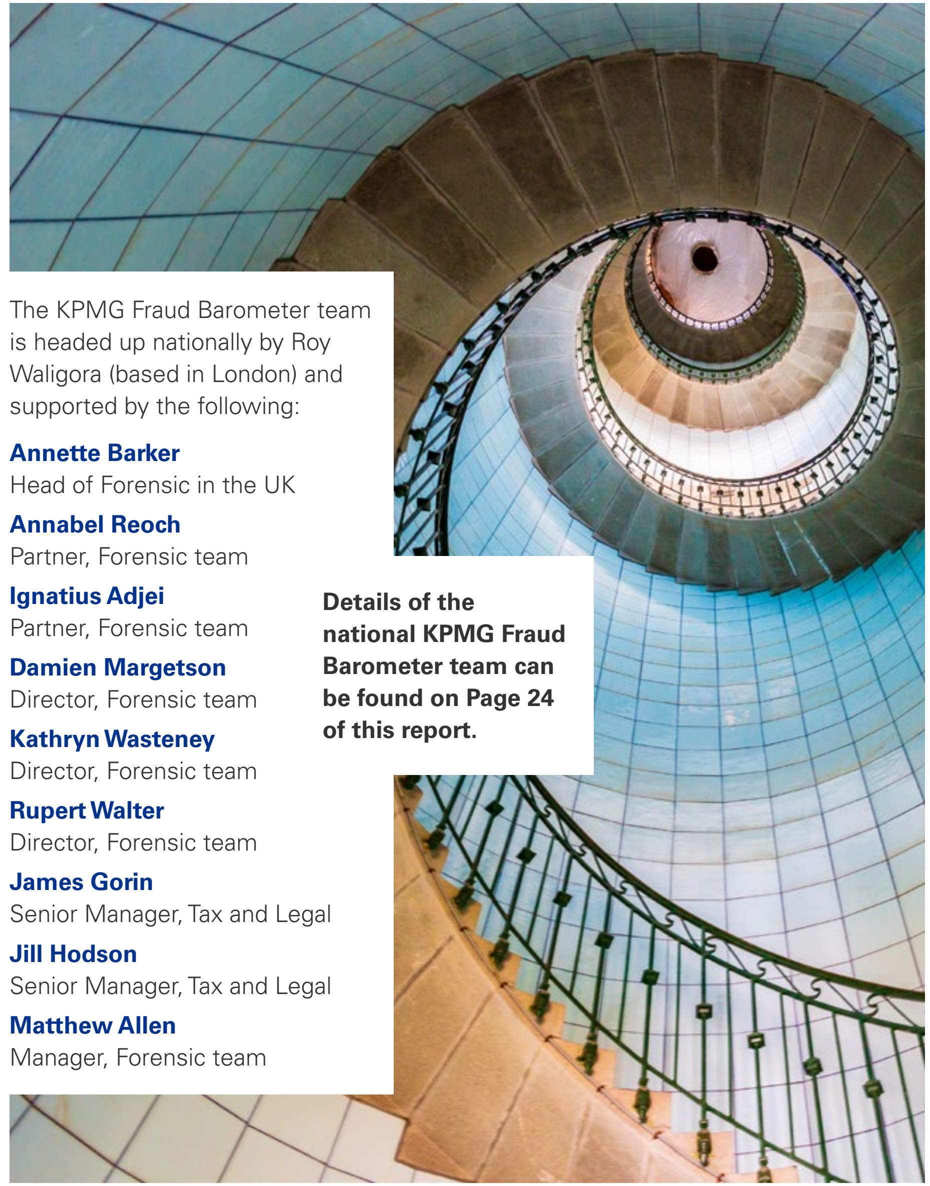
There is real concern in the public and private sectors in the UK that fraud is now at unprecedented levels – according to the Home Office, fraud accounts for over 40% of crime but receives less than 1% of police resource.

In response we have seen the government issue its Fraud Strategy and there is new legislation including the "failure to prevent fraud" offence introduced in the Economic Crime and Corporate Transparency Act 2023.

Following from this, business is responding by refreshing approaches to fraud prevention and management in an ever-evolving field. With this context in this year's KPMG Fraud Barometer, one of the longest running surveys of its type in the UK, we have sought to present the picture of higher value fraud cases together with insights from our specialists on emerging fraud trends with a look at the new legislation, Tax, ESG, Financial Services, Data Analysis and AI.

I hope you enjoy this year's report and I wish to thank my fellow contributors and team that have made this year's publication possible. If you have any questions about the report and / or wish to have a discussion on how we can help you better prevent, detect and respond to fraud then please get in touch.

Roy Waligora,
Partner and Head of
UK Investigations, KPMG



The KPMG Fraud Barometer team is headed up nationally by Roy Waligora (based in London) and supported by the following:

Annette Barker
Head of Forensic in the UK

Annabel Reoch
Partner, Forensic team

Ignatius Adjei
Partner, Forensic team

Damien Margetson
Director, Forensic team

Kathryn Wasteney
Director, Forensic team

Rupert Walter
Director, Forensic team

James Gorin
Senior Manager, Tax and Legal

Jill Hodson
Senior Manager, Tax and Legal

Matthew Allen
Manager, Forensic team

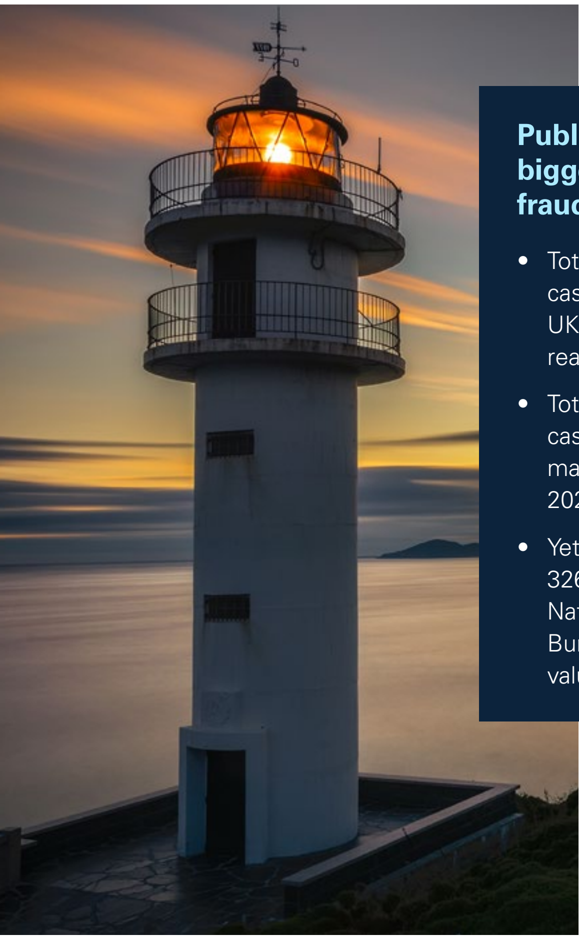
Details of the national KPMG Fraud Barometer team can be found on Page 24 of this report.

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Contents

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The national picture



Public sector becomes biggest victim of fraudsters'

- Total value of alleged fraud cases of over £100k reaching UK Crown Courts in 2023 reached £992.9 million.
- Total volume of alleged fraud cases of over £100k increased marginally from 221 cases in 2022 to 226 in 2023.
- Yet, in 2023, there were 326,199 reports made to the National Fraud Intelligence Bureau with a reported loss value of £2.1 billion.

Figures published today from KPMG UK's Fraud Barometer, which records alleged fraud cases with a value of £100k and above, revealed that the total volume of fraud cases heard in UK Crown Courts has slightly increased from 221 cases in 2022 to 226 cases in 2023 whereas value decreased slightly from £1.1 billion to £992.9 million

Fraud in the UK is perceived to be at unprecedented levels and according to the Home Office, fraud accounts for over 40% of crime but receives less than 1% of police resource[1]. As overall fraud levels continue to rise, today's figures suggest Crown Courts cannot keep up with prosecuting the perpetrators of this crime and case backlogs remain a challenge. To put today's numbers in context, in 2023, there were 326,199 reports made to the National Fraud Intelligence Bureau with a reported loss value of £2.1 billion.

Whilst the total value of reported high value fraud cases heard in UK Crown Courts has slightly declined since 2022, decreasing from £1.1 billion to £992.9 million in 2023 (a decrease of 12 percent), it is evident that criminals are still managing to dupe victims out of large amounts. This is despite legislative and business efforts to turn the tide on fraud.

The general public continues to be taken advantage of by perpetrators of fraud. In 2023, 78 cases of fraud were perpetrated against a member of the public, for a total value of just over £58.3 million, compared with 74 in 2022, totalling £137.4 million. Evidence indicates that some members of the general public are becoming repeat victims of fraud. According to The UK Government's Fraud Strategy, in the year ending December 2022, 1 in 15 adults were victims of fraud, with 18 percent of this group falling victim to fraud more than once.

As with previous years, professional criminals were the biggest perpetrator type by volume (90 cases). However, by value, private individuals were the biggest perpetrator responsible for £426.6 million across 23 cases. This value is largely driven by a single super case with a value of approximately £416 million involving misrepresentation of assets held in a trust.

1. https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public#:~:text=Most%20importantly%2C%20victims%20must%20know,than%201%25%20of%20police%20resource."Policy paper: Fraud Strategy: stopping scams and protecting the public

KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Roy Waligora,
Partner and Head of
UK Investigations, KPMG

> **"The timely prosecution of economic crime remains a challenge, so in the context of rising fraud rates, it is disappointing to see little change in the number of high-value fraud cases being heard in UK Crown Courts. Impending changes in the law intended to improve fraud prevention and reporting, including the 'failure to prevent fraud' offence introduced in the Economic Crime and Corporate Transparency Act 2023[2], combined with investment in technologies such as generative AI to improve fraud detection, could make it even harder for courts to keep up."**

Fraud in the public sector remains persistent

The most common victim type by value during 2023 was Government (£592.7 million). In contrast, in 2022 the most common victim type by value was Financial Institutions (£609.2 million). Commercial Business (£164.6 million) and Investors (£121.7 million) were the next most common victims by value in 2023. Although this could be perceived negatively when taken at face value, it could also be considered positive progress that the government has managed to bring so many fraudsters to justice, including in relation to some legacy COVID-19 fraud cases as well as one significant tax fraud case, being a failure to declare assets with a total value of £416 million.

> **Roy Waligora added:**
> **"Fraud against the government during the pandemic skyrocketed. The 2023 Fraud Barometer data illustrates that prosecuting the offenders is an ongoing issue and one that is likely to continue next year. With the cross-party Public Accounts Committee highlighting the need for the government to do more to recoup money lost to COVID-19 fraud, I expect to see this trend continue into 2024."**

The cost-of-living crisis spurs insider fraud

As the cost-of-living crisis continues, it is inevitable that cases of individuals stealing from their employer will become more prevalent. In 2023, employees and management were significant perpetrators of fraud, involved in nearly half of all cases (43 and 58 cases, respectively), to the staggering combined value of £221.3 million. With a steep decline in job hiring activity, according to the most recent KPMG and REC, UK Report on Jobs, this may create pressure on individuals that could potentially lead to increased levels of insider fraud or possibly enable individuals to rationalise fraud.

> **Roy Waligora observed:**
> **"We are only seeing the tip of the iceberg when it comes to fraud cases triggered by the cost-of-living crisis. While employers want to be able to trust their staff, the temptation to divert funds to their own account is too much for some employees, so businesses need to ensure they have appropriate safeguards in place to protect against fraudulent activity from the inside."**

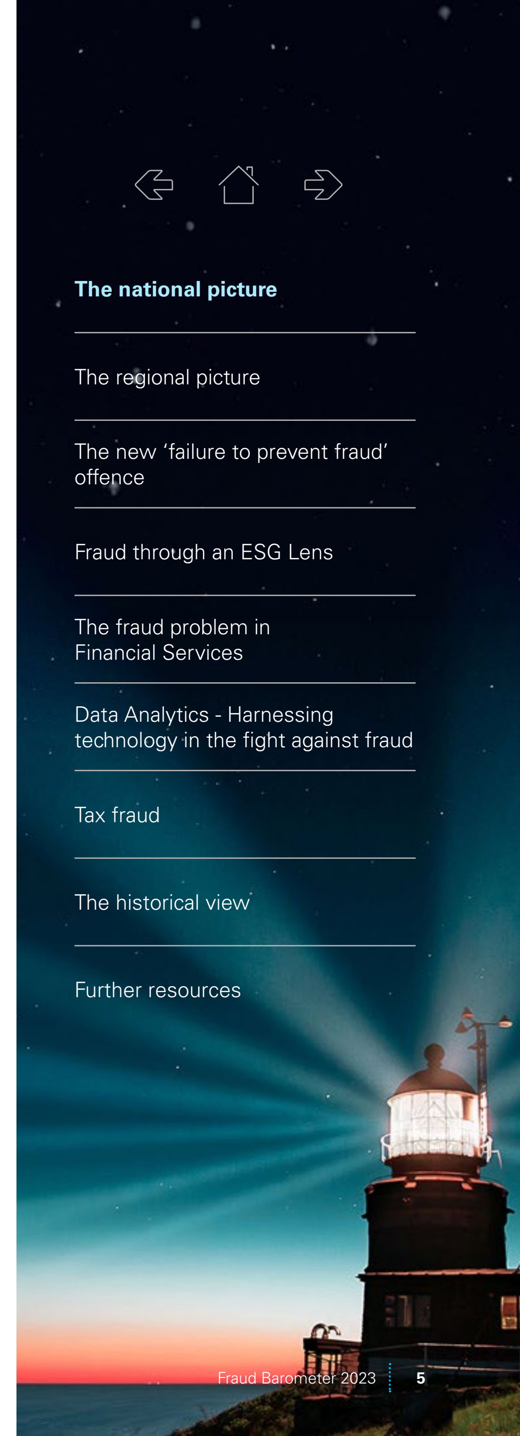
Embezzlement rules as the most common fraud tactic

In relation to insider fraud, embezzlement (by either managers or employees committing embezzlement against their employers, or people stealing from client accounts, charitable funds etc.) has consistently been the most common fraud type by volume within the Fraud Barometer over the last few years. 2023 was no exception, with embezzlement being the most common fraud type by volume (35 cases).

The highest fraud type by value was tax fraud, due to the aforementioned super case with a total of £416 million. Investment fraud was the second highest type of fraud by value (£126.2 million), followed by VAT fraud (£105.1 million).

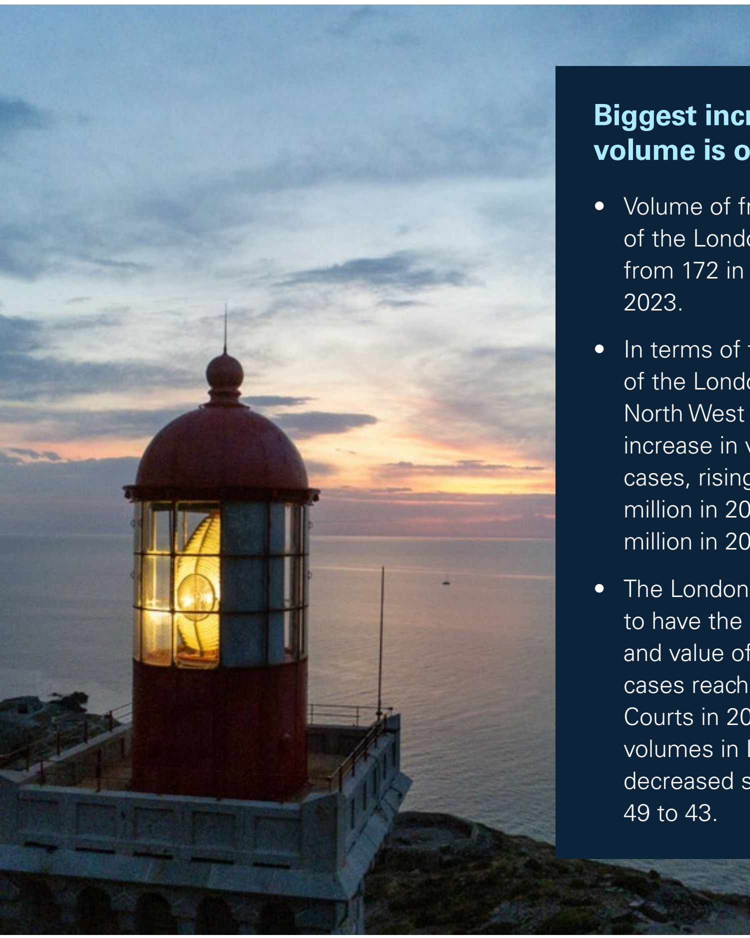
> **Reflecting on the data, Roy Waligora, said:**
> **"Employees often have a good understanding of their employer's controls and processes and may be able to conceal their fraudulent activity more easily to commit embezzlement. Often, we see cases of embezzlement carried out over several years before being detected. However, the newly legislated 'failure to prevent fraud' offence may result in businesses implementing stronger internal controls, which could help mitigate the risk of this crime happening."**

2. https://www.legislation.gov.uk/ukpga/2023/56/enacted" Economic Crime and Corporate Transparency Act 2023



KPMG
© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The regional picture



Biggest increase in fraud volume is outside London

- Volume of fraud cases outside of the London region increase from 172 in 2022 to 183 in 2023.
- In terms of fraud value outside of the London region, the North West saw the biggest increase in value of fraud cases, rising from £24.7 million in 2022 to £122.1 million in 2023.
- The London region continues to have the highest volume and value of alleged fraud cases reaching UK Crown Courts in 2023, albeit fraud volumes in London have decreased slightly from 49 to 43.

Figures published today from KPMG UK's Fraud Barometer, which records alleged fraud cases with a value of £100k and above, showed that reported fraud outside the London region saw the biggest increase in fraud volume from 172 in 2022 to 183 in 2023. Fraud volumes either increased or remained the same as prior year for all regions outside of London, with the exception of Scotland which saw a slight decrease in fraud volumes from 24 to 21 cases.

By contrast, reported fraud values with a value of £100k and above, outside of the London region, decreased by 47 percent from almost £552 million in 2022, to £291.5 million in 2023. Yorkshire and the Midlands in particular saw the biggest decreases in reported fraud values during 2023. Fraud values in Yorkshire and the Midlands decreased by 88 percent and 62 percent respectively in 2023. These decreases are largely driven by no super cases being reported in 2023 across these regions, compared with 2 super cases in 2022, i.e. cases with a value of £50 million or more. The highest value cases in the Yorkshire and Midlands regions were £20 million and £30 million respectively in 2023.

Fraud values in the London region increased to £701.4 million across 43 cases, up significantly from £577.5 million across 49 cases in 2022. This is largely driven by a single super case with a value of approximately £416 million involving tax fraud.

Across the UK, the North West region had the second highest value of fraud cases with £122.1 million. By volume, the Midlands experienced the second highest amount with 37 cases reaching Crown Courts throughout 2023.

KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Annette Barker,
Head of KPMG Forensic UK at KPMG

> **"Given that London is a major financial hub, it is understandable why the capital is the UK's fraud hotspot. However, the high levels of fraud in the North West and the Midlands, which both have less financial activity than London, show that nowhere is safe from fraudsters."**

Professional criminals elude the law in the London region

Although the London region continued to have the highest volume and value of fraud cases, in 2023, fewer professional criminals were brought to court compared to 2022. In 2023, 18 cases totalling £123.7 million were heard in the London region, compared to 24 cases worth £265.7 million in 2022.

The North West saw the biggest jump in terms of fraud value committed by professional criminals, up from £8.1 million in 2022 (nine cases) to £101 million in 2023 (11 cases).

Whereas the North East and Yorkshire regions saw the biggest decrease in value from £269.5 million in 2022 (11 cases) to £8.6 million in 2023 (15 cases). Fraud values in the South East decreased slightly from £7.9 million in 2022 (nine cases) to almost £4 million in 2023 (seven cases).

> **Reflecting on the data, Annette Barker, said**
>
> **"As fraud has grown in sophistication and complexity, it has, therefore, become harder to prosecute professional criminals for their acts. Fraudsters appear to have wised up to this, committing even more crimes."**

Cases involving the Scottish public plummets

Nationally, the general public continues to be taken advantage of most frequently by perpetrators of fraud; in 2023, 78 cases of fraud were against a member of the public, for a total value of £58.3 million, compared with 74 in 2022, totalling £137.4 million. London bears the brunt of this crime, with 16 cases heard in 2023 worth £32.1 million.

The total volume and value of alleged fraud cases heard in the Scottish courts decreased in 2023 to 21 cases with an aggregate value of £11.9 million, down from 24 cases with an aggregate value of £17.4 million in 2022. Scotland saw a significant drop in terms of the value and volume of alleged fraud against the general public. In 2022, there were 11 cases to the value of £10.3 million, while in 2023, there were just five cases to the value of slightly over £1 million. Yet, a recent report by the Scottish Police Authority revealed a 68 percent increase in fraud cases over the last five years, so the threat to the general public is not going away.

> **Annette Barker added:**
>
> **"With the Scottish Police Authority reporting fraud reaching unprecedented levels, the volume of reported fraud cases reflected in the Fraud Barometer suggest a more nuanced situation. What we do know is that fraudsters are persistent, and individuals and organisations in Scotland should remain alert to the risk of fraud."**

KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The new ‘failure to prevent fraud’ offence

- Damien Margetson and Kathryn Wasteney

Everywhere you look, there are alarming statistics about fraud in the UK. The National Fraud Intelligence Bureau, part of the City of London Police, has quantified the value of reported losses due to fraud in the year ended 31st of December 2023 at £2.1 billion. [The UK Government’s Fraud Strategy](), published last year, highlighted that across England and Wales, there were 3.7 million incidents of fraud reported in 2022, accounting for over 40 percent of all reported crime.

> **The National Fraud Intelligence Bureau, part of the City of London Police, has quantified the value of reported losses due to fraud in the year ended 31st of December 2023 at £2.1 billion.**

In response to the high levels of fraud, the Government has announced a significant shift in its approach to tackling fraud, which includes:

- Strengthening how government, law enforcement, regulators, industry and charities work together to reduce fraud levels;
- A £100 million investment in law enforcement;
- Changes in the law intended to improve fraud prevention and reporting; and
- The implementation of a new system for victims to report fraud to the police.

The new ‘failure to prevent’ offence

One of the measures introduced under the Economic Crime and Corporate Transparency Act 2023, which received Royal Assent on 26th of October 2023, is a new ‘failure to prevent fraud’ offence.

This offence is the next in a series of ‘failure to prevent’ offences intended to encourage organisations to take responsibility for poor systems and controls that may be exploited by individuals to break the law.

You may be aware of the existing ‘failure to prevent’ offences:

- The ‘failure to prevent bribery’ offence introduced under the UK Bribery Act 2010; and
- The ‘failure to prevent the facilitation of tax evasion’ offences introduced under the Criminal Finances Act 2017.

KPMG
© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Under the 'failure to prevent fraud' legislation, a large organisation (defined in line with the Companies Act 2006[3]) may be prosecuted with the potential for an unlimited fine where an 'associated person' (such as an employee, agent or subsidiary) commits a fraud offence intended to benefit the organisation or any person to whom the 'associated person' provides services on behalf of the organisation, regardless of whether senior management of the organisation was aware of the offence being committed. This may apply even if the organisation and the 'associated person' are based outside of the UK.

It is the word 'benefit' that makes this legislation interesting and something that most companies will have to seriously consider. It means that organisations (which include not-for-profit entities and incorporated public bodies as well as companies) will have to assess whether or not their current fraud risk frameworks cover fraud perpetrated by the organisation or just focus on the more common but not relevant (in this context) fraudulent attacks on the organisation, such as theft by employees or attacks from organised criminals.

The factsheet published by the UK Government on the 'failure to prevent fraud' offence makes it clear that the definition of fraud benefiting the company is wide, covering not only misreporting (for instance in the annual report and accounts) but also:

- Dishonest sales and trading practices, hiding information from parties such as consumers or investors; and
- Dishonest practices in financial markets.

Organisations will need to consider whether statements they make about ESG-related matters, the effectiveness of their goods and services and any other reporting, either publicly or to specific third parties are accurate. This also covers statements made by any third-party agents acting on their behalf.

The consequence of this fraud occurring could be greater than an unlimited fine and could result in serious reputational damage.

Is there a defence?

The 'failure to prevent fraud' offence legislation suggests that an organisation will be able to avoid prosecution if it is able to prove that, at the time that the fraud offence was committed, it had 'reasonable procedures' in place to prevent this type of fraud from occurring.

Guidance on what constitutes 'reasonable procedures' is due to be published by the UK Government before the 'failure to prevent fraud' offence comes into force.

It's widely anticipated that this guidance will be similar in nature to the guidance published by the Ministry of Justice in 2011 in relation to the 'adequate procedures' in the context of the 'failure to prevent bribery' offence and the guidance on 'reasonable procedures' published by HMRC in 2017 in relation to 'failure to prevent the criminal facilitation of tax evasion'.

Both of these guidance documents have been principle driven and refer to the importance of preventative procedures not being a tick-box exercise or a checklist of procedures; rather, they should be embedded into the framework of the organisation.

3. An organisation meeting at least two of the three following criteria: annual turnover of more than £36 million, balance sheet total of more than £18 million and/or more than 250 employees.

What can organisations do now to prepare?

Organisations need to consider what anti-fraud procedures they currently have in place and ask the following questions:

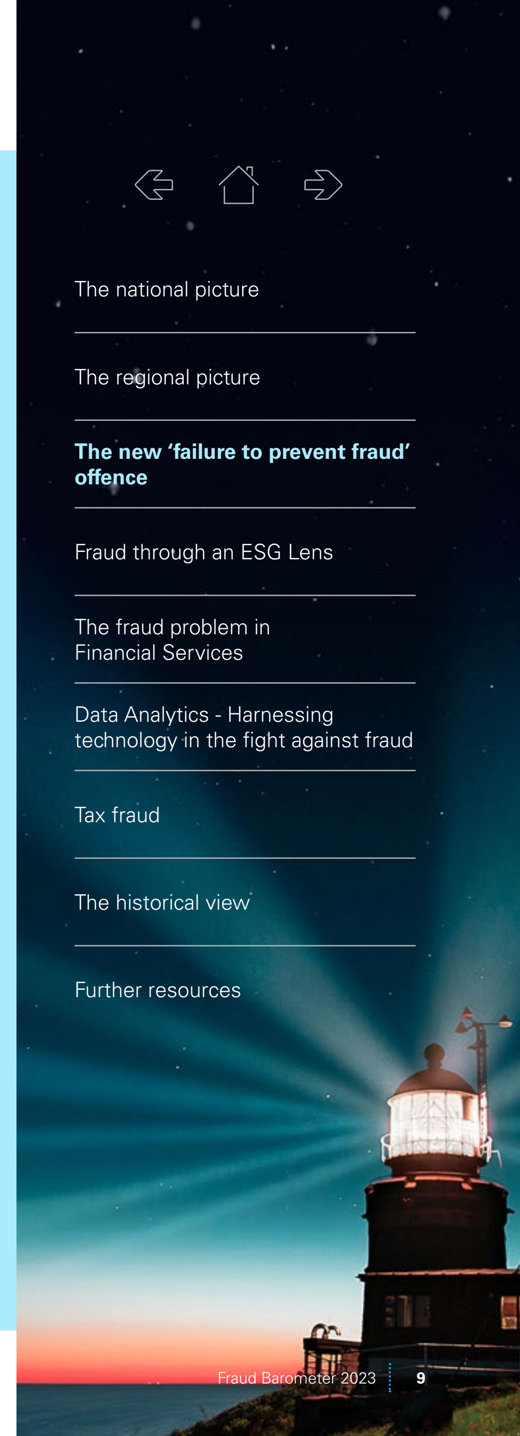
Who is responsible for fraud risk at a Board level?

Do our current assessments consider the risk of fraud that benefits the company?

If they do, how wide is this assessment – is it just limited to the Finance function?

Can we demonstrate a strong anti-fraud culture at our organisation?

How widespread is fraud training? Does it explain what the responsibilities of our employees are and empower them to speak up if they need to?



KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Whilst the questions above would appear to be relatively straightforward, the responses that we have received to our KPMG Fraud Risk Questionnaire would suggest that organisations still have a lot to do.

- More than a third of respondents felt that their businesses had not properly assigned the responsibility for preventing fraud;
- More than 50 percent of respondents indicated that their organisations hadn't properly assessed the fraud risks facing their business and potential impact; and
- More than a third of individuals do not feel that their organisation has been effective in providing training and awareness to combat fraud and thus has not promoted an anti-fraud culture that is likely to be a critical component of the 'reasonable procedures' to prevent fraud under the 'failure to prevent fraud' offence.

There are several fraud cases included in the 2023 Fraud Barometer data that involved the types of fraud offences within the scope of the 'failure to prevent fraud' offence, such as:

- Senior management of a business alleged to have altered paperwork relating to police escort services that was used to overcharge customers for the transport of engineering components;
- A former company director who scammed a finance company through amending or fabricating documents to secure a loan;
- A fraudster who falsified documents in order to mislead investors through a Ponzi scheme that was used to support his own failed business and conceal the company's true financial position; and
- Two former Company Directors who used lies, false claims and a connected company purported to be an independent sales firm to trick customers into signing up to expensive energy contracts.

In all these fraud cases the fraudsters were prosecuted directly for their offences. If similar offences were to be perpetrated at large organisations in the future once the 'failure to prevent fraud' offence comes into force, it is highly likely that not only would the individuals who committed fraud be subject to criminal prosecution, the organisations where they work could also be prosecuted for failing to prevent fraud from occurring, unless they were able to demonstrate that 'reasonable procedures' to prevent fraud had been implemented and the individuals who committed fraud were acting to circumvent these.

In closing, the action being taken by the UK Government in response to the very high levels of fraud that are present in the UK is a positive step forward and we should welcome the legislative changes that come with the 'failure to prevent fraud' offence. This, along with the other measures being introduced by the UK Government, will hopefully make Directors fully realise that they have a responsibility to do more in this area and embrace the requirement to have demonstrable 'reasonable procedures' in place to prevent fraud.

KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Fraud through an ESG Lens

- Annabel Reoch

The growing importance of environmental, social and governance (ESG) factors is fundamentally reshaping businesses. Internal and external stakeholders are all putting pressure on organisations to revisit how their operations impact the world, how they contribute to society, and how they conduct themselves.

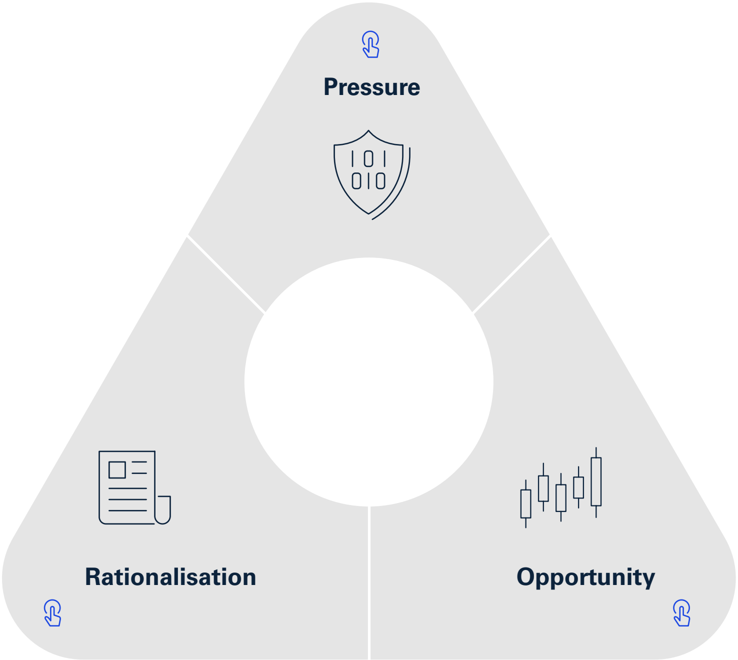
And these factors have become critical for lasting growth. This is changing not just products and services, processes, operations and supply chains but also how fraud can present itself; there are new pressures and incentives at play. So, companies now need to consider the risks of fraud from an ESG perspective in their fraud risk management programmes.

What do these risks look like? Let's understand them through the fraud triangle:

ESG risks meet all angles of the fraud triangle

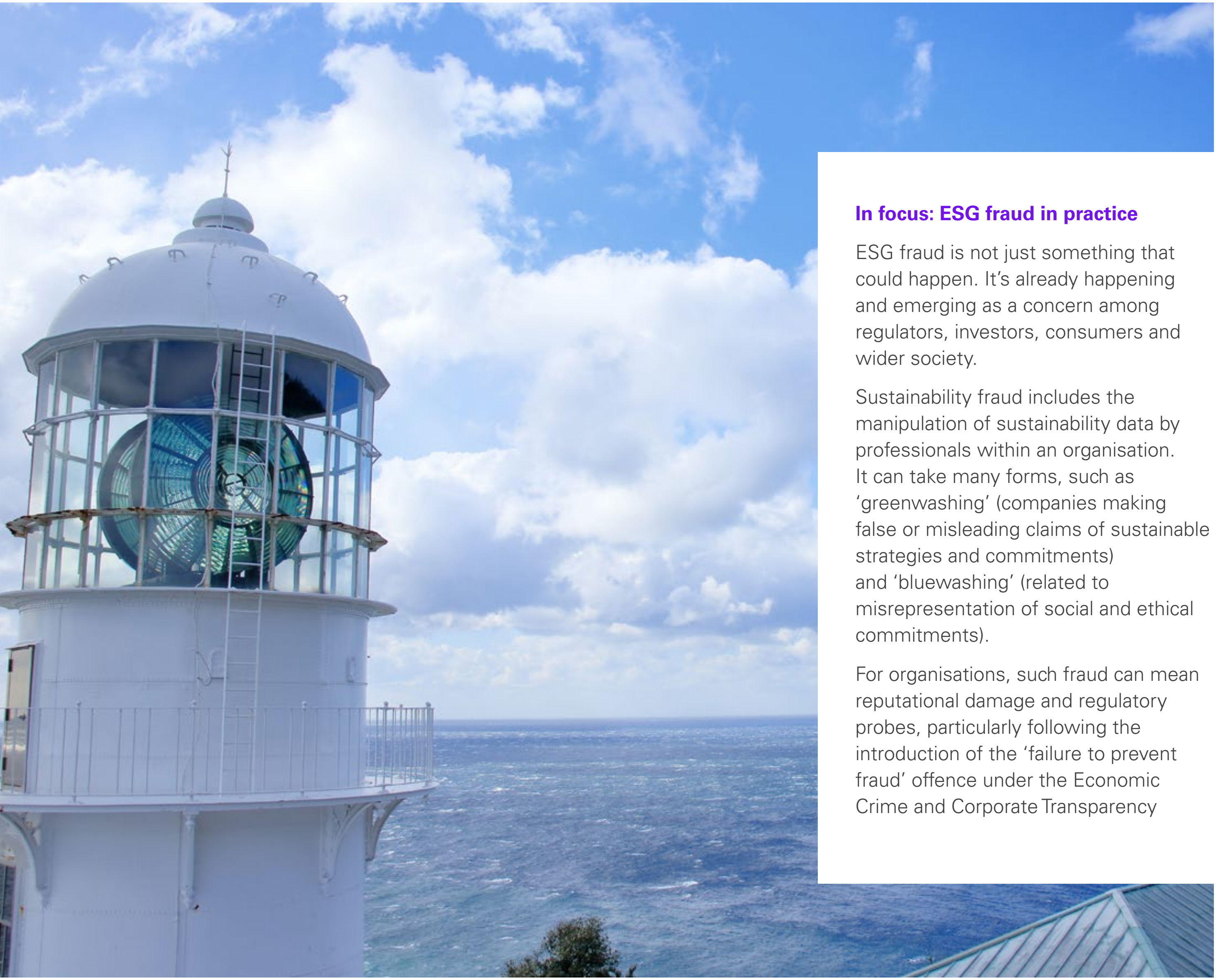
The Fraud Triangle is a framework used to explain why individuals commit fraud. Drawing on criminological research from Edwin Sutherland and Donald R. Cressey, Steve Albrecht coined the term to model conditions that lead to a higher risk of fraud.

The triangle consists of three components: **pressure, opportunity, and rationalisation**. All three elements must be present for fraud to occur.



Click on each shape for more details

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



In focus: ESG fraud in practice

ESG fraud is not just something that could happen. It's already happening and emerging as a concern among regulators, investors, consumers and wider society.

Sustainability fraud includes the manipulation of sustainability data by professionals within an organisation. It can take many forms, such as 'greenwashing' (companies making false or misleading claims of sustainable strategies and commitments) and 'bluewashing' (related to misrepresentation of social and ethical commitments).

For organisations, such fraud can mean reputational damage and regulatory probes, particularly following the introduction of the 'failure to prevent fraud' offence under the Economic Crime and Corporate Transparency Act 2023, which could capture acts of deception through ESG reporting and claims that benefit the organisation. The only possible defence under the legislation is that the business had 'reasonable procedures' in place to prevent or detect the fraud.

It is therefore more important than ever for businesses to establish credibility and trust in ESG reporting. They need to approach ESG fraud risk management with a comprehensive view, reviewing fraud prevention and detection and how non-financial reporting internal processes and controls could be strengthened.

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The fraud problem in Financial Services

- Ignatius Adjei

The UK's banking industry is at the front line of the fight against fraud, with almost all the proceeds travelling through accounts, and attempts by fraudsters to exploit banking customers are a daily occurrence in our lives.

Whilst UK Finance reported in its 2023 Annual Fraud Report[4] that there was an eight percent decrease in overall fraud losses for the year 2022 in comparison to 2021, social engineering continues to grow and is a leading cause of payment fraud losses.

The Evolving Threat of Social Engineering Fraud

Online fraud is prevalent, with nearly nine in ten adult internet users having encountered content online they believe to be scams[5]. New technology also brings new opportunities for fraudsters, who are continuously refining their methods of social engineering with a view to committing fraud and employing ever more sophisticated methods to target victims.

Quick response (QR) codes are becoming a part of everyday life, and criminals are taking advantage of this in the form of 'Qishing'. Malicious QR codes are designed to look legitimate and can be placed in advantageous locations where they would be commonly scanned, such as car parks. The victim is then redirected to a phishing website in an attempt to harvest credentials and information.

Another sophisticated approach is 'Vishing'. By using voice-based 'deepfakes' to impersonate family members or work colleagues, criminals can trick their victims into making urgent payments.

As technology advances, scammers are increasingly exploiting the interconnected nature of our digital lives, and financial institutions are having to become adaptive with their anti-fraud measures to keep up.

Regulatory Changes

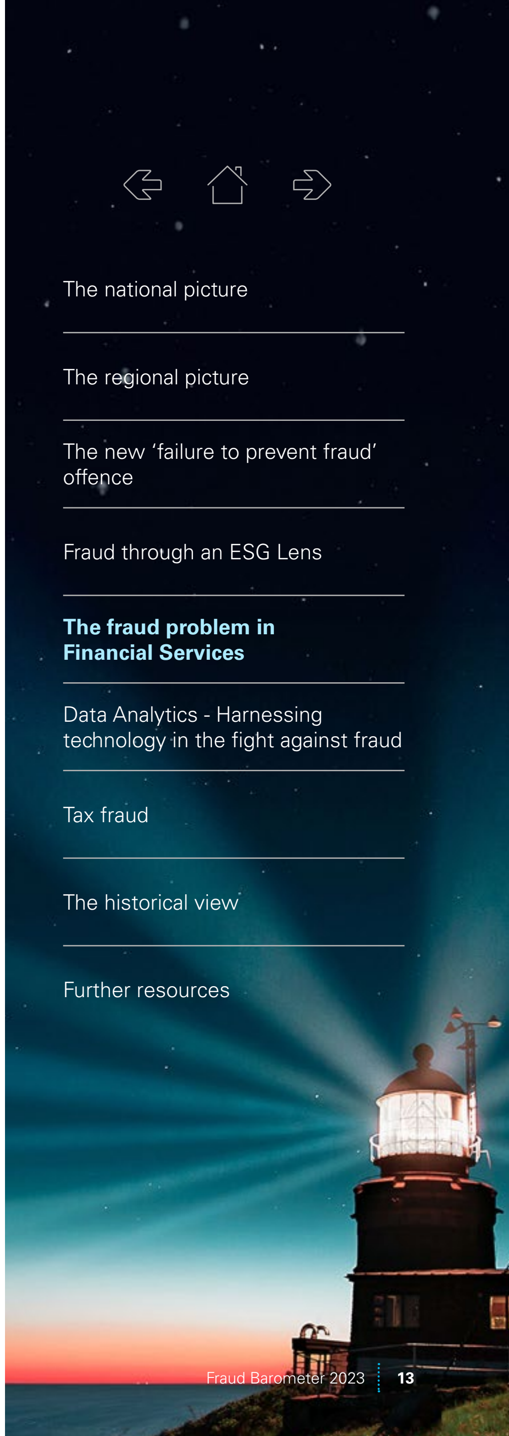
Authorised push payment (APP) fraud, whereby criminals trick their victims into sending money directly from their account to the criminals, has quickly become one of the most significant types of payment fraud, both in the UK and globally.

Despite an increase of 5 percent in the proportion of APP frauds that are refunded to victims by banks[6], consumer bodies and regulators in the UK remain dissatisfied with the ongoing losses experienced by customers.

New measures are now proposed by the Payment Systems Regulator (PSR) to fight payment scams with the objective of protecting customers from fraud by giving banks and other payment providers a stronger incentive to prevent scams. Banks will effectively be required to 'Prevent or Pay'. In addition, the new reimbursement requirements, which are due to be implemented in October 2024, are set to encourage banks to shift their focus beyond solely preventing customers from falling victim to scams and redirect attention towards identifying and addressing accounts within their books that receive the fraudulent payments. These accounts, known as 'money mules', sometimes unwittingly act as middlemen between the victim and fraudster.

The impact of these changes is likely to push financial institutions towards assessing their existing anti-fraud controls and response times to ensure the tougher new standards are able to be met. Furthermore, institutions will be incentivised to prevent or identify potential money mules on their books as early as possible to avoid the split responsibility of reimbursing victims. With these regulations on the horizon, it is even more important for institutions to have a balanced counter-fraud framework that both protects customers from fraud and implements stringent controls and processes to identify and prevent money mules and fraudulent actors internally.

4. https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023
5. https://www.ofcom.org.uk/__data/assets/pdf_file/0025/255409/online-scams-and-fraud-summary-report.pdf
6. https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023



KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Data Analytics - Harnessing technology in the fight against fraud

- Rupert Walter

Now, more than ever, fraud is big business. Through facilitating the global reach of fraudsters and adding a veil of legitimacy to their dubious schemes, technology is helping drive this boom.

However, technology is also leading the fightback, presenting opportunities for ever broader and deeper efforts to identify and combat fraud. Deployed sensibly, technological advances can offer a significant operational impact, both within and outside of the counter-fraud domain. As an example, 10% of CEOs considered that the ‘top benefit’ of investing in generative AI is improved fraud detection[7].

The use of ‘forensic analytics’ with technology aimed at identifying potential problem areas, whatever the cause, as opposed to the more narrow-focused ‘fraud detection analytics’, provides multiple use cases for the same investment. Given the rapid pace of change, organisations are increasingly looking to outsource forensic analytics entirely as a managed service that is cheaper and more effective than an in-house offering. Among the factors hindering the work of Chief Risk Officers, both the deficiencies of IT systems and data quality problems continue to stand out, followed by a lack of resources[8].

Some key considerations for 2024 are:

- **Establishing the fundamentals for success;**
- **The importance of constructive failure;**
- **Harnessing the power of generative AI; and**
- **Forensic analytics as a managed service.**

Establishing the forensic fundamentals for success

Planning

“Rubbish in, rubbish out” and “fail to plan, plan to fail” are two important mantras when deploying forensic analytics. In the face of competing budget demands, having a well-defined objective and a thorough understanding of the types of analytics available are essential for setting clear, measurable, and achievable targets.

These in turn can be used to demonstrate return on investment and the ‘value-add’. A considered approach also facilitates cross-functional working, supporting engagement with other teams and providing multiple use cases for the same infrastructure development.

Data quality

Analytics can only provide insights into the information that is available. If the data quality and required granularity aren’t available, then the resulting insight (or, rather, lack thereof) may be disappointing. KPMG’s Fraud Questionnaire found that more than 50% of respondents indicated that their organisations hadn’t properly assessed the fraud risks facing their business and potential impact[9].

Counter-fraud (as well as wider risk) analytics therefore starts at the risk management framework stage:

- What are the fraud risks I need technology to help mitigate?
- What data markers indicate behaviour of potential concern?
- Am I recording the right data points to look for these data markers?

Broader benefits of forensic approach

Fraud is one of the possible causes for anomalies in data analysis. However, control weaknesses and excess expenditure are other issues that can be identified by using a forensic approach. By way of example, overpayment for goods might simply be the result of poor planning rather than a concerted effort to defraud, but the underlying analytics to spot the discrepancy is the same, as is the overall cash-draining impact on the business.

7. https://kpmg.com/xx/en/home/insights/2023/09/kpmg-global-ceo-outlook-survey.html
8. https://kpmg.com/us/en/articles/2023/2023-cro-survey.html
9. https://kpmgfraudriskquestionnaire.com/

KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

For this reason, ‘forensic’ analytics (as opposed to ‘fraud’ analytics) has a much wider application across the organisation rather than solely fraud detection. Shaping the analytics efforts with this in mind establishes a greatly enhanced return on investment, offering longevity as well as capabilities to other parts of the business. For example, the same analytics setup that supports expenses monitoring driven by machine learning can also underpin AI-enabled contract compliance management.

The importance of constructive failure

Fraudsters are experts at the dark art of subterfuge, dressing up illegitimate transactions to appear almost identical to legitimate dealings. In many cases, the way to spot the difference is by relying on the context of the transaction - does the transaction make sense as part of that bigger picture?

Our extensive experience suggests that the primary reason for the failure in analytics, be it an overabundance of false positives or even an inability to identify the necessary data markers, is the lack of necessary data to provide that essential context.

Educating the business with the knowledge of what is missing and why it is important can drive the necessary change in business behaviours and systems usage. It provides the information required by those in positions of governance to be able to determine to what extent the lack of data maturity inhibits the deployment of effective analytics and whether that is an acceptable risk.

Harnessing the power of generative AI

Whether you have engaged with AI services or not, change is coming. Though there are still flaws in Large Language Models (LLMs) and the associated technology, hallucinations (where the model generates text that is incorrect, nonsensical, or not real) being a prime example, the potential power of the technology is immense.

From a Forensic standpoint, generative AI is changing the way we mine both structured and unstructured data for proactive monitoring as well as investigations. We already use it to provide an additional layer of insight, and where supported by normal processes, it is an effective enabler, especially as an early case assessment tool for investigations.

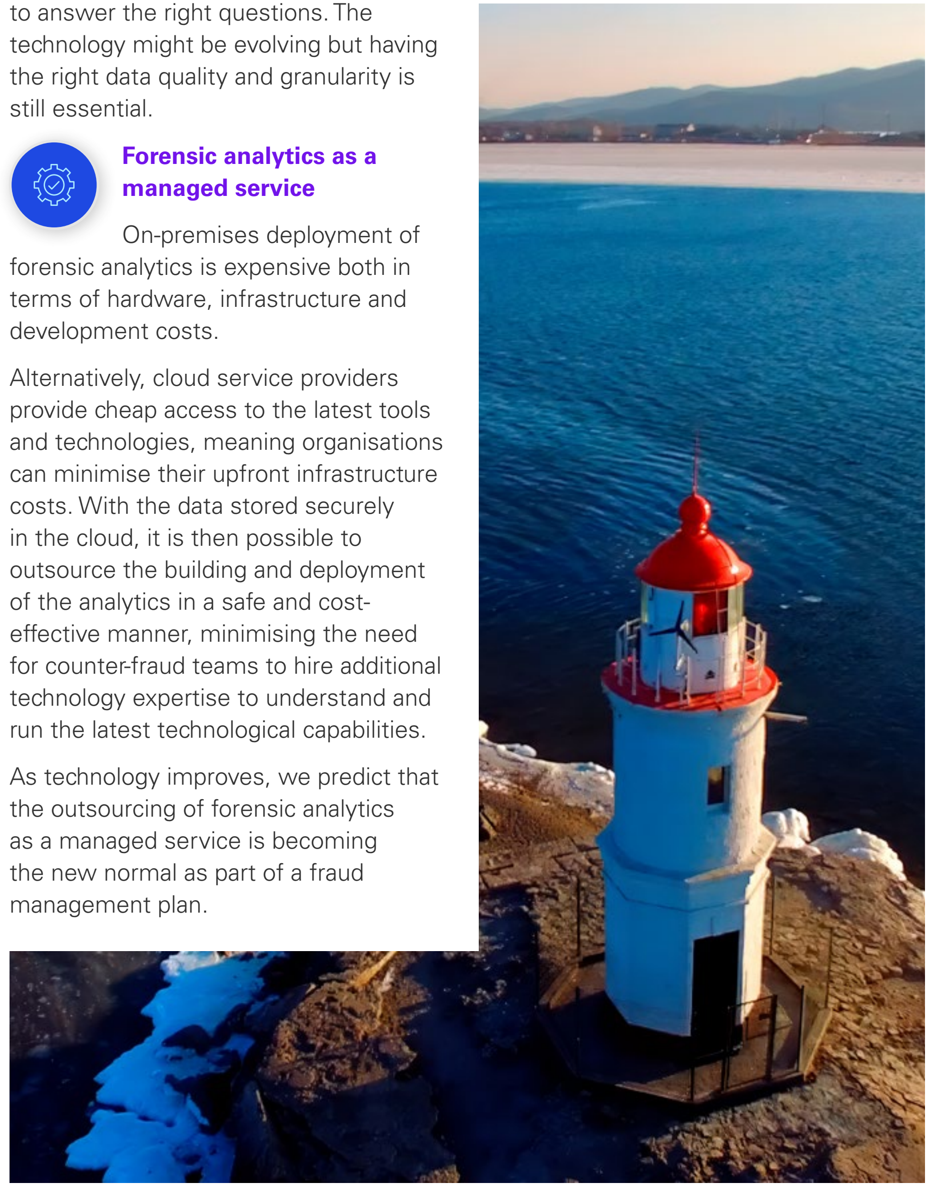
Sensible early adoption of the new technology will allow counter-fraud teams (and others) to gain an understanding of how best to marshal this emerging technology. With this understanding, the business can ensure that it is tracking the right data points to answer the right questions. The technology might be evolving but having the right data quality and granularity is still essential.

Forensic analytics as a managed service

On-premises deployment of forensic analytics is expensive both in terms of hardware, infrastructure and development costs.

Alternatively, cloud service providers provide cheap access to the latest tools and technologies, meaning organisations can minimise their upfront infrastructure costs. With the data stored securely in the cloud, it is then possible to outsource the building and deployment of the analytics in a safe and cost-effective manner, minimising the need for counter-fraud teams to hire additional technology expertise to understand and run the latest technological capabilities.

As technology improves, we predict that the outsourcing of forensic analytics as a managed service is becoming the new normal as part of a fraud management plan.



© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Tax fraud

- James Gorin and Jill Hodson

Tax fraud, including tax evasion, evasion of duty, tax refunds and VAT fraud, is consistently one of the most common fraud types observed within the Fraud Barometer dataset. In 2023, Tax fraud was one of the most common fraud types with a combined value of £542.3 million across 22 cases, a significant increase in value from 2022 in which there were 25 cases of tax fraud with a combined value of £16.1 million. This significant increase was largely driven by a single tax fraud (failure to declare assets) case with a value of £416 million.

There was also a significant increase in reported VAT fraud cases of £100k and above that were heard in the UK's Crown Courts in 2023. VAT fraud increased from £6.2 million in 2022 to £105.1 million in 2023, despite the volume of cases decreasing by one (there were 10 cases of VAT fraud in 2023, down from 11 cases in 2022).

Although the volume of VAT fraud cases has decreased slightly during the year, the value of frauds committed are on average significantly higher, and therefore it is increasingly important for businesses to establish strong controls to mitigate the risk of tax fraud and associated losses.

HMRC – Investigation of tax fraud

HMRC operate a selective prosecution policy with respect to tax fraud, meaning criminal investigations are reserved for cases where HMRC need to send a strong deterrent message, or where the conduct involved is such that only a criminal sanction is appropriate. Where a criminal investigation is not undertaken, HMRC instead undertake tax fraud investigations through its civil fraud investigation procedure under Code of Practice 9 ("COP9"). COP9 investigations are only conducted through HMRC's specialist Fraud Investigation Service directorate.

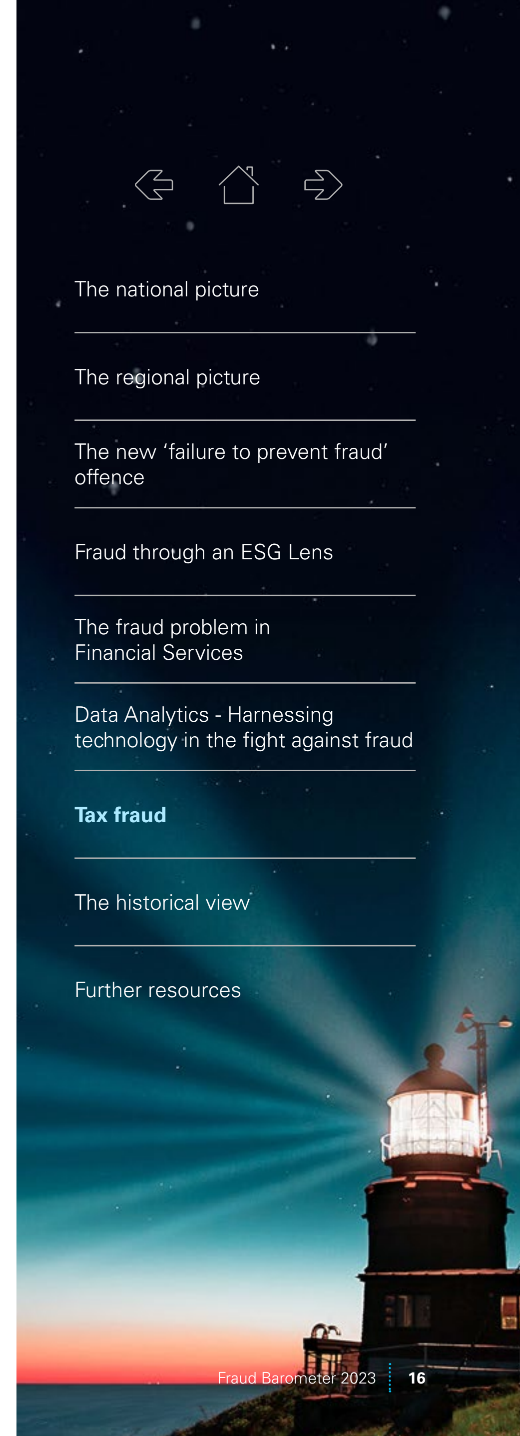
Under the civil fraud investigation procedure, the recipient of COP9 is given the opportunity to make a disclosure of all their deliberate behaviour (tax fraud) that brings about a loss of any form of tax or duty. In return for making a full disclosure of any tax fraud committed, HMRC agrees not to undertake a criminal investigation into those frauds.

This disclosure process is performed via the Contractual Disclosure Facility ("CDF"), through which a two-stage disclosure is made to HMRC, the first of which requires the submission of an Outline Disclosure of the frauds committed within 60 days of HMRC issuing a COP9 notice. The process concludes through a financial settlement, including tax, late payment intertest and penalties typically between 35 and 100 percent of the tax due, depending on various matters such as the degree of cooperation with the disclosure and investigation process.

HMRC opened a total of 361 investigations in the year to 5 April 2023, through its civil fraud investigation procedure. 592 investigations were closed for a total yield (tax, interest, and penalties) of £147.3 million.

HMRC can still undertake a criminal investigation into any fraud that is not disclosed to them or if an individual denies committing fraud when issued with COP9. A failure to respond to COP9 is treated as a denial. At the end of the process, an individual is required to sign a Certificate of Full Disclosure and a Statement of (worldwide) Assets and Liabilities. These documents contain a warning that HMRC can seek a prosecution if the documents contain any material errors or omissions.

VAT fraud was also within the top three fraud types by value in 2023, with a combined value of £105.1 million across 10 cases.



KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Recent examples of recipients of COP9 who failed to fully comply with the process or who made material omissions in their disclosure and were subsequently moved to a criminal investigation include:

Tax fraud – failure to declare assets

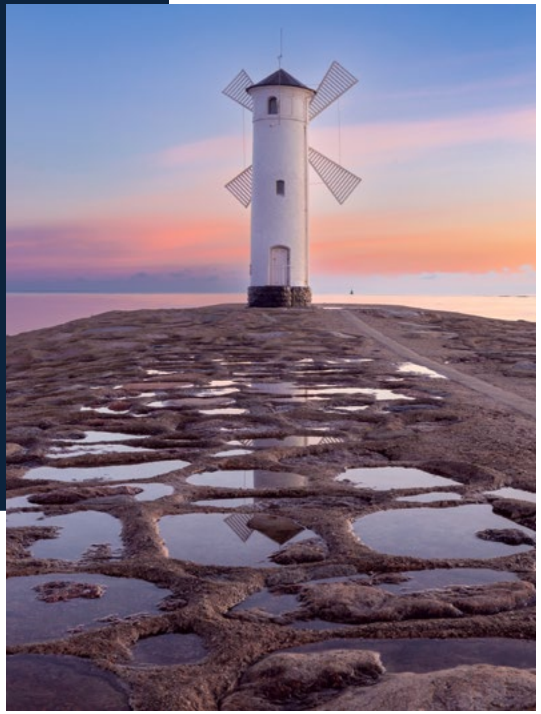
A billionaire former F1 motor racing boss was prosecuted in October 2023 following a lengthy tax fraud investigation conducted by HMRC under COP9. He was offered the opportunity to make a full, open, and honest disclosure through the CDF process. However, during the investigation it was found that the individual misrepresented his connection with an offshore trust.

He later admitted a single charge of fraud by false representation during a hearing at Southwark Crown Court on 12 October 2023. The £416 million fraud is the key driver for the increased value of tax fraud (failure to declare assets) observed within the 2023 Fraud Barometer data.

VAT returns fraud

A tiling business owner in Northampton submitted fraudulent VAT returns with inflated payments for materials, which generated repayments which he kept. He ignored HMRC's attempts at contacting him through correspondence, including the offer of making a disclosure through the COP9 CDF process. The individual contacted HMRC three months after the offer period expired, by which time the case had been transferred for criminal investigation.

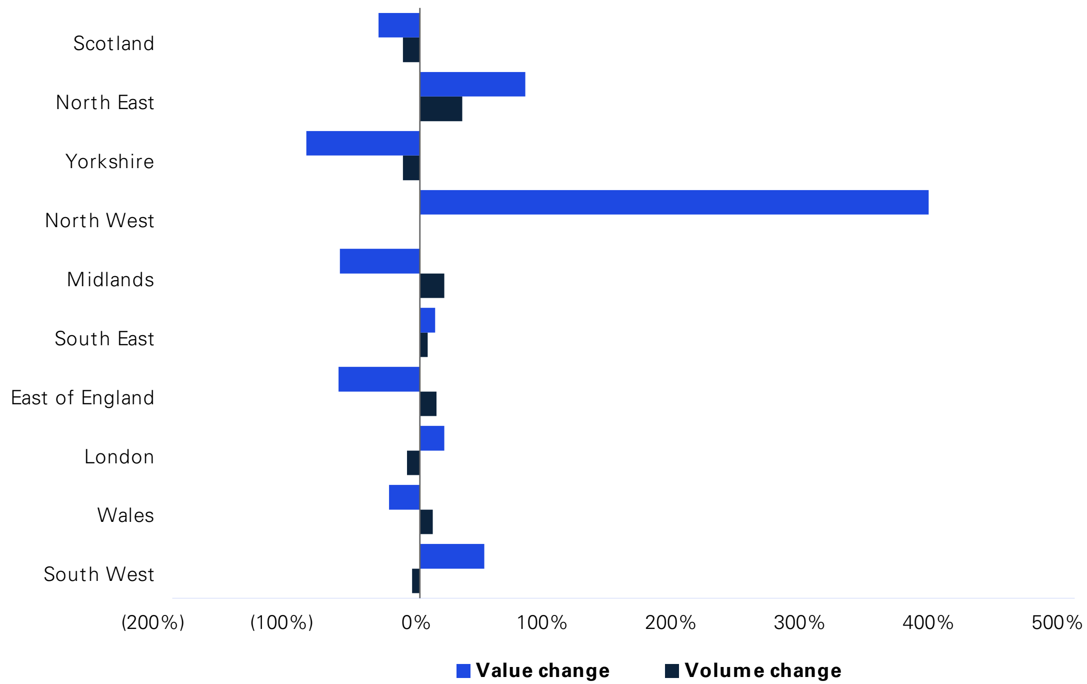
He admitted five counts of tax fraud totalling £492k in Northampton Crown Court in June 2022 and was sentenced to two years in prison, suspended for two years.



© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

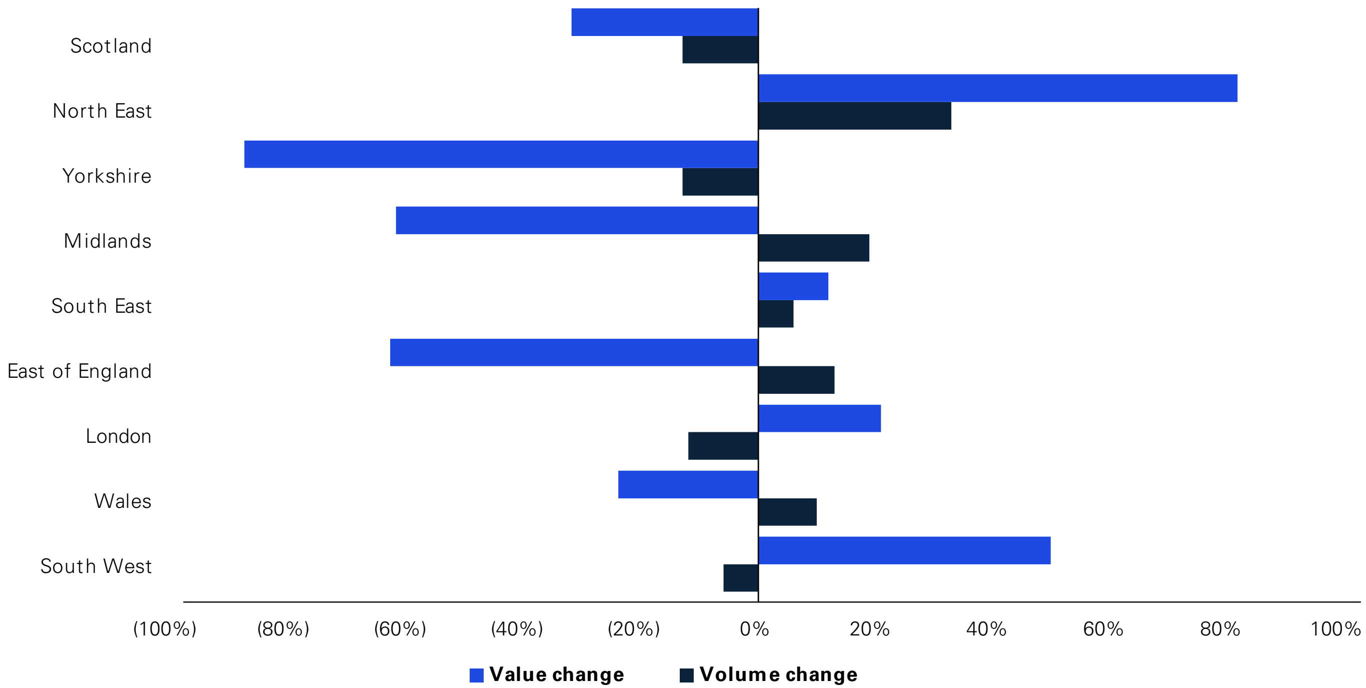
The historical view

Change in volume and value of cases by geographic region (2023 versus 2022)



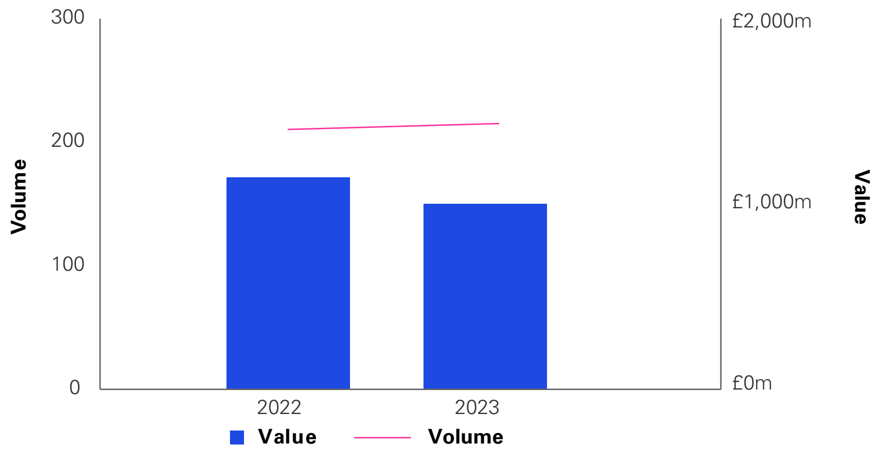
© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Change in volume and value of cases by geographic region, excluding North West (2023 versus 2022)

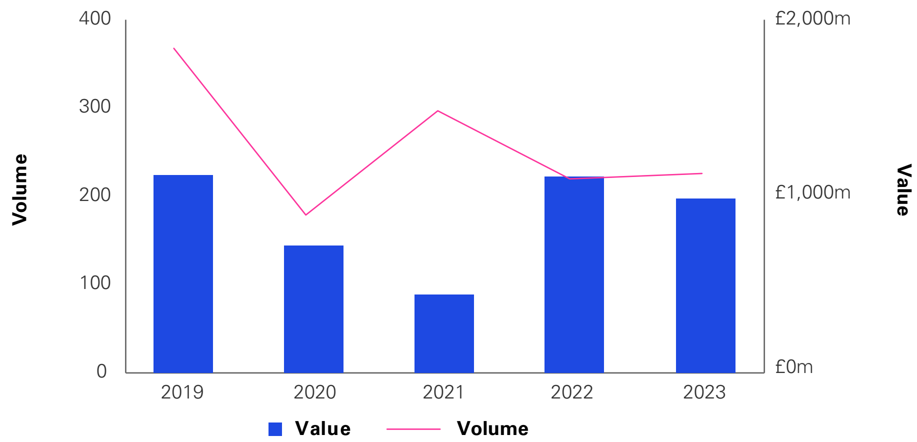


© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

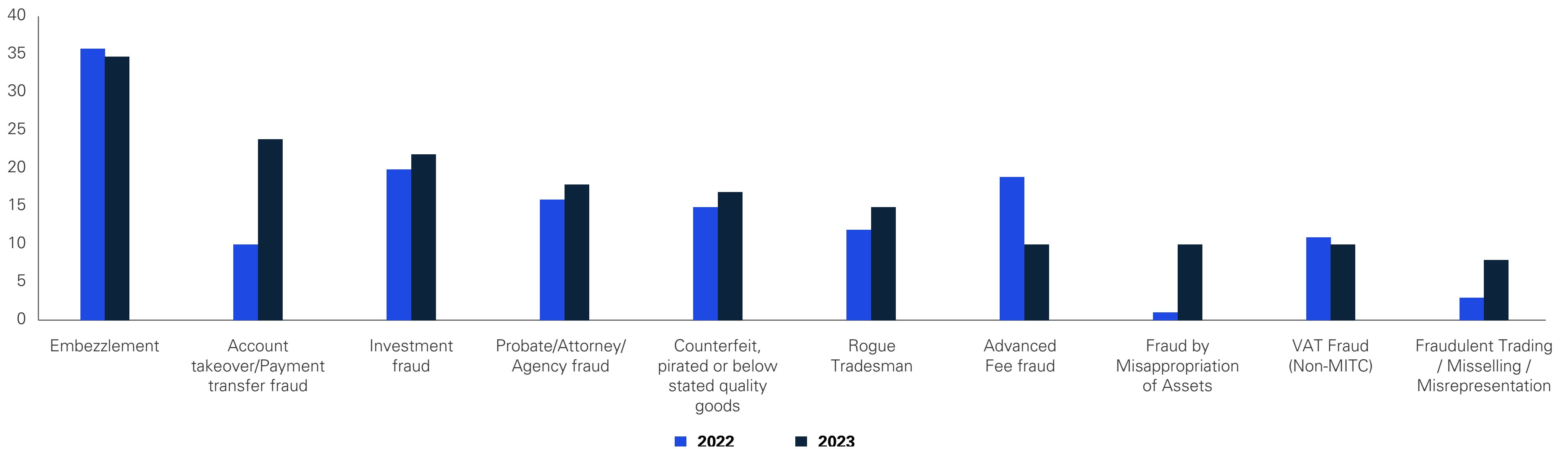
Change in total volume and value of cases recorded (2023 versus 2022)



Change in total volume and value of cases recorded over the last five years



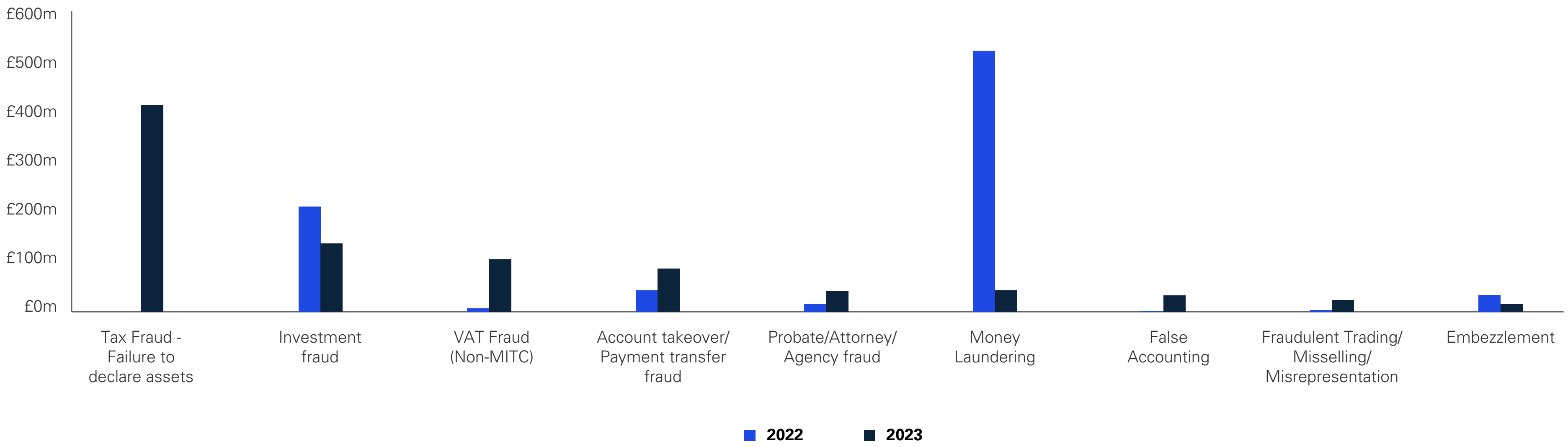
Top frauds by case volumes in 2023, with prior years comparison

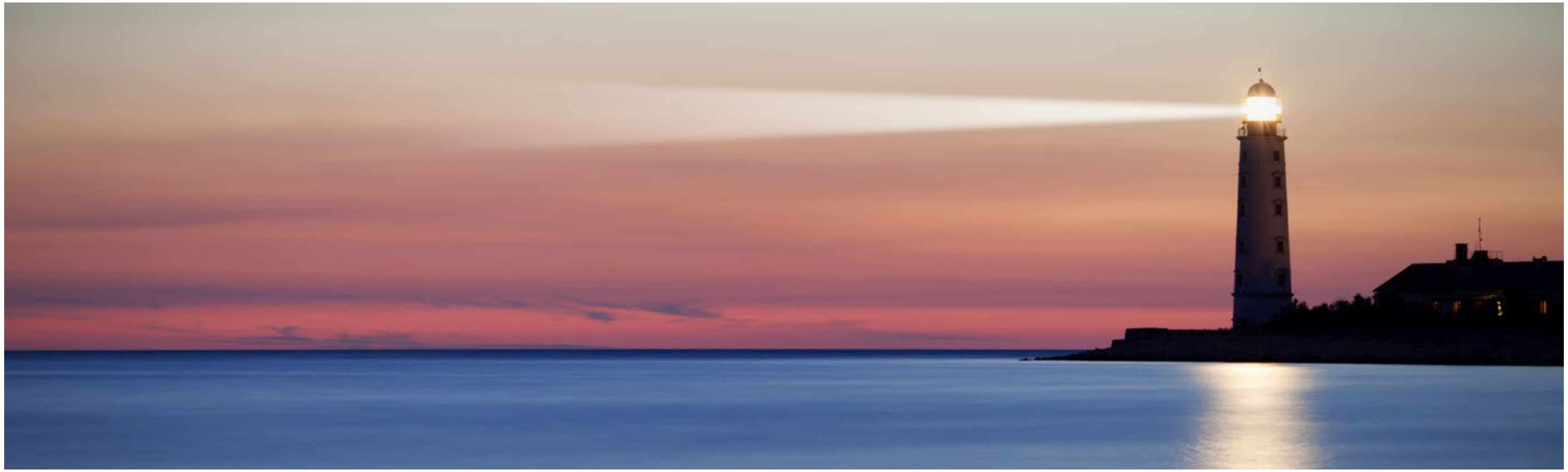


KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Top frauds by case values in 2023, with prior years comparison

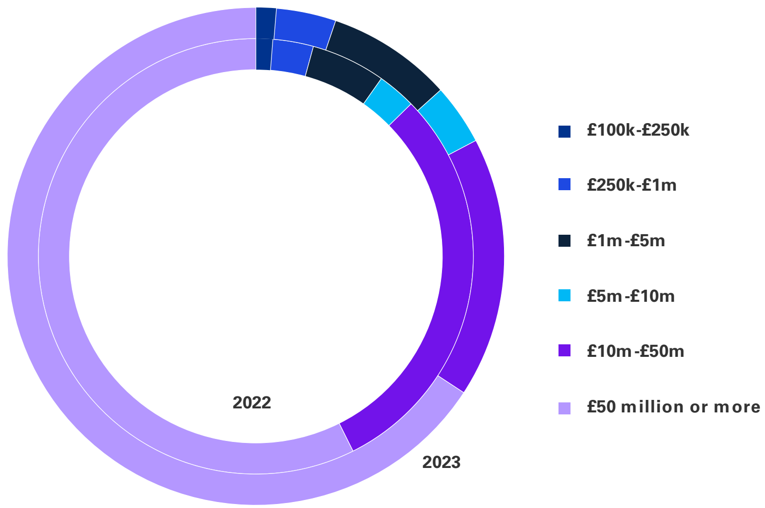




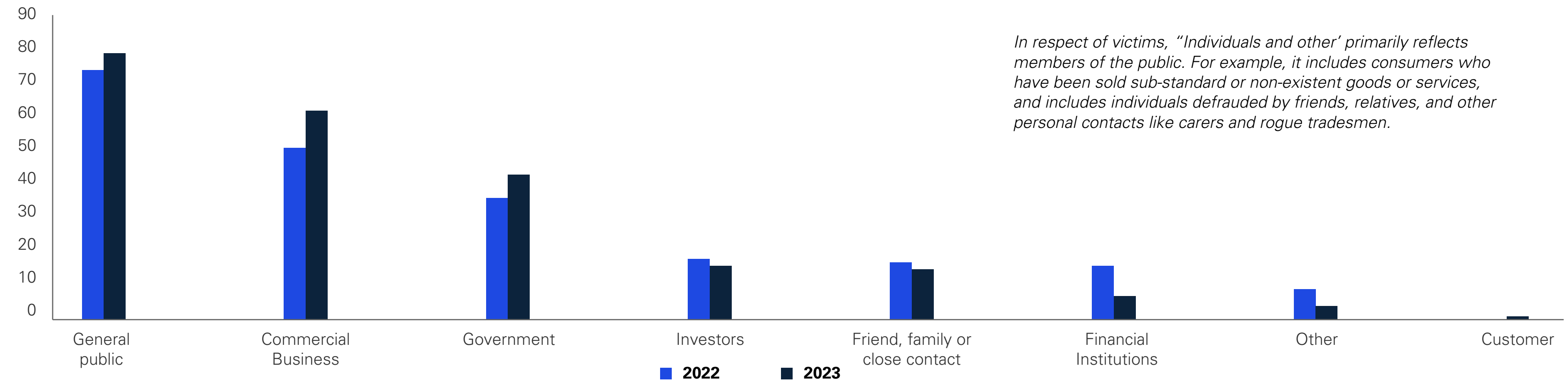
KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Proportion of values in Fraud Barometer, by case value range



Fraud volumes by victim, 2022-2023



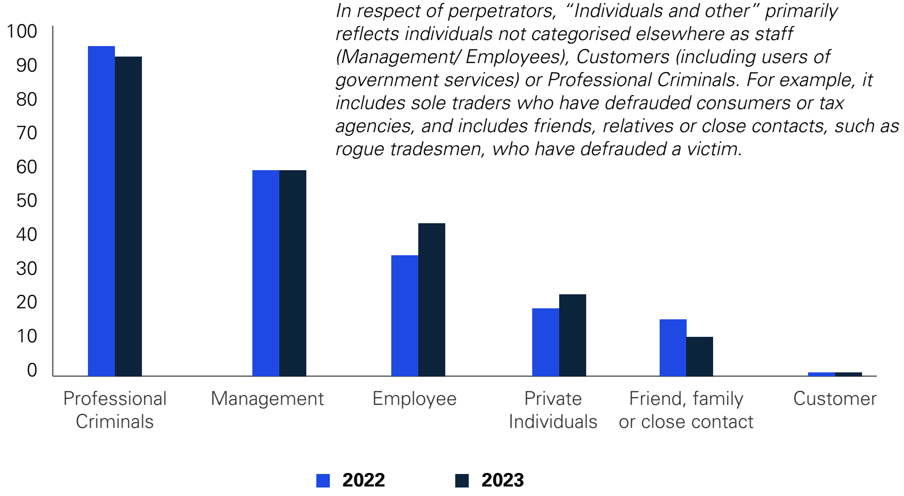
In respect of victims, "Individuals and other' primarily reflects members of the public. For example, it includes consumers who have been sold sub-standard or non-existent goods or services, and includes individuals defrauded by friends, relatives, and other personal contacts like carers and rogue tradesmen.

KPMG

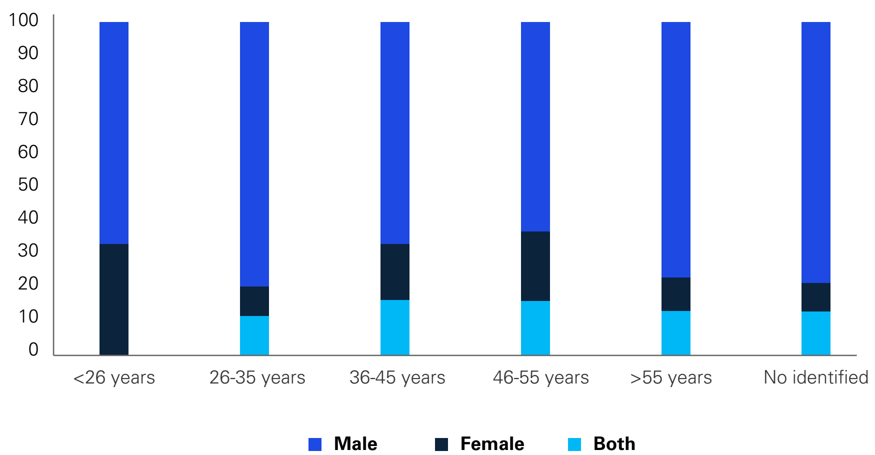
© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Fraud volumes by perpetrator, 2022-2023

In respect of perpetrators, "Individuals and other" primarily reflects individuals not categorised elsewhere as staff (Management/ Employees), Customers (including users of government services) or Professional Criminals. For example, it includes sole traders who have defrauded consumers or tax agencies, and includes friends, relatives or close contacts, such as rogue tradesmen, who have defrauded a victim.



Frauds in 2023 by perpetrator age, analysed by gender (volume of cases)



KPMG

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Further resources

Please see our website for regular updates and articles from our experts on financial crime developments and fraud risk management. KPMG has been leading the way in terms of helping organisations to improve internal controls that also address fraud

Please contact us should you want to find out how we can help you improve your internal control framework.

The KPMG Fraud Barometer National team

Roy Waligora

Head of Investigations and Fraud Barometer Lead Partner
KPMG Forensic
roy.waligora@kpmg.co.uk
+44 (0) 746 490 2991

Matthew Croad

Senior Manager
KPMG Forensic
matthew.croad@kpmg.co.uk
+44 (0) 774 745 6380

Cuthbert Chiduku

Manager
KPMG Forensic
cuthbert.chiduku@kpmg.co.uk
+44 (0) 775 937 1598

Sophia Devaney

Manager
KPMG Forensic
sophia.devaney@kpmg.co.uk
+44 (0) 791 837 5864

Phoebe Calloway

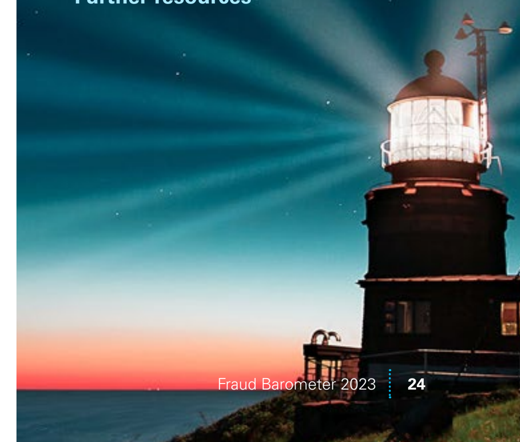
Assitant Manager
KPMG Forensic
phoebe.calloway@kpmg.co.uk
+44 (0) 755 414 5892

Rishiharan Ragulan

Apprentice
KPMG Forensic
rishiharan.ragulan@kpmg.co.uk
+44 (0) 777 829 9919

Chloe Tomlinson

Graduate
KPMG Forensic
chloe.tomlinson@kpmg.co.uk
+44 (0) 795 531 2810



© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.com/uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Public

CREATE: CRT152958A | Febraury 2024