KPMG

# Fraud Barometer 2024

## A snapshot of fraud in the UK

May 2025

–

kpmg.com/uk

# Welcome

**This year's survey reveals a mixed message — whilst national fraud statistics show persistently high volumes and values of fraud, the value of high value fraud cases in UK courts was sharply down in 2024 at £453.2 million, compared to the prior year of £992million.**

I am delighted to publish KPMG's latest Fraud Barometer, one of the longest running surveys of its kind in the UK, where we track fraud cases reported in the media over £100k.

Fraud remains a pervasive problem in the UK, and the current mood seems bleak - low economic growth, geopolitical uncertainty and an ongoing cost of living crisis, drives concern that the fight against fraud faces even more competition for scarce resources to make meaningful headway. Whilst this outlook is challenging, we examine how new regulations and technologies offer some optimism in the fight against fraud.

We take a closer look at the national and regional picture and we have collated relevant and up to date insights from our Forensic specialists on hot topics including:

- Developments in Payments Fraud and the forces behind tackling it;
- A look at AI being used by fraudsters and how it is used for fraud detection;
- An update on the Economic Crime and Corporate Transparency Act and all you need to know about the failure to prevent fraud offence ahead the effective date of 1 September 2025;
- Why Government remains a significant victim of fraud; and
- Effective whistleblowing in an evolving regulatory landscape.

I trust you will find this year's report helpful 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 feel free to contact us.

**Roy Waligora,**
Partner and Head of UK Investigations, Forensic

The KPMG Fraud Barometer team is headed up nationally by Roy Waligora (based in London).

The following KPMG professionals contributed articles to this edition of the Fraud Barometer:

**Annette Barker**
Partner, Forensic

**Ignatius Adjei**
Partner, Forensic

**Damien Margetson**
Director, Forensic

**Richard Haynes**
Director, Forensic

**Rupert Walter**
Director, Forensic

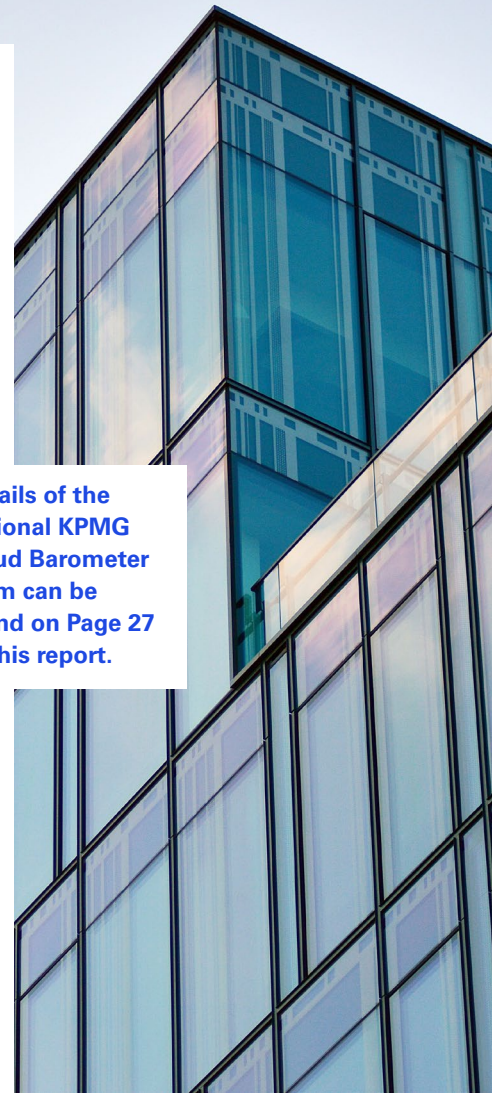
**Michael Wong**
Director, Forensic

**Annabel Hewitt**
Senior Manager, Forensic

**Wing Tung Lee**
Manager, Forensic

**Benjamin Cowley**
Manager, Forensic

**Details of the national KPMG Fraud Barometer team can be found on Page 27 of this report.**



The national picture
The regional picture
What are the key forces shaping the fight against payment fraud?
Fraud in the era of AI
The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?
An overview to whistleblowing
The battle against Government fraud
The historical view
Further resources

# Contents


01 The national picture

02 The regional picture

03 What are the key forces shaping the fight against payment fraud?

04 Fraud in the era of AI

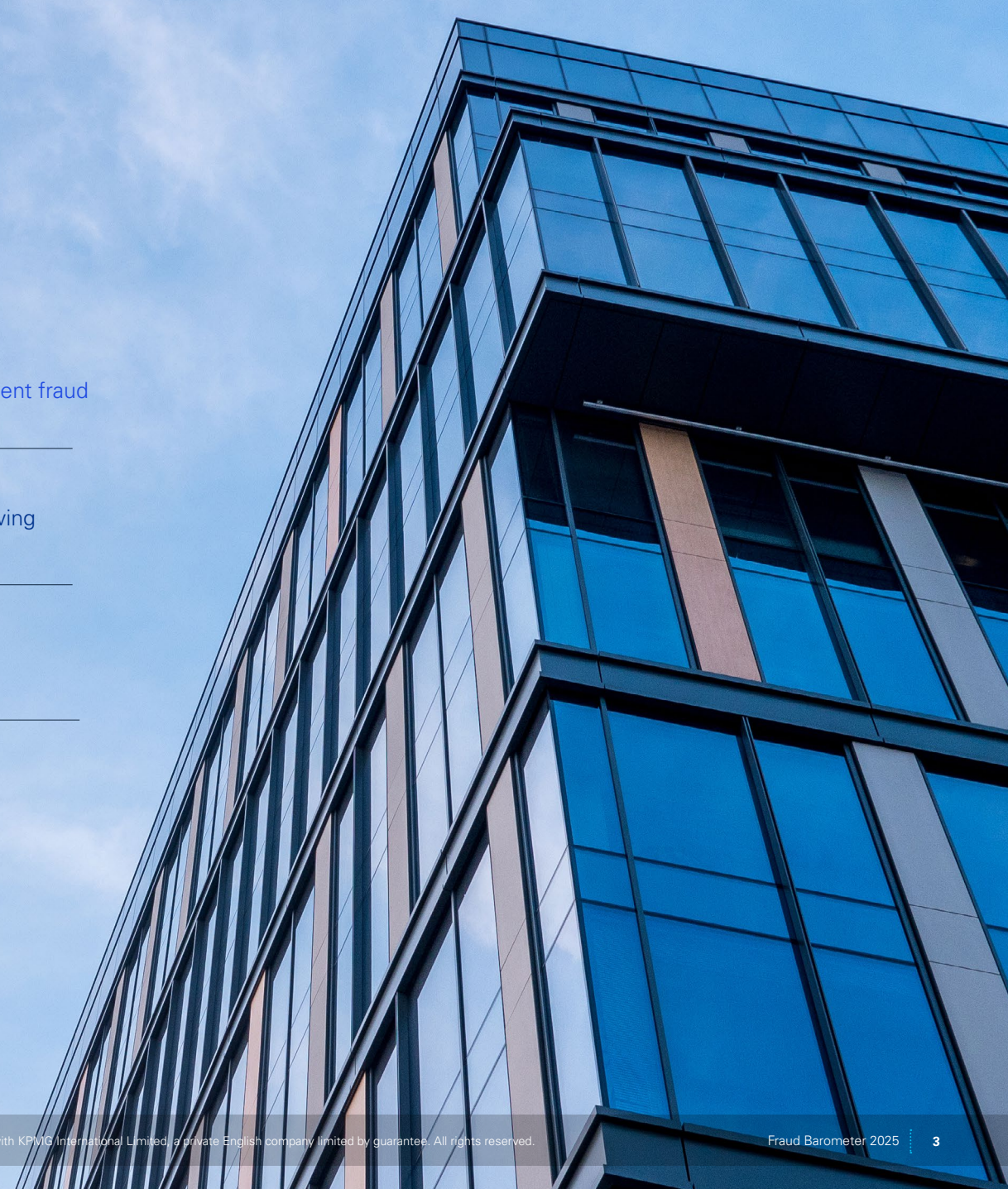
05 The Government guidance for the ‘failure to prevent fraud’ offence is now here – what are the 5 key things you need to know?

06 The battle against government fraud

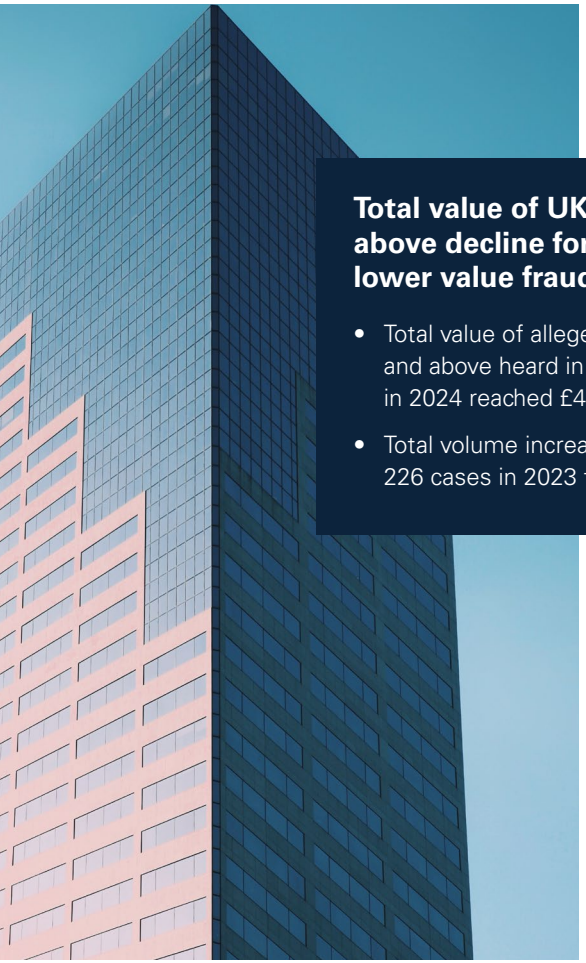
07 An overview to whistleblowing

08 The historical view

09 Further resources

# The national picture



**Roy Waligora,**
Partner and Head of UK Investigations, Forensic

**Total value of UK frauds worth £100k and above decline for the second year, whilst lower value fraud rises.**

- Total value of alleged fraud cases of £100k and above heard in the UK Crown Courts in 2024 reached £453.2 million.
- Total volume increased marginally from 226 cases in 2023 to 236 cases in 2024.

Figures released from KPMG UK's 2024 Fraud Barometer, which records alleged fraud cases with a value of £100k and above, revealed that the total value of fraud cases being heard in UK Crown Courts has declined for the second year in a row. Total fraud value decreased by 54% from £992.9 million in 2023 to £453.2 million in 2024. This decrease is partly driven by a single super case in 2023 with a value of £416 million.

Excluding this high value case, total value of alleged frauds heard in UK Crown Courts decreased by 21% in 2024.

By contrast, the total volume of fraud cases heard in UK Crown Courts has increased slightly from 226 cases in 2023 to 236 cases in 2024, an increase of 4%.

Whilst the number of high value fraud cases heard in UK Crown Courts has decreased, reports of fraud to the National Fraud Intelligence Bureau have remained high. Data published by the National Fraud Intelligence Bureau indicates that during 2024 over 318k reports of alleged fraud were made to Action Fraud with a total reported loss value of £2.3 billion.[1] This represents a decrease in the number of fraud reports but an increase in the total reported loss value compared to 2023, when there were over 326k reports totaling £2.1 billion in alleged losses. This movement suggests that whilst fewer fraud incidents were reported to Action Fraud in 2024, the incidents that were reported during 2024 had, on average, larger losses associated with them than the incidents reported in 2023.

The Office for National Statistics estimates that there were 3.9 million fraud incidents in England and Wales between 1 October 2023 and 30 September 2024, a 19% increase compared to the year ended 30 September 2023.[2]

A further contributing factor for the fall in high values frauds in 2024 is the increasing backlog of cases waiting to be heard in the Crown Courts, which reached a "series peak" of over 73k cases as of September 2024.[3]

1. NFIB Fraud and Cyber Crime Dashboard, which is based on a data from Action Fraud
2. Office for National Statistics, Crime in England and Wales: year ending September 2024
3. Ministry of Justice Criminal court statistics quarterly: July to September 2024


**The national picture**
The regional picture
What are the key forces shaping the fight against payment fraud?
Fraud in the era of AI
The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?
An overview to whistleblowing
The battle against Government fraud
The historical view
Further resources

**The fall in value of fraud cases heard during 2024 does not mean that fraud in the UK was any less prevalent. By contrast, the increase in volume of cases may suggest that lower value fraud, which may take longer to detect and report, is on the rise.**

**The Fraud Barometer only looks at reported cases heard in UK courts with a value of £100k or above, so the likelihood is that there are many more frauds below £100k that are not captured within this report. According to information published by the National Fraud Intelligence Bureau and the Office for National Statistics, the number of reported fraud cases is rising, indicating that fraud remains a significant concern in the UK.**

### Professional criminals continue to target the Government and general public

As with the prior year Fraud Barometer, the government continues to be the most significant victim of fraud by value 2024, with total alleged frauds worth £236.1 million across 56 cases, compared with total frauds of £592.7 million across 43 cases in 2023, including the £416 million high value case. Excluding the super case, volume of fraud perpetrated against Government increased by 34%.

By volume, as with previous years, the general public continues to be taken advantage of most frequently by fraudsters; in 2024 there were 79 cases of alleged fraud committed against members of the public with a total value of £50.4 million. In 2023 there were 78 cases totalling £58.3 million committed against the general public.

Professional criminals continued to be the most active perpetrators of fraud by volume and were responsible for nearly half of fraud cases observed (113 out of the 236 fraud cases). In 2024 professional criminals were also the highest perpetrator by value, responsible for £372.9 million across these 113 cases. This is an increase of 23% compared with prior year fraud values (£302.2 million).

**Fraud against the Government and general public remains a persistent issue. Opportunist fraudsters are increasingly targeting members of the public through various schemes, such as selling counterfeit or below-quality goods, advanced fee frauds, and social engineering. The public, and Government, must remain alert to the risk of fraud, particularly in light of developing technologies and the rise in deepfake frauds and use of Artificial Intelligence to commit fraud.**

### Organised crime drives surge in Benefit fraud

Benefit fraud increased significantly from £2.3 million across six cases in 2023, to £59.5 million across seven cases in 2024, an increase of 2462%. This was primarily driven by a £53 million income support fraud case involving an organised crime group who were found guilty of submitting fraudulent claims for Universal Credit over several years.

**While it is an aim of His Majesty's Government to provide benefits and financial aid to eligible individuals in need of support, the temptation to misuse benefit schemes can be too much for some. Accordingly, the Government should seek to ensure there are appropriate safeguards and controls in place to protect against high levels of Benefit fraud, which the Fraud Barometer data suggests increased in 2024.**

### Wheels of justice are in motion as COVID-19 related prosecutions increase

The courts continued to tackle legacy COVID-19 related frauds in 2024, including cases of individuals fraudulently claiming COVID-19 related grants, furlough payments and bounce-back loans. Government Grant fraud increased significantly by 3138%, from one £434k case in 2023, to nine cases with a combined value of £14.1 million in 2024.


**The national picture**

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government fraud

The historical view

Further resources

**Whilst the aggregate value of fraud is down in this Fraud Barometer, geopolitical tensions including tariffs are putting pressure on cost and supply chains, which will no doubt drive future cases of fraud. Managing risk in the supply chain and focusing on third party risk management in these uncertain times will be a key process and control that companies can use to prevent loss.**

## Other key findings

- Of the 236 cases heard in 2024, 69% of perpetrators were male and 28% were aged 36-45 years old.
- Cases of insider fraud committed by managers and employees remained significant, accounting for 34% of total cases (46 cases were committed by management and 35 cases by employees respectively).
- As with previous years, the London and South East region continues to have the largest volumes and value of fraud, accounting for 31% of total fraud volumes and 72% of total fraud value for 2024.
- All six EU / Government Grant fraud cases heard in UK Crown Courts in 2024 related to falsification or inappropriate claims for COVID-19 related financial support, as the courts continue to tackle legacy COVID-19 fraud cases.
- Cases of money laundering increased from six cases with a combined total of £44.2 million in 2023, to nine cases totalling £128.2 million in 2024. This is largely driven by a £104 million super case involving a pair of professional criminals who were found guilty for their involvement in smuggling over £100 million cash from the UK to the UAE over a period of 11 months.[4]

4. Each of the cases classified as money laundering had a fraud component as the predicate offence, which is why they have been included within the Fraud Barometer data.


**The national picture**

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government fraud

The historical view

Further resources

# The regional picture

**Annette Barker,**
Partner, Forensic

**The Fraud Barometer indicates that the London and South East region contributed the biggest proportion of fraud across the UK during 2024.**

- As with previous years, the London and South East region had the highest volume and value of alleged fraud cases reaching UK Crown Courts in 2024.
- 74 out of 236 cases were in the London and South East region with a combined value of £325.1 million.
- The Midlands had the second highest value and volume of alleged fraud cases heard in the Crown Courts during 2024, with £49.6 million across 39 cases.

Figures published from KPMG UK's 2024 Fraud Barometer, which records alleged fraud cases with a value of £100k and above, showed that the London and South East region saw the biggest fraud values heard in UK Crown Courts throughout 2024, with a total value of £325.1 million. Although this was a decrease compared with the prior year fraud value (£725.8 million), the decrease was largely driven by a single super case in 2023 with a value of £416 million. Excluding this case, fraud within the London and South East region increased by £15.3 million (5%). Fraud volume in the region increased from 62 to 74 cases, indicating lower value frauds are becoming more common.

Across the UK, the Midlands region had the second highest value and volume of fraud cases during 2024, totaling £49.6 million over 39 cases.

The national picture is that the total volume of fraud cases heard in UK Crown Courts has increased by 4% from 226 cases in 2023 to 236 cases in 2024. By contrast, total value has decreased from £992.6 million in 2023 to £453.2 million in 2024. With fraud continuing to rise, today's figures suggest lower value fraud is on the rise.


The national picture

**The regional picture**

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government Fraud

The historical view

Further resources

**Whilst the decrease in total value of fraud cases above £100k offers some reassurance, London continues to be the UK's fraud hotspot. Given that London is a major financial hub, it is understandable why the capital continues to have the highest volume and value of fraud. However, the figures reported today for the Midlands region show that nowhere is safe from fraudsters who do not let geographical boundaries constrict their activity.**

## Government, commercial businesses and the General Public continue to be impacted most by fraudsters

By value, the Government was the biggest victim of fraud with combined fraud losses of £236.1 million in 2024 across 56 cases, compared with 43cases totalling £592.7 million in 2023. Of the frauds reported during 2024, £195.1 million relates to the London and South East region (83% total Government fraud value), across 23 cases.

This is largely driven by two high value cases heard in the London and South East region with a value of £104 million and £53 million respectively.

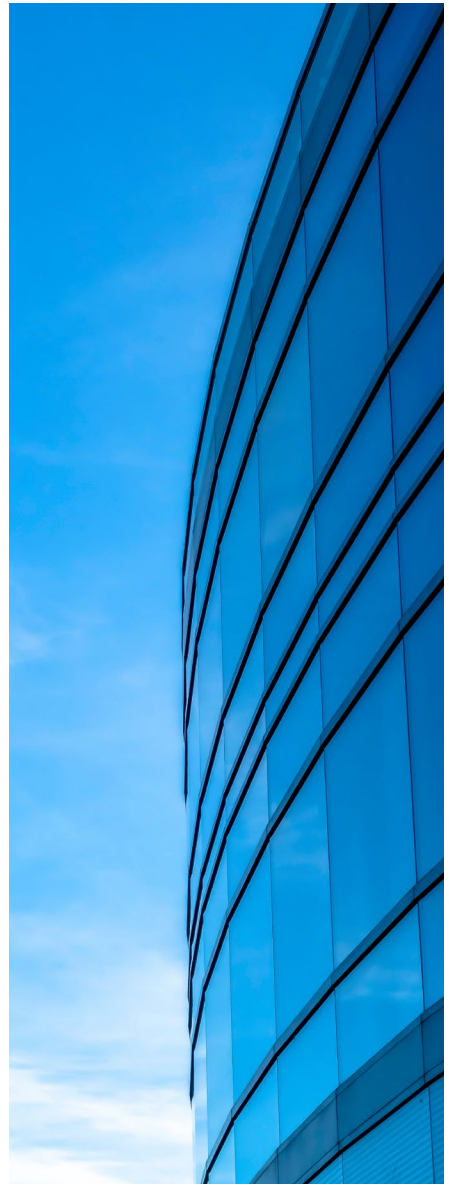
By volume, the general public continues to be taken advantage of most frequently by perpetrators of fraud. In 2024 there were 79 cases of alleged fraud against members of the general public, for a total value of £50.4 million, compared with 78 in 2023 totalling £58.3 million. As with the prior year, London and the South East continues to see higher levels of fraud heard in the Courts, with 19 cases heard in 2024 worth £10.4 million. The South West and Wales region had the second highest volume with 17 cases totalling just under £14 million in 2024.

**Hopefully the reduction in the value of fraud cases being heard in the Courts, which relate to the Government and the general public, is an indication of a corresponding reduction in the value of fraud cases committed. However, the data suggests that lower value fraud is on the rise as fraud volumes have increased. The Government and members of the general public should therefore remain vigilant and be alert to the danger fraudsters pose.**

## Cases involving the East of England declines significantly

Fraud cases heard in courts in the East of England region decreased significantly by both value and volume, from nine cases within a combined value of £11.8 million in 2023, to three cases with a combined value of £701k in 2024. The three cases heard in 2024 related to a £151k Expenses and Payroll fraud; a £150k Probate / Attorney fraud where a relative fraudulently obtained control of the victim's finances; and a £400k Advanced fee fraud involving a scammer.

**There was a considerable fall in volume and value of fraud cases heard in the East of England during the year. Whilst it is important to remain vigilant and regularly review and update fraud defences, especially in light of the new failure to prevent fraud offence for all corporations, it is encouraging to see that steps have been taken to combat fraud.**




The national picture

**The regional picture**

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government Fraud

The historical view

Further resources

# What are the key forces shaping the fight against payment fraud?

- Ignatius Adjei and Wing Tung Lee

In the first half of 2024, the UK experienced £570 million in payment fraud losses,[5] a 1.5% decrease from the same period in 2023. While this signals a stabilisation in fraud levels, the losses remain substantial.

UK Finance has reported a rise in unauthorised fraud,[6] driven by increasingly sophisticated social engineering tactics that manipulate victims into unknowingly authenticating fraudulent transactions. In contrast, authorised fraud[7] has decreased, due to stricter monitoring, better customer education, and improved processes encouraging careful payment verification.

**KPMG's own Fraud Barometer data shows a decrease in total alleged losses due to payment transfer fraud from £83.7 million in 2023 to £11.2 million in 2024.**

Throughout 2024, payment fraud continued to evolve, with remote purchase fraud emerging as a major concern, driven by sophisticated social engineering tactics and the misuse of stolen credentials. Other fraud risks included account takeover through phishing and automated bots for credential stuffing and fake account creation.

In this article, we will explore how regulatory measures, operational shifts, and technological advancements are shaping and transforming the payment fraud landscape.

5. Over £570 million stolen by fraudsters in the first half of 2024 | Insights | UK Finance
6. Unauthorised fraud involves transactions made without the account holder's consent, often through methods like phishing, malware, or identity theft.
7. Authorised fraud, commonly known as APP fraud, occurs when individuals are deceived into willingly transferring money to fraudsters.


The national picture

The regional picture

**What are the key forces shaping the fight against payment fraud?**

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government fraud

The historical view

Further resources

## Evolving regulatory environment

The regulatory landscape continues to evolve to address emerging fraud risks. The introduction of Strong Customer Authentication[8] by the Financial Conduct Authority between 2019 and 2022 initially led to a decline in unauthorized remote purchase fraud. However, recent trends show a resurgence as fraudsters find ways to bypass the authentication controls, highlighting the need for stronger fraud detection systems, continuous monitoring and more robust authentication protocols.

Meanwhile, the Mandatory Scam Reimbursement requirement was introduced to address Authorised Push Payment ('APP') fraud in 2024.[9] This regulation mandates that financial institutions reimburse victims up to £85k per fraud incident, building on protections initially set out in the voluntary Contingent Reimbursement Model ('CRM') Code.

Although it is too early to gauge the full impact, some banks report a shift toward unauthorised fraud, including a rise in card fraud. At the same time, concerns are mounting over first-party fraud, as individuals increasingly exploit reimbursement rules – a trend that could intensify as fraudsters adapt and awareness of these protections grows.

## Operational and technological improvements

Financial institutions are adapting their operating models in response to the ever-evolving fraud landscape. Fraud prevention is becoming more data-driven, leveraging advanced tools like transaction monitoring, behavioural biometrics, and machine learning models. For instance, behavioural biometrics can flag potential fraud by detecting inconsistent typing rhythms or a sudden shift from a usual device, such as switching from a personal phone to an unfamiliar desktop during an online transaction.

Counter fraud specialists, data scientists, and Management Information ('MI') engineers are joining forces to leverage customer data more effectively, enabling proactive fraud detection and targeted prevention strategies. Counter fraud specialists identify emerging threats and define key risks, which guide data scientists in developing machine learning models to analyse transaction patterns and detect anomalies. These models, in turn, generate insights that MI engineers translate into real-time dashboards, ensuring investigation teams have the actionable intelligence needed to respond quickly and effectively.

Closer collaboration between counter fraud and Anti-Money Laundering ('AML') teams is driving operational efficiency while enhancing customer protection. For example, financial institutions are integrating AML checks with fraud detection processes during customer onboarding, enabling the identification of stolen or synthetic identities without causing delays. Additionally, many financial institutions are re-evaluating nearshore and offshore operational models, aiming to optimise resources while maintaining robust and effective fraud prevention frameworks.

## Conclusion

In summary, the stabilisation in payment fraud losses reflects the combined impact of regulatory enforcement, operational efficiencies, and technological innovation.

However, technology is a double-edged sword. Whilst advancements in machine learning and AI improve fraud detection, technologies such as generative AI and deepfakes can also create significant vulnerabilities if not carefully managed (see page 11 of this report for further information about how the development of AI is impacting the fraud landscape). As fraud evolves, so must the industry's commitment to innovation and collaboration to sustain the downward trend and protect consumers.

8. Strong Customer Authentication | FCA
9. APP fraud reimbursement protections | Payment Systems Regulator


The national picture

The regional picture

**What are the key forces shaping the fight against payment fraud?**

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government fraud

The historical view

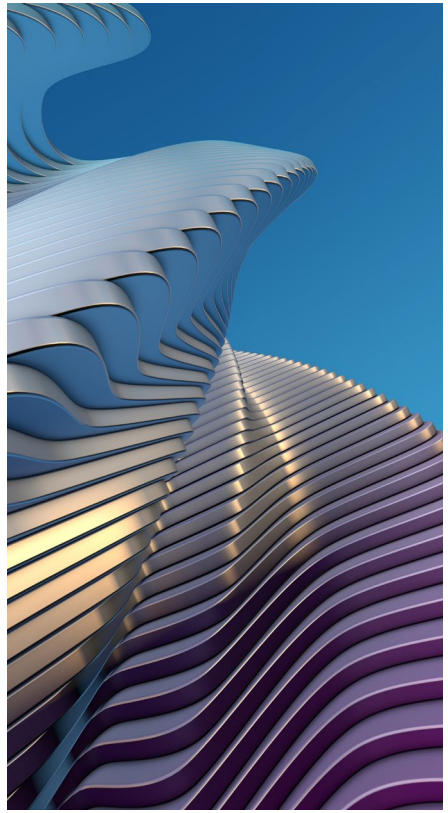
Further resources

# Fraud in the era of AI

- Rupert Walter and Benjamin Cowley

Artificial Intelligence ('AI') is significantly reshaping the landscape of fraud, marking an evident shift in both the prevention and perpetration of fraudulent activities. As AI technologies advance, their integration into organisations is becoming increasingly prevalent, with companies eager to harness AI's transformative power.

The surge in adoption has, in part, been facilitated by the lowering technical barriers to AI use, exemplified by user-friendly platforms like ChatGPT and Copilot, which democratise access to sophisticated AI capabilities. However, this accessibility also presents challenges; as AI becomes more powerful and easier to use, fraudsters are leveraging these very technologies to develop new and increasingly sophisticated schemes, posing challenges to existing detection mechanisms.



## AI in the hands of fraudsters

By harnessing the advanced capabilities of AI, fraudsters are evolving traditional scams and crafting new, intricate techniques that pose significant challenges. Phishing attempts have become highly personalised, utilising contextually relevant lures that are ever more challenging to differentiate from genuine communications. The progression of Large Language Models has enabled the creation of AI-generated text that is virtually indistinguishable from content written by humans, thereby enhancing the effectiveness of scams.

The increased prevalence of deepfake technology and the creation of synthetic identities present emerging threats, with fraudsters now capable of impersonating trusted figures, such as CEOs, using convincingly fabricated audio and video. This manipulation has led to the unauthorised disclosure of sensitive information, the transfer of funds to fraudulent accounts, and other damaging actions, all under the guise of a legitimate request. These new techniques represent a significant and evolving threat that requires vigilant awareness at both an individual and corporate level.

## How AI is assisting in counter fraud activities

Counter fraud activities have historically been slow to embrace AI. Though ubiquitous, AI has struggled to cope with the complexity and variety of threats that a counter fraud professional might typically encounter. However, the advancement of AI-driven fraud schemes and the increasing availability of generative AI, is starting to fundamentally change how organisations approach counter fraud operations.


The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

**Fraud in the era of AI**

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government fraud

The historical view

Further resources

AI can form a key element of a fraud prevention strategy by providing organisations with improved capability to both proactively monitor and reactively investigate fraudulent activities. Proactive monitoring involves the continuous analysis of transactions and behaviours to identify anomalies that may indicate fraud. Early identification of such anomlies can enable an organisation to take action before significant damage occurs.

The anticipated emergence of AI Assistants, powered by generative AI and natural language processing, promises a transformative shift in reactive fraud investigations. These AI modules are expected to perform basic investigative tasks under human supervision, thereby streamlining the process and enabling investigators to focus on complex analysis and decision-making.

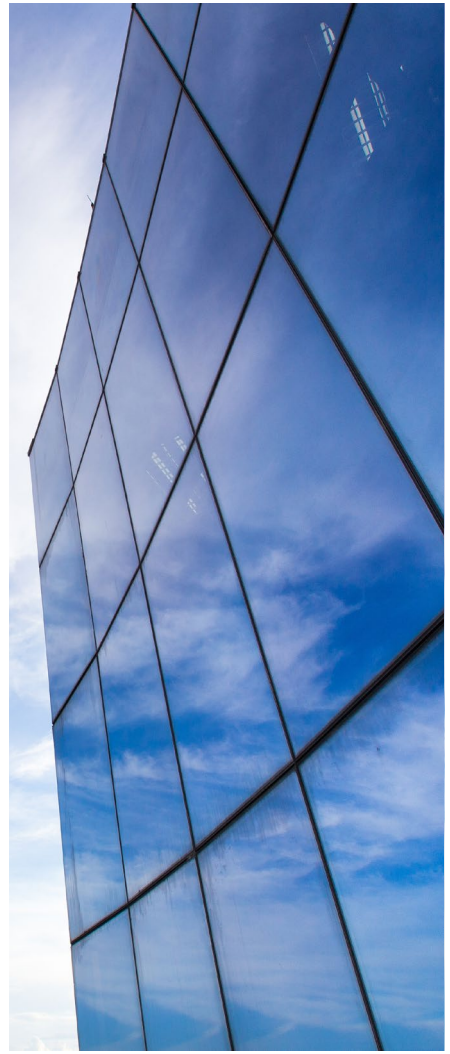
The deployment of advanced AI and machine learning algorithms for fraud detection offers a multitude of benefits, including increased operational efficiencies, which may allow organisations to allocate resources more effectively. Advanced monitoring capabilities can enable the detection of subtle and evolving fraud patterns, while enhanced due diligence processes can enable comprehensive vetting of transactions and third parties. Moreover, AI-driven systems may significantly improve accuracy in fraud detection and reduce the number of false positives identified that have historically burdened counter fraud teams.

## How are organisations safely deploying AI

Safe, secure, and impactful deployment of AI technologies starts with a thorough assessment of an organisation's technological maturity to confirm that both the necessary infrastructure and expertise are readily available to support AI-driven initiatives. Often, the primary obstacle to technology deployment lies within an organisation's data governance framework. High data quality and availability are crucial, as AI systems generally depend on detailed and accurate datasets to detect patterns and anomalies that may signal fraudulent activities. A strategic evaluation of an organisation's goals and technological readiness should steer the selection of AI solutions so that investment is tailored to meet the organisation's specific fraud prevention objectives and directed at the areas where AI can offer the greatest value.

However, deployment of AI should not only involve identifying areas of strategic value; heightened regulatory scrutiny and the potential for reputational damage underscore the necessity for stringent safeguards. To fully obtain value from AI solutions and preserve stakeholder trust in AI systems it is equally important to consider ethical AI practices. Well-defined governance frameworks guide the deployment and ongoing application of AI, incorporate regular consistent evaluation and modification to address emerging fraud threats, and help to ensure compliance with evolving regulatory mandates. Integral to these efforts is the comprehensive education and training of employees, which should be aimed not only at enhancing proficiency with AI technologies but also at cultivating an ethical and vigilant organisational culture attuned to the nuances of fraud prevention.

While AI may introduce organisations to advanced and intricate fraud schemes, it simultaneously unlocks significant potential benefits in the counter fraud space. Like any technological advancement, there exists a perpetual battle between fraudsters and the organisations they are seeking to defraud, each striving to outpace the other and maintain a strategic advantage.




The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

**Fraud in the era of AI**

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government fraud

The historical view

Further resources

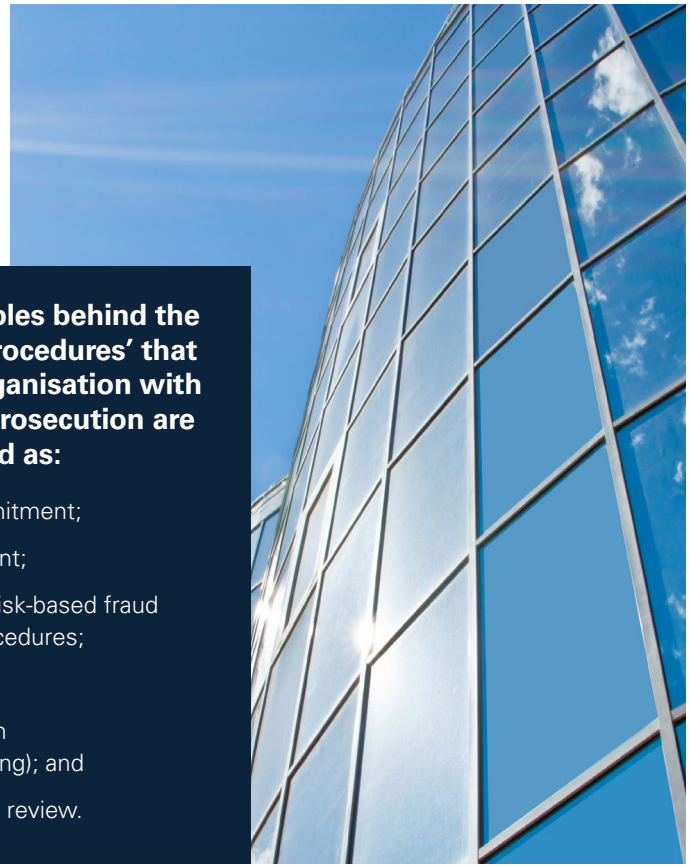
# The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

- Damien Margetson and Annabel Hewitt

In KPMG UK's 2023 Fraud Barometer we covered the new 'failure to prevent fraud' offence which was introduced by the Economic Crime and Corporate Transparency Act 2023 ('ECCTA'). As a one-sentence recap, when the 'failure to prevent fraud' offence comes into force on 1 September 2025 an organisation can be prosecuted under the ECCTA (potentially resulting in a fine) if a relevant fraud offence is committed by an associated person that is intended (directly or indirectly) to benefit the organisation or any person to whom the associated person is providing services on behalf of the organisation, and the organisation did not have 'reasonable procedures' in place to prevent the fraud.

## Government guidance supporting the 'failure to prevent fraud' offence

The Government has now published the guidance on the 'failure to prevent fraud' offence[10] (the 'guidance') to sit alongside the ECCTA legislation.



**The six principles behind the 'reasonable procedures' that provide an organisation with a defence to prosecution are now confirmed as:**

- Top level commitment;
- Risk assessment;
- Proportionate risk-based fraud prevention procedures;
- Due diligence;
- Communication (including training); and
- Monitoring and review.

The six principles underlying 'reasonable procedures' to prevent fraud don't bring much surprise given we were expecting to see a lot of similarities between the 'failure to prevent fraud' offence and the two previously introduced 'failure to prevent' offences relating to bribery and the facilitation of tax evasion.

However, there are slight nuances around the precise wording and the order in which the procedures are presented has changed from the initial draft of the guidance. The moving of 'Top level commitment' to be the top of the list may signify the importance of senior management buy-in to the prevention of fraud and that the effectiveness of fraud prevention procedures stems from this buy-in.

Regardless of this, the full guidance document is a must-read for all organisations.

10. https://assets.publishing.service.gov.uk/media/67868e29c6428e013188179c/Failure+to+Prevent+Fraud+Guidance+-+English+Language+v1.6.pdf


The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

**The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?**

An overview to whistleblowing

The battle against Government fraud

The historical view

Further resources

## Our 5 key takeaways are set out below:

### 1. ‘Benefit’ can be financial or non-financial

We tend to see organisations placing a greater focus on the types of fraud where they are or could be the victim, such as misappropriation of assets by employees or external fraudsters. While it is undoubtedly important to recognise and seek to address these risks, the ‘failure to prevent fraud’ offence does not apply to this type of fraud. Rather, the types of fraud where the organisation is intended to benefit are in scope. These are wide-ranging and include, as examples, false accounting, false statements and fraudulent trading. In our experience, consideration of the types of fraud where the organisation itself is intended to benefit rarely extends past the Finance department (and this tends to focus on the numbers in the financial statements) or are not considered at all.

But what about all of the other information that could be misreported to provide a benefit?

ESG is an obvious place to consider here with pressure from investors, other stakeholders, society and even bold commitments from organisations themselves that they don’t want to be seen to backtrack on.

And what about other departments?

Think of a sales agent making a misleading claim about the organisation’s products/services while seeking to win more sales, or even making false statements about a competitor with the intention to disadvantage them. It is this breadth in the types of fraud in scope for the ‘failure to prevent fraud’ offence that has the real potential to catch an organisation out. Suddenly it is less about the Finance department and the numbers and more about everyone and everything in the organisation.

### 2. Benefit can be inferred

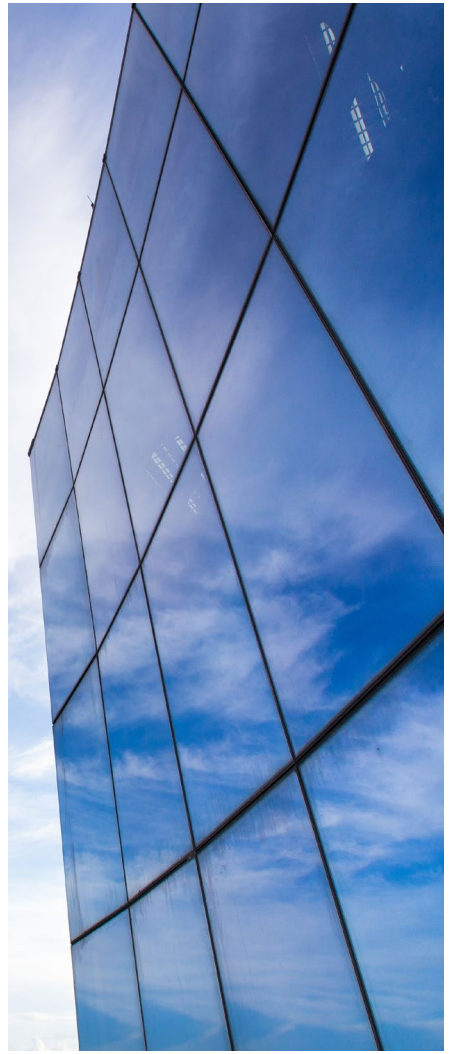
Complexity is added because benefitting the organisation does not always have to be the motivation behind the associated person committing the fraud. An example drawn upon in the guidance is where a salesperson working on commission engages in mis-selling products or services to increase their own commission. As this type of fraud primarily results in money going into the salesperson’s own pocket, this would typically be thought of as misappropriation.

However, this type of fraud also increases the organisation’s sales and, critically, the intention to benefit the organisation can be inferred in this instance. Even though this was not the associated person’s sole, or primary, motivation for committing the fraud, the organisation may still be in breach of the ECCTA and so could face prosecution for the ‘failure to prevent fraud’ offence.

And another layer of complication? Fraud perpetrated by an associated person that benefits an organisation’s clients is also caught by the ECCTA, with the inference of benefit to the organisation on whose behalf the associated person is providing services (presumably because – why else would they do it?).

### 3. Risk assessment is only one of the principles

Given the breadth of fraud offences in scope of the ‘failure to prevent fraud’ offence, carrying out a thorough risk assessment is incredibly important, there’s no doubt about that. If an organisation doesn’t properly understand its fraud risks (financial or otherwise) then it is ill-equipped to deal with them. But the ‘reasonable procedures’ defence is so much more than a risk assessment.




The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

**The Government guidance for the ‘failure to prevent fraud’ offence is now here – what are the 5 key things you need to know?**

An overview to whistleblowing

The battle against Government fraud

The historical view

Further resources

After all, the impact of the risk assessment lessens if, for example, anti-fraud controls are circumvented because culturally employees think it's acceptable to do so. Expected behaviours need to be communicated but can only truly be embedded via top level commitment to fraud prevention.

In other words, it's not enough to just state that the organisation has a zero-tolerance approach to fraud, there has to be genuine action from those at the top to help the organisation to live and breathe it at the various levels within the organisation. Monitoring is also crucial to ensure that the processes actually work.

Think of the 'reasonable procedures' like a jigsaw puzzle – all of the pieces need to fit together to increase the likelihood of a successful defence.

**4. Document the decisions made and revisit them**

The guidance is clear that "the fraud prevention plan should be proportionate to the risk and the potential impact". The principles are not prescriptive as it is recognised that what is appropriate for one organisation may not be appropriate to all organisations.

A common theme in the guidance, however, is that decisions should be documented. For example, there may be instances where it is appropriate for an organisation to take no, or limited, action with regards to a certain fraud risk but the message is that there should be clear rationale behind this which should be captured in writing.

It's also important to remember that an organisation's "response" to this legislation is not something to be done once and then neatly filed away. Risks evolve and circumstances change, whether driven by internal developments or the wider economic environment. It is clear from the guidance that frequent review is expected to ensure that the 'reasonable procedures' evolve with the organisation.

**5. The extent of overseas impact is not clear cut**

The guidance says "The offence will not apply to UK organisations whose overseas employees or subsidiaries commit fraud abroad with no UK nexus". It goes on to explain "By UK nexus, we mean that one of the acts which was part of the underlying fraud took place in the UK, or that the gain or loss occurred in the UK".

For a UK Group with overseas subsidiaries, it is difficult to see how a fraud that benefits an overseas subsidiary does not ultimately flow up the Group to provide a gain in the UK too. It seems that the kind of fraud committed may be particularly important here in determining whether or not the UK company could be found wanting.

Practical application of the rules will become more apparent as prosecutions occur but it may be advisable for organisations to err on the side of caution with actions taken to improve fraud risk management around the Group and not just in the UK.

### So, what can an organisation do now to respond to the legislation?

First and foremost, organisations should be concerned about having 'reasonable procedures' in place to prevent fraud not simply to provide a defence to a potential prosecution, but to actually protect the organisation from fraud in the first place. You've heard the saying that prevention is better than cure – this would be a great example of that in practice.

Unfortunately, when things do go wrong, we commonly see that organisations have not committed the resources to ensuring that a robust fraud risk management framework is in place. It is worth remembering that the cost of getting it "right" could be a fraction of what an organisation may have to pay out should they be successfully prosecuted under the ECCTA for the 'failure to prevent fraud' offence. It's also important to note that, even though the legislation isn't concerned about the types of fraud where the organisation is the victim, taking steps to improve the fraud risk management framework off the back of this legislation will likely help to improve fraud risk management for all types of fraud, because we can say without doubt that every organisation experiences misappropriation fraud on some level. Although there are different types of fraud, the way that an organisation ultimately tries to protect itself from fraud is really the same.

Organisations should now find themselves in a key window of activity as there is a 9-month implementation period written into the guidance to allow organisations time to respond and ensure that they have 'reasonable procedures' in place that are proportionate for their circumstances.

### In summary, there is no "one size fits all" answer

The guidance is clear that an organisation should have effective governance over its fraud prevention framework, so formally designating responsibility to an appropriate individual is likely to be a critical step in ensuring that someone is accountable for driving action, reducing the risk of this topic falling down the agenda and exposing the organisation to potentially significant risk.

With the 9-month implementation period ending on 1 September 2025, organisations should take action now to avoid being left on the starting blocks. The clock is ticking.


The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

**The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?**

An overview to whistleblowing

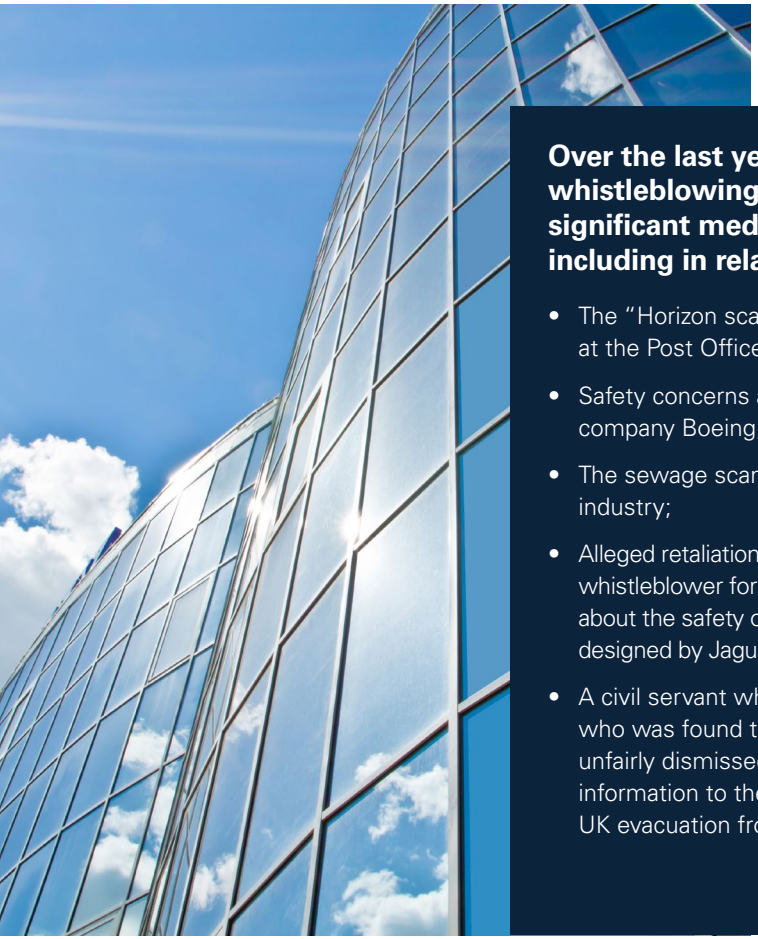
The battle against Government fraud

The historical view

Further resources

# An overview to whistleblowing

- Richard Haynes and Matthew Croad



**Over the last year whistleblowing has received significant media attention, including in relation to:**

- The "Horizon scandal" at the Post Office;
- Safety concerns at the aerospace company Boeing;
- The sewage scandal in the water industry;
- Alleged retaliation against a whistleblower for raising concerns about the safety of electric cars designed by Jaguar Land Rover; and
- A civil servant whistleblower who was found to have been unfairly dismissed after disclosing information to the media about the UK evacuation from Afghanistan.

These and other whistleblowing cases have highlighted that many organisations have inadequate or poorly implemented whistleblowing processes. Whilst the reasons for this can vary, we frequently find that organisations overlook the importance of establishing effective whistleblowing mechanisms.

Whistleblowing should be a core component of an organisation's compliance and governance frameworks. Effective whistleblowing can facilitate the detection and prevention of misconduct, unethical behaviour, unlawful activities, or other wrongdoing, which may help organisations to avoid or limit serious damage, harm and loss associated with such activities. This can include significant reputational damage for organisations that fail to respond appropriately to whistleblowing reports.

## What is whistleblowing?

Whistleblowing is when an individual (the whistleblower) raises a concern to one or more individuals in a position of authority. The nature of the concern can vary but may involve alleged acts or omissions relating to breaches of an organisation's policies and procedures, misconduct, perceived danger, risk, unethical behaviour (including fraud or bribery and corruption), unlawful activity or other wrongdoing.

Generally, the term whistleblowing is thought about in the context of when a whistleblower, with knowledge of suspected misconduct being committed in, by or on behalf of an organisation, makes a report to a relevant group[11] leading to action (such as an investigation) to confirm the accuracy of the report and, where deemed necessary, further responsive action to address the misconduct.

11. Such as senior management within the organisation, a regulator, a law enforcement agency, the press, or the general public.


The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

**An overview to whistleblowing**

The battle against Government fraud

The historical view

Further resources

## The European Union ('EU') Whistleblowing Directive

From a European perspective, one of the most significant recent developments in the whistleblowing landscape was the publication of the EU Whistleblowing Directive[12] (the 'Directive') in 2019. This was prompted, at least in part, by strong public pressure on policymakers to improve protection for whistleblowers linked to high-profile whistleblowing reports.[13]

The Directive instructed each EU Member State to implement legislation requiring in-scope organisations to adopt minimum standards (based on best practices) in their whistleblowing processes, including around the:

- Establishment of accessible, confidential and secure whistleblowing reporting channels;
- Implementation of mechanisms to enable whistleblowing reports to be responded to and followed-up on a timely basis;[14]
- Provision of training around whistleblowing to relevant groups of individuals, such as employees; and
- Protection of whistleblowers from retaliation.[15]

From December 2023, the Directive has applied to all private and public sector organisations[16] with more than 50 employees, all regulated entities within the financial services sector and entities susceptible to money laundering or terrorist financing, regardless of their size.

Certain EU Member States have implemented more stringent legislation that goes beyond the minimum standards established by the Directive. For example, Sweden has extended whistleblowing protection to individuals who provide assistance to a whistleblower.

As the UK is no longer an EU Member State, there is no legal requirement for the UK to implement the Directive. However, the Directive remains relevant for UK organisations with operations in the EU and the minimum standards established by the Directive may be helpful to organisations seeking to implement an effective whistleblowing process as it is a useful reference point.

## Why effective whistleblowing is important

Effective whistleblowing may bring multiple benefits for an organisation, these include:

- Misconduct, unethical or unlawful activity may be easier to detect and detection may occur earlier. This can enable such activity to be addressed more quickly and stop it continuing or escalating, which may potentially prevent or limit further damage, harm and loss;
- Individuals may be less likely to perpetrate misconduct, unethical or unlawful activity at organisations where other individuals are encouraged to speak up about such activity and management are more likely to take appropriate action in response;
- Organisations may find it easier to establish an open and honest culture, which can potentially result in improved levels of communication, productivity and trust;
- Significant reputational damage may be avoided if whistleblowing occurs through appropriate internal channels rather than to external parties; and
- Whistleblowing may help organisations to identify areas of risk, including those that are new or emerging, and understand them better.

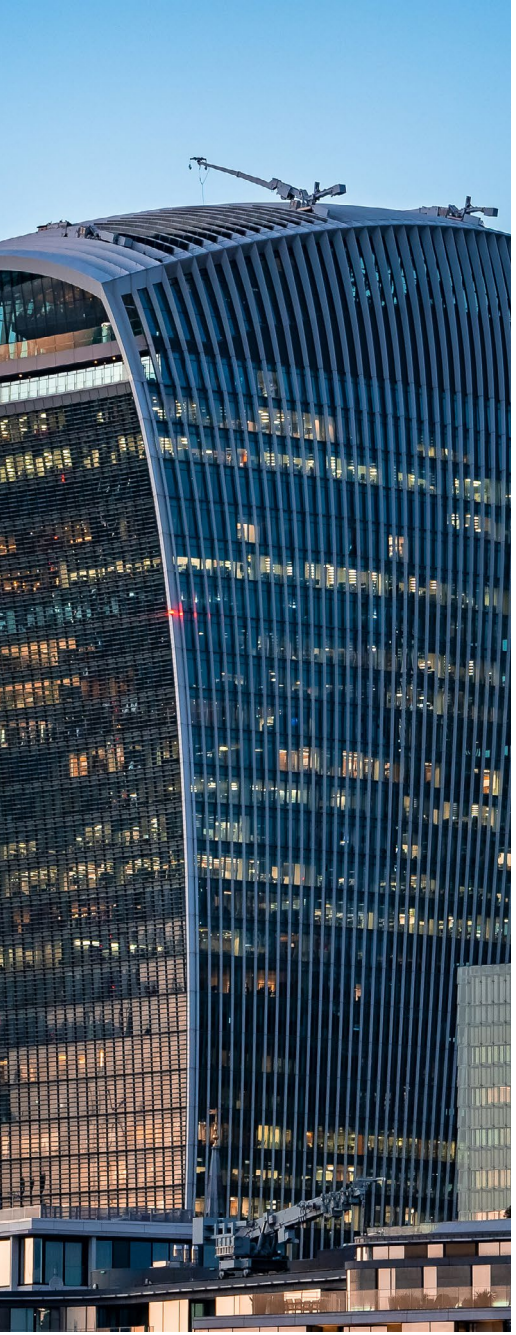
Furthermore, the UK is currently experiencing high levels of fraud. Estimates from the latest version of the Crime Survey for England and Wales published by the Office for National Statistics (the 'ONS') indicate that individuals experienced 3.9 million fraud incidents in the year ended 30 September 2024.[17] However, the actual extent of fraud in the UK may be significantly higher as the ONS estimates that fewer than one in seven fraud offences are reported to the police or Action Fraud.

Operating in an environment with high levels of fraud may result in organisations receiving higher numbers of whistleblowing reports and put increased strain on whistleblowing mechanisms. For those organisations without effective whistleblowing processes, this could present a serious problem.

Whistleblowing is referenced 32 times in the guidance published by the Government in relation to the 'failure to prevent fraud' offence (see page 13 of this report for further information).

12. Directive - 2019/1937 - EN - eu whistleblowing directive - EUR-Lex
13. Such as the leaking of the Panama Papers and LuxLeaks.
14. The Directive includes a prescriptive specific timeline, including requirements for organisations to acknowledge receipt of a whistleblowing report within seven days and provide an update to the whistleblower on the investigation within three months of the initial report.
15. This protection is available to individuals who report breaches of EU law within specific areas (such as public procurement, financial services, and transport safety) that they reasonably believe, at the time of the whistleblowing report, to be true and to constitute a threat or harm to a specified public interest. The whistleblower must also make their report in the context of their "work-based relationship" with an organisation.
16. Both companies and public bodies.
17. Crime in England and Wales - Office for National Statistics


The national picture
The regional picture
What are the key forces shaping the fight against payment fraud?
Fraud in the era of AI
The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?
**An overview to whistleblowing**
The battle against Government fraud
The historical view
Further resources



For organisations to whom the 'failure to prevent fraud' offence is applicable, evidence that established whistleblowing processes are effective may be important in demonstrating whether the organisation has implemented 'reasonable procedures' to prevent fraud.

## Key components of effective whistleblowing

There are various components involved in the establishment of effective whistleblowing mechanisms, including:

- **Investment in appropriate technology:** To encourage whistleblowing, individuals need to have trust in whistleblowing channels. Therefore, it is important for the underlying technology to enable whistleblowing reports to be made in an anonymous, confidential and secure manner. A robust audit trail may help to improve confidence in whistleblowing reporting and reduce inappropriate interference. Technology can also facilitate a faster response to whistleblowing reports, for example, by supporting effective triage of whistleblowing reports.
- **Independence and proportionality in response:** An organisation's response to each whistleblowing report should be independent and proportionate to what is communicated to help avoid unnecessary costs and ensure appropriate action is taken. This may require the establishment of a robust triage process to help evaluate the significance of each report, implementation of a framework to help an organisation determine how to respond in different situations and the involvement of independent individuals in the organisation's response.
- **Monitoring and review:** Regular monitoring and review of whistleblowing mechanisms may help organisations to determine whether they are operating effectively and help to identify issues on a timely basis. This should involve consideration of the end-to-end whistleblowing lifecycle and build on lessons learned in relation to historic whistleblowing reports.

## What organisations may want to consider in relation to whistleblowing

Organisations seeking to assess and, where necessary, improve the effectiveness of their whistleblowing processes may wish to ask the following questions:

- Does the organisation proactively promote awareness of its whistleblowing channels?
- How many reports were received through the organisation's whistleblowing channels in the last year? Does this suggest that potential barriers exist discouraging individuals from making a whistleblowing report?
- Are whistleblowing reports triaged effectively?
- How long does it take for whistleblowing reports to be investigated? Who is responsible for this?
- What monitoring is performed over whistleblowing?
- When was the organisation's whistleblowing policy last reviewed and updated?
- What training is provided around whistleblowing? Who is this provided to?

**The importance of, and increasing focus on, whistleblowing should prompt organisations to consider reviewing their whistleblowing arrangements and, where necessary, make investments to improve the effectiveness of their whistleblowing processes.**


The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

**An overview to whistleblowing**

The battle against Government fraud

The historical view

Further resources

# The battle against Government fraud

- Michael Wong

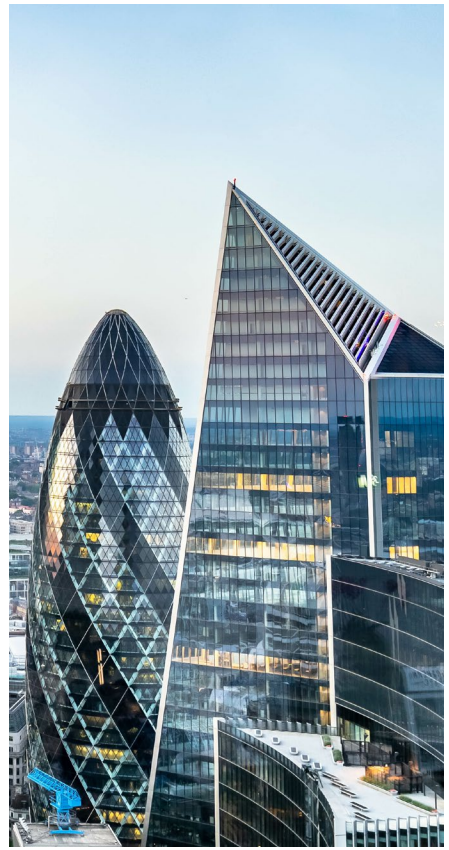
The latest findings from the KPMG UK's 2024 Fraud Barometer a significant shift in the landscape of government-related fraud cases, with the total value plummeting from £592.7 million in 2023 to £236.1 million in 2024. This notable decrease might initially prompt a round of applause for those involved in fighting fraud. However, a closer examination suggests that the battle is far from over.

A landmark case in 2023 involved misrepresentation of assets held in a trust with a value of approximately £416.0 million. This case represented a significant victory for HMRC, the CPS, and taxpayers alike. Yet, when we exclude this outlier, an unsettling trend emerges: nearly a 34% year-on-year increase in the value of the government-related Fraud Barometer cases.[18] This uptick underscores a persistent challenge, especially when juxtaposed against the Public Sector Fraud Authority's estimate of annual fraud and error in public spending, which ranges between £33.0 billion and £59.0 billion.[19]

Fraud will always occur where there are gains to be had. Like the fabled scorpion, pondering whether to sting its frog companion and drown them both, the fraudster will commit fraud because it's in their nature. Where there is opportunity, pressure and rationalisation, they will defraud simply because they can and they do, even if they hurt themselves and those close to them. The narrative of a North Lincolnshire company director, who, with the aid of his wife, brother and two associates, orchestrated a tax fraud scheme amounting to over £7 million, serves as a stark reminder. He was jailed for six years and his accomplices for a total of seven and a half years, despite the brother and two associates being found to have made only nominal financial gains, if any at all.

The real sting in the tail when it comes to fraud against the public sector, is that there is no 'faceless corporation' to pick up the tab or deal with the consequences (note: there never really is). The repercussions extend far beyond the headlines. In an era where Winter Fuel Payments have been cut, there is a social housing "crisis"[20] and local council funding for 2024-25 is projected to be 18% lower in real terms than a decade ago,[21] the impact of fraud on the public purse is more pronounced than ever. Fraud Barometer cases highlight instances where fraudsters have allegedly caused harm to victims and prevented support from being provided to the right people, including:

- £128.2 million of alleged fraud-related money laundering activities, pointing to a dark web of drug dealing, human trafficking, and armed robbery.
- An organised gang's extraction of over £50.0 million in benefits meant for the most vulnerable in society, marking the largest benefit fraud prosecution in England and Wales.



18. KPMG Fraud Barometer data: 2023(a) = 592,687,616; 2024(b) = 236,087,398; Ecclestone case(c) = £416,000,000. (b-(a-c))/(a-c) = 30%
19. Cross Government Counter Fraud Functional Strategy 2024-2027
20. https://chamberuk.com/englands-social-housing-crisis/
21. https://ifs.org.uk/publications/how-have-english-councils-funding-and-spending-changed-2010-2024


The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

**The battle against Government fraud**

The historical view

Further resources

- £14.1 million in alleged COVID-19 and furlough-related fraud across just nine cases, diverting crucial funds from legitimate businesses to fraudsters' extravagant lifestyles.
- A council worker's acceptance of kickbacks from an accomplice, leading to £233k in fraudulent contracts being awarded by a cash-strapped local authority and homes not being maintained as intended.

Recent developments will strengthen the public sector counter fraud agenda. For example, the Government's recently appointed Covid Fraud Commissioner will draw on expertise from across the public sector to seek to recoup public money lost in pandemic-related fraud, and have fraudsters looking over their shoulders or waiting for a knock on the door.

Many entities across the public sector also fall within the scope of the new corporate criminal offence of 'failure to prevent fraud' (see page 13 of this report for further information about the offence), with an emphasis on building an effective anti-fraud culture and increased corporate accountability to do so.

Yet, with fraud constituting around 40% of all recorded Crime in England and Wales,[22] the urgency to bolster prevention, detection, and response mechanisms, particularly in the public sector, cannot be overstated. As taxpayers and service users, the cost of inaction affects us all, underscoring the need for a concerted effort to turn the tide against fraud.

22. Recorded Crime in England and Wales - Office for National Statistics


The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

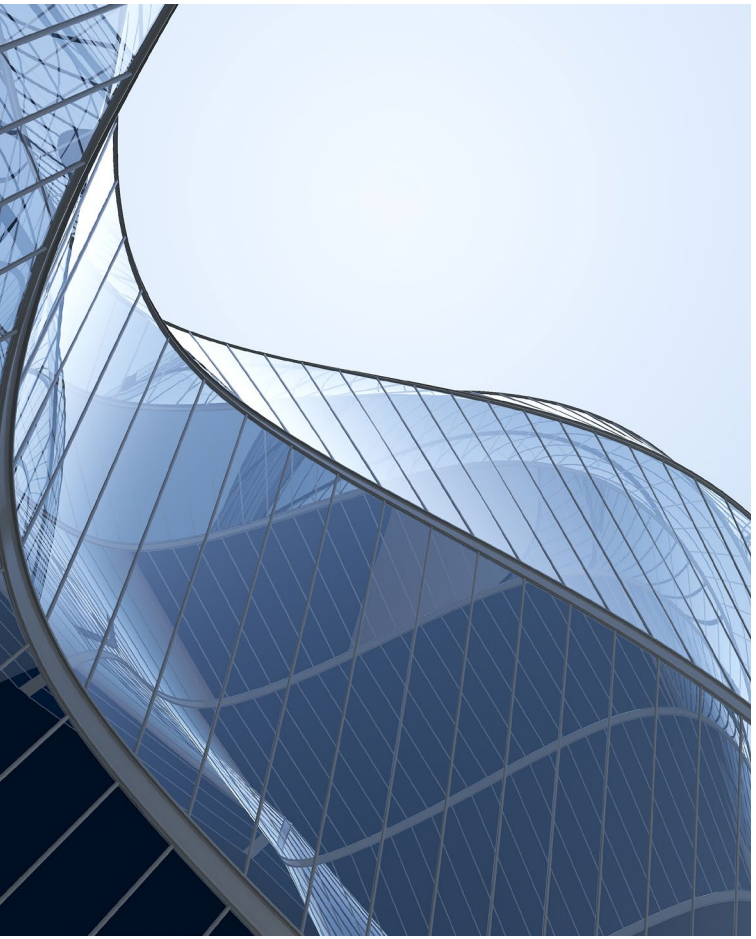
An overview to whistleblowing

**The battle against Government fraud**

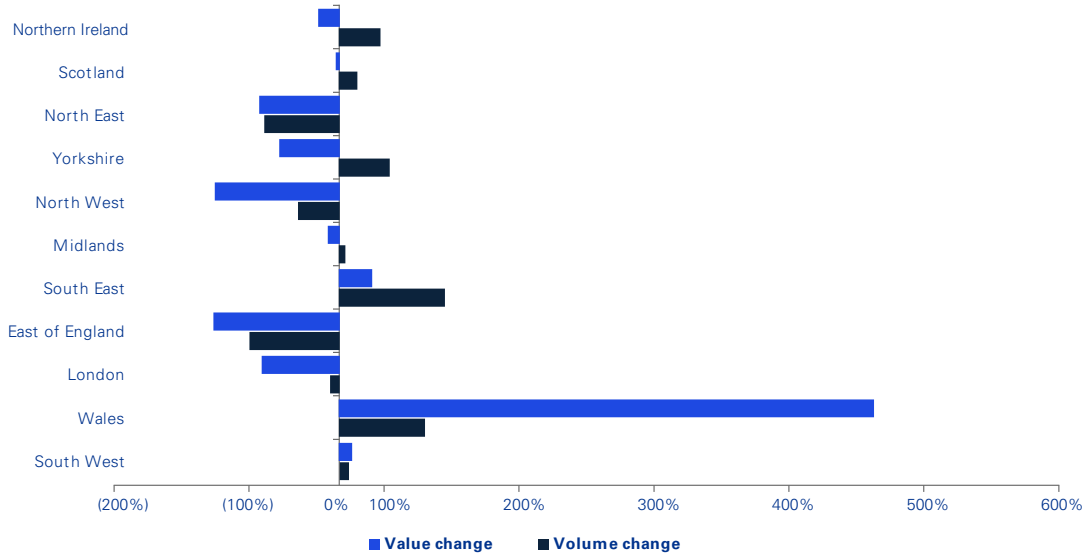
The historical view

Further resources

# The historical view



**Change in volume and value of cases by geographic region (2024 versus 2023).**





The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

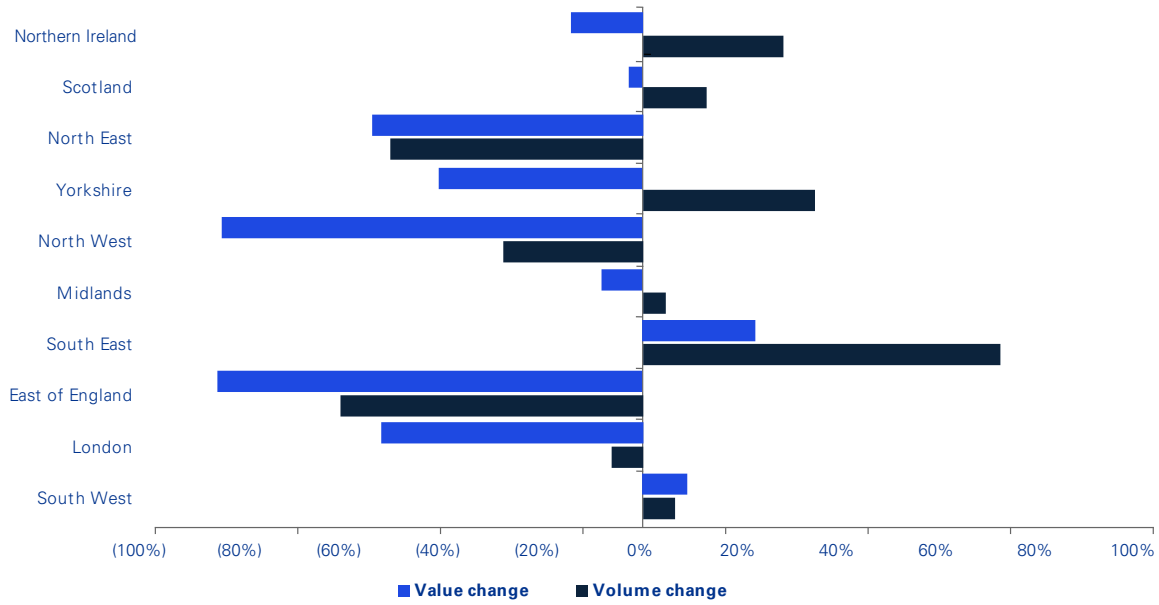
An overview to whistleblowing

The battle against Government fraud

**The historical view**

Further resources

## Change in volume and value of cases by geographic region, excluding Wales (2024 versus 2023)





The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

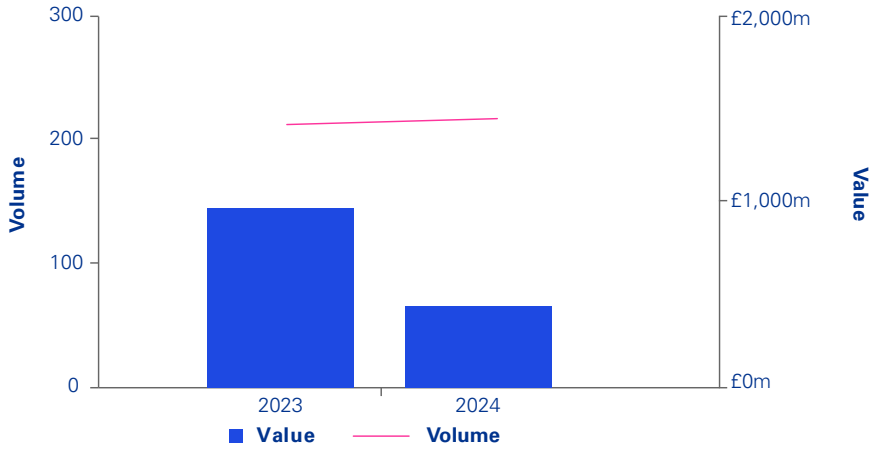
An overview to whistleblowing

The battle against Government fraud

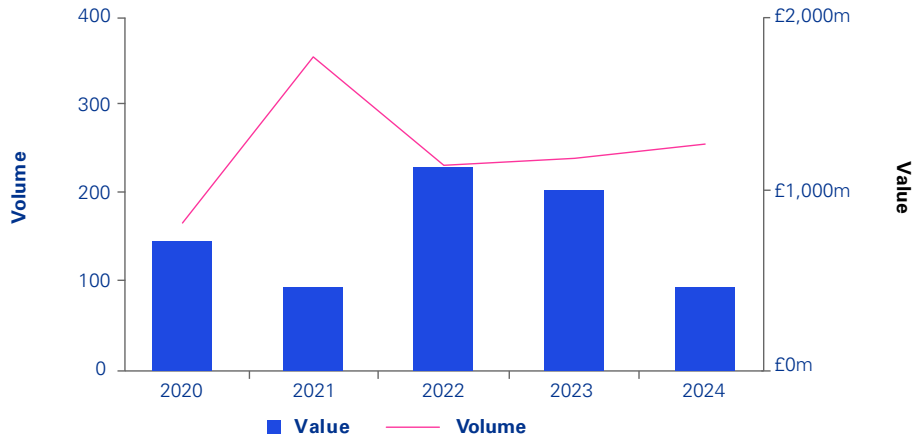
**The historical view**

Further resources

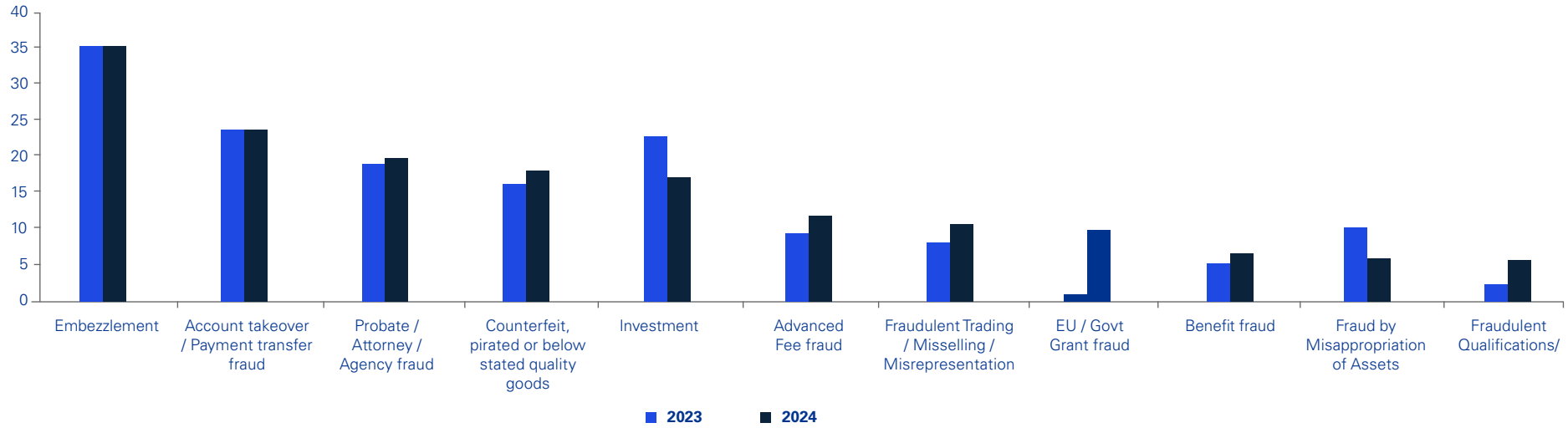
## Total volume and value of cases recorded (2024 versus 2023)




## Total volume and value of cases recorded over the last five years




## Top frauds by case volumes in 2024, the prior year comparison





The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

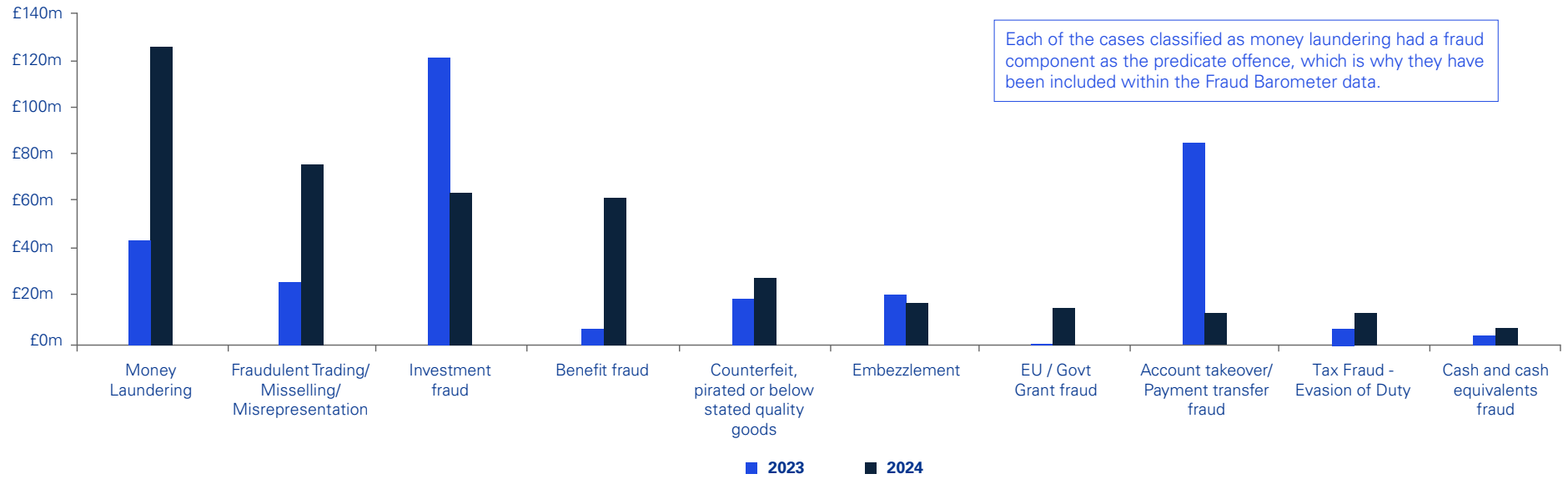
An overview to whistleblowing

The battle against Government fraud

**The historical view**

Further resources

## Top frauds by case values in 2024, with the prior year comparison




Each of the cases classified as money laundering had a fraud component as the predicate offence, which is why they have been included within the Fraud Barometer data.


The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

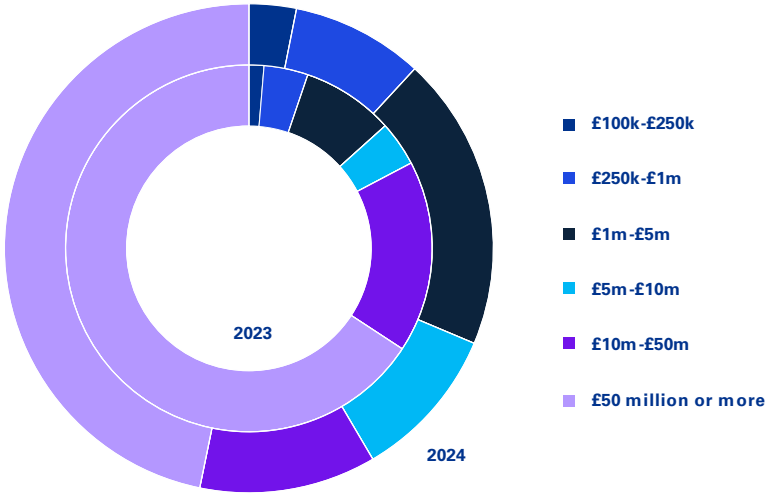
An overview to whistleblowing

The battle against Government fraud

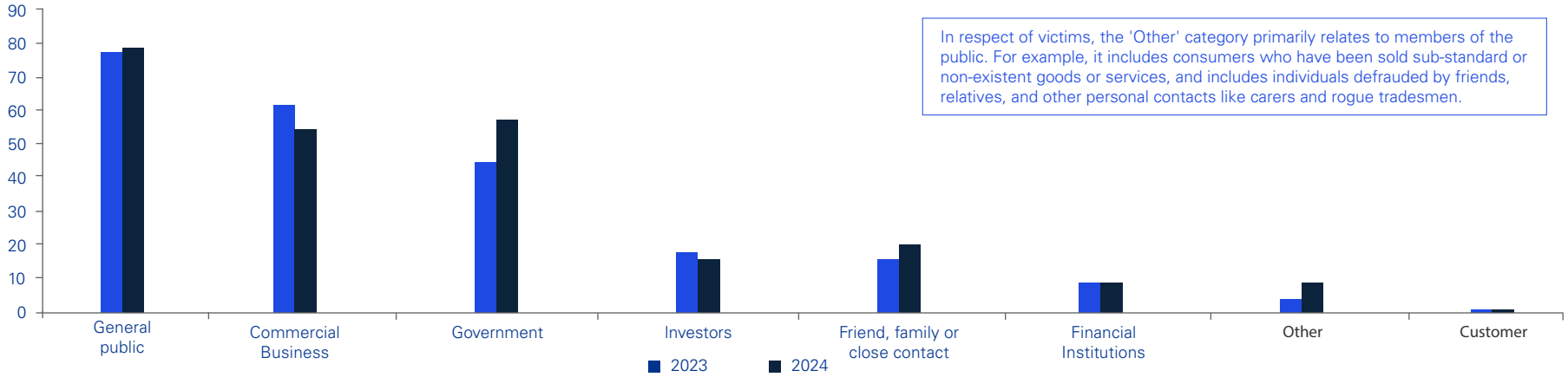
**The historical view**

Further resources

## Proportion of values in Fraud Barometer, by case value range




## Fraud volumes by victim, 2023-2024




In respect of victims, the 'Other' category primarily relates to 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.


The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government fraud

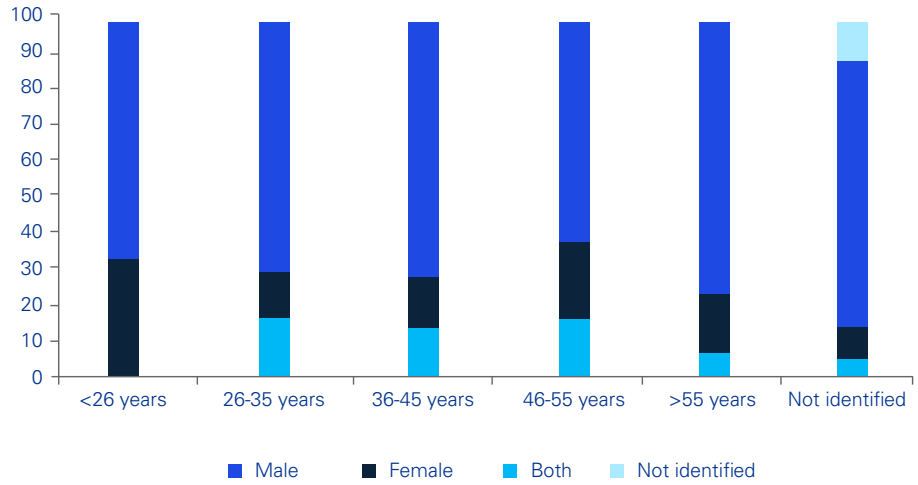
**The historical view**

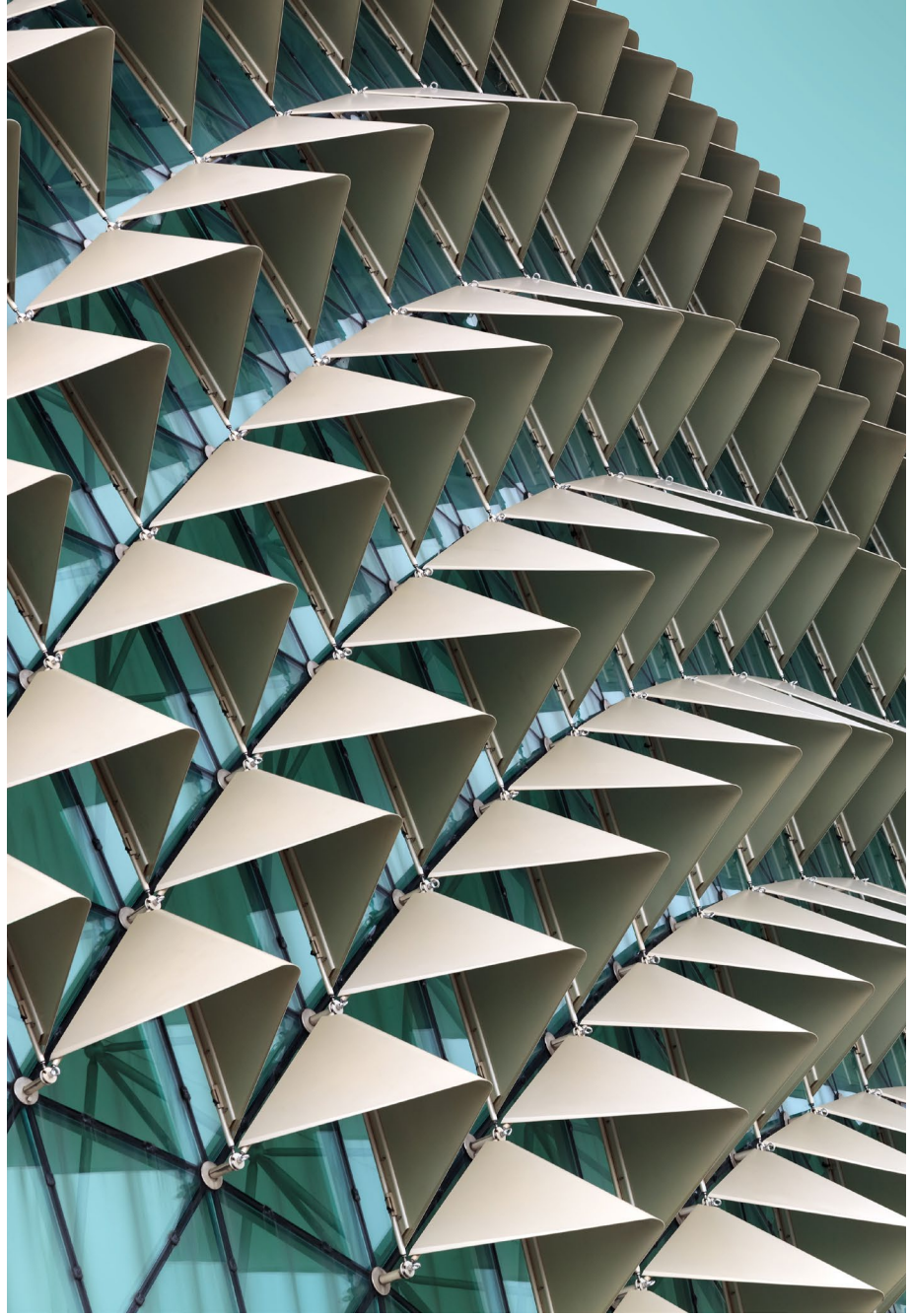
Further resources

## Fraud volumes by perpetrator, 2023-2024


In respect of perpetrators, the 'Other' category 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.

## Gender and age distribution of fraud cases by volume in 2024




The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government fraud

**The historical view**

Further resources

# Further resources

Please see our website[23] 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 to prevent, detect or respond to fraud, or help your organisation to prepare for the 'failure to prevent fraud' offence coming into force.

23. https://kpmg.com/uk/en/home/insights.html

## The KPMG Fraud Barometer National team


### Roy Waligora
**Head of Investigations and Fraud Barometer Lead Partner**
KPMG Forensic
E: roy.waligora@kpmg.co.uk
T: +44 (0) 746 490 2991

### Matthew Croad
**Senior Manager**
KPMG Forensic
E: matthew.croad@kpmg.co.uk
T: +44 (0) 774 745 6380

### Cuthbert Chiduku
**Manager**
KPMG Forensic
E: cuthbert.chiduku@kpmg.co.uk
T: +44 (0) 775 937 1598

### Phoebe Calloway
**Assistant Manager**
KPMG Forensic
E: phoebe.calloway@kpmg.co.uk
T: +44 (0) 755 414 5892

### Rishiharan Ragulan
**Apprentice**
KPMG Forensic
E: rishiharan.ragulan@kpmg.co.uk
T: +44 (0) 777 829 9919

### Chloe Tomlinson
**Graduate**
KPMG Forensic
E: chloe.tomlinson@kpmg.co.uk
T: +44 (0) 795 531 2810

### Honor McKenzie
**Graduate**
KPMG Forensic
E: honor.mckenzie@kpmg.co.uk
T: +44 (0) 793 535 0831



The national picture

The regional picture

What are the key forces shaping the fight against payment fraud?

Fraud in the era of AI

The Government guidance for the 'failure to prevent fraud' offence is now here – what are the 5 key things you need to know?

An overview to whistleblowing

The battle against Government fraud

The historical view

**Further resources**

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



Document Classification: KPMG Public

CREATE: CRT159173D | May 2025