FraudTrack 2025

Reflecting on an environment of perpetual change

IDEAS | PEOPLE | TRUST

FraudTrack 2025

Reflecting on an environment of perpetual change

Contents

FraudTrack methodology

The data analysis used for FraudTrack 2025 is based on UK fraud and economic crime cases reported in the public domain as having a monetary value of £50,000 and above from 1 December 2023 to 30 November 2024 ("2024"). FraudTrack data periods run from December to November in the following year. For simplicity, each year is referred to by the year the period ends in. The data collected is used to identify trends in the fraud and economic crime matters reported during the current period, as well as providing a means to compare to reported data from previous years. We have not carried out any verification work on the reported items. Whilst attempts have been made to ensure the FraudTrack data does not include duplicate reported cases, it is acknowledged that any unclear, overlapping or inaccurate reports could potentially impact the accuracy of the FraudTrack data and therefore the reported trends.

A word from Stephen Peters, Head of Investigations

Fraud continues to be one of the most important risks facing businesses, individuals, and public institutions. Despite ongoing efforts to combat financial crime, perpetrators of fraud remain highly adaptable, exploiting new technologies, regulatory gaps, and human vulnerabilities to further their schemes. As we assess the trends of 2024 and look ahead to 2025 and beyond, it is clear that fraud is not only persistent but evolving in its breadth and complexity.

This past year has seen a shift in both the methods used to perpetrate fraud and the responses from businesses and regulators. The rise of sophisticated AI and tech-driven frauds has reinforced the need for robust fraud prevention strategies, while increased regulatory scrutiny and new legislation is prompting organisations to take fraud risk management more seriously. At the same time, it is generally accepted that fraud remains vastly underreported, particularly when it comes to individuals, raising important questions about awareness, accountability, and the true scale of the problem.

With new legislation shaping corporate responsibilities and financial institutions strengthening their protection measures, there is reason for optimism. However, the fraud landscape is constantly shifting, and the coming year will likely bring fresh and unforeseen challenges. As fraudsters continue to refine their tactics, businesses must do the same – embedding stronger controls, leveraging technology for detection and prevention, and fostering a culture where fraud awareness is front of mind.

While eliminating fraud entirely is an aspiration that is unlikely to be achieved, staying ahead of emerging threats is both possible and necessary. A proactive, collaborative and focussed approach will be key in the ongoing fight against financial crime.

Stephen Peters
Partner and Head of Investigations

Fraud and economic crime value declines despite reported incident numbers holding steady

The value of reported fraud and economic crime took a dramatic plunge last year, falling to £550 million, down from £2.3 billion in 2023. This sharp decline was largely driven by a 63% drop in reported high-value cases (those exceeding £50 million) when compared to the previous year.

Looking at the bigger picture, this shift aligns with a broader five-year downward trend in reported fraud. However, 2021 remains a significant anomaly, standing out as a peak year due to the surge in fraudulent activity during the COVID-19 pandemic.

Figure 1: Total reported fraud values from 2020 to 2024 (£m)

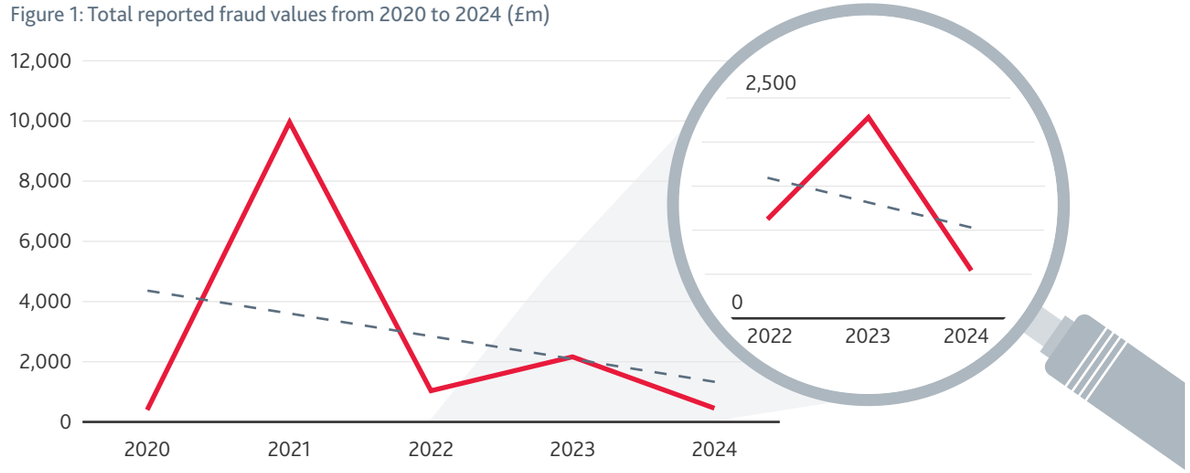
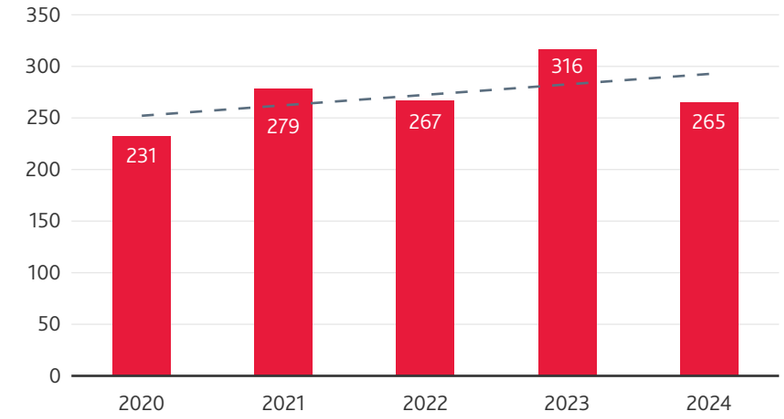
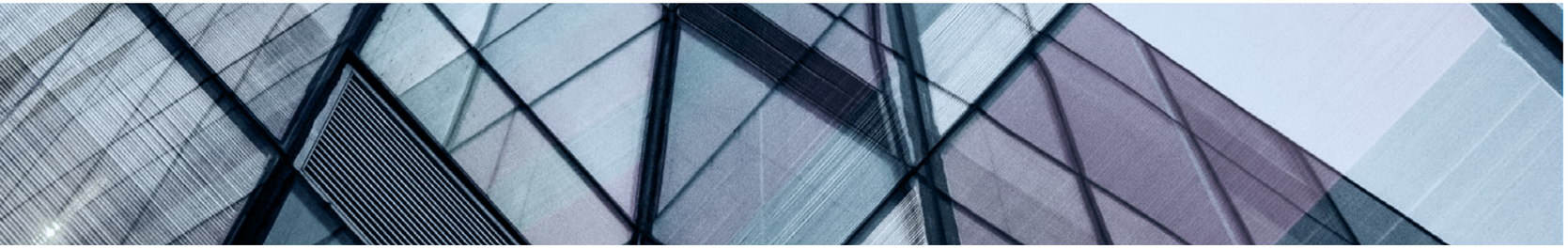


Figure 2: Total number of fraud cases reported per year over past 5 years





Alongside the steep decline in total reported fraud value in 2024, the number of fraud cases has also seen a 16% drop, although interestingly the five-year trend shows an upward trajectory and remains broadly steady. The combined effect is that the average fraud value has plummeted by 71% compared to 2023, reinforcing the impact of fewer high-value fraud cases last year.

This downward shift in reported fraud was also reflected in our BDO Fraud Survey 2024, which found that 42% of UK businesses experienced fraud in 2024 – significantly lower than the 83% reported in 2023.

High-value fraud and economic crime cases: a closer look

Only three high-value UK cases were reported last year, totalling £371 million, a notable decrease from the eight cases reported in 2023, which amounted to £1.9 billion.

Together, these three cases represented around 70% of the total reported fraud value for the year:

- **The Gold Money Laundering case:** a high-profile money laundering case where £266 million of criminal cash was reportedly laundered through a gold trading operation
- **The Money Transfer Laundering case:** a case involving the alleged laundering of £55 million by a Chinese gang through an international network and an informal money transfer system
- **The Universal Credit fraud:** a £50 million fraud where a five-member Bulgarian gang were reported to have defrauded the Department of Works and Pension ('DWP') regarding fraudulent Universal Credits claims.

High-value cases such as these have the potential to cause significant repercussions, not only for the affected companies, but for the wider economy. This could happen in two key ways:

1. **Financially**, they drain substantial resources from both public and private sectors, potentially leading to increased costs for businesses and taxpayers
2. **Reputationally**, they can damage trust in regulators, institutions and systems.

Successful high-value fraud and economic crime can also encourage further criminal activity if not addressed, creating a cycle of crime that becomes increasingly difficult to break. It is therefore crucial that the corporate world continues its momentum in improving anti-fraud culture whilst government policies, regulations and legislation help tackle these issues head-on to protect financial stability and maintain public confidence.

Can new legislation help reduce fraud?

New fraud and financial crime legislation is incentivising large organisations to step up their fraud prevention strategies. Legislation such as the Failure to Prevent fraud offence, introduced under the Economic Crime and Corporate Transparency Act (ECCTA) which comes into force in September 2025, is set to hold organisations criminally responsible for failing to prevent fraud committed by their employees or associates for the organisation's benefit. To avoid prosecution, businesses will need to demonstrate that they have implemented 'reasonable fraud prevention measures', inspiring many large organisations to increase investment in their fraud protection infrastructures.

In the BDO Fraud Survey 2024, we found:

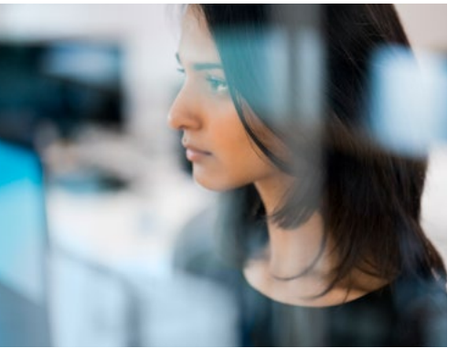
- **78%** of businesses had begun preparations for ECCTA
- **43%** reported an increase in fraud awareness since the introduction of ECCTA.

"The introduction of the Economic Crime and Corporate Transparency Act (ECCTA) and the new corporate criminal offence for failing to prevent fraud is a significant step forward in the UK's efforts in tackling fraud. It is encouraging to see organisations taking this seriously and enhancing their fraud risk management strategies. This proactive approach is crucial not only to protect themselves from being victims of fraud but also to ensure they don't inadvertently benefit from fraudulent activities, which could lead to offences under the act."

Ian Bennington
Partner
Ethics and Compliance Services National Lead

Fraud and economic crime typology patterns

In 2024, the top three main types of fraud and economic crime by value were: (i) money laundering, (ii) non-corporate fraud[1], and (iii) third party fraud.[2] These three categories together made up over 90% of the total reported fraud and economic crime value and nearly 70% of the total number of incidences reported.

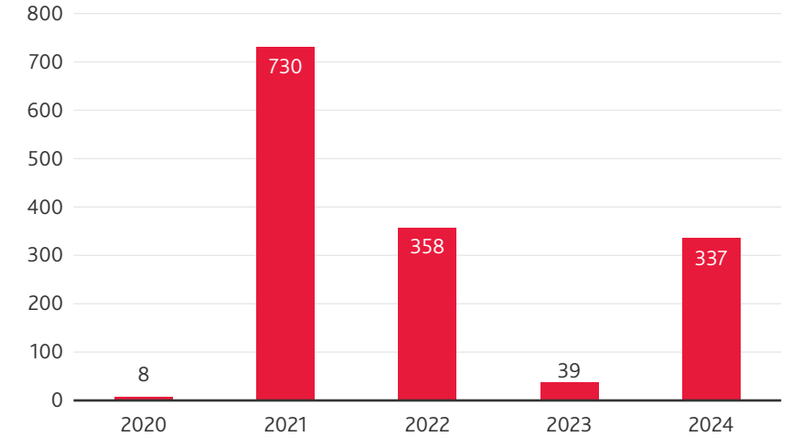


Money laundering boom

In 2024, money laundering was the largest reported main fraud and economic crime type by value, which at £337 million represented 61% of the total 2024 value. The average reported value of money laundering in 2024 was £19.84 million, a 10-fold increase on the 2023 average value of £1.96 million.

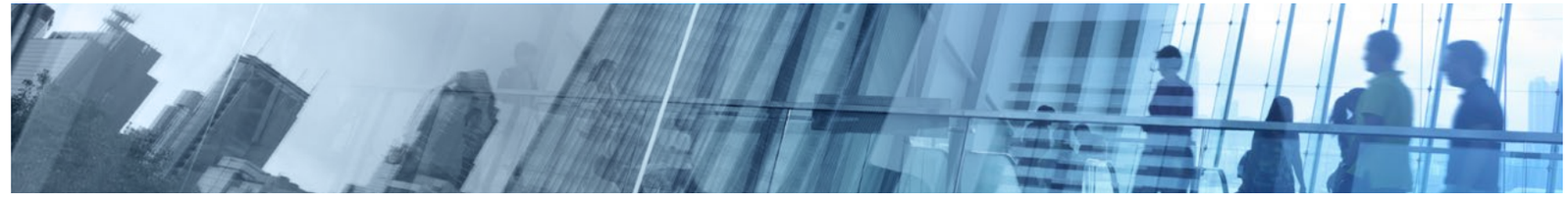
The majority of the £337 million total value of reported money laundering matters in 2024 related to just two cases: The Gold Money Laundering case (£266 million) and the Money Transfer case (£55 million). The Gold Money Laundering case recently hit the headlines again after the retrial of the five defendants and reportedly involved the use of large volumes of criminal cash to buy gold, which was then shipped to Dubai. The Money Transfer Laundering case led to seven individuals being jailed for reportedly operating an undercover money laundering ring aimed at international university students seeking to bypass limits on the amount of cash that can be taken out of China.

Figure 3: Total reported money laundering fraud values over past 5 years, 2020 to 2024 (£m)



"The National Crime Agency's latest National Strategic Assessment 2025 of Serious and Organised Crime highlights that there is a realistic possibility that over £100 billion is laundered through and within the UK each year. This makes money laundering a critical factor in how corporate entities assess their financial crime risk management frameworks and risk assessments. While money laundering isn't always reported as fraud, illicit gains from fraudulent activities often need to be processed through financial systems. With fraud prevention and anti-money laundering high on the agenda for regulators and Government agencies, companies should view these offences through a combined lens. An integrated approach to managing fraud and money laundering risk is essential."

Fiona Raistrick
Partner
Financial Services



[1] Frauds committed by an individual or a group of individuals (for the avoidance of doubt this category excludes frauds committed by perpetrators that are employees or customers of the victim entity)

[2] Whereby a third party of a company, such as its customers or suppliers, commits fraud against it.

Fraud and economic crime typology patterns

Continued

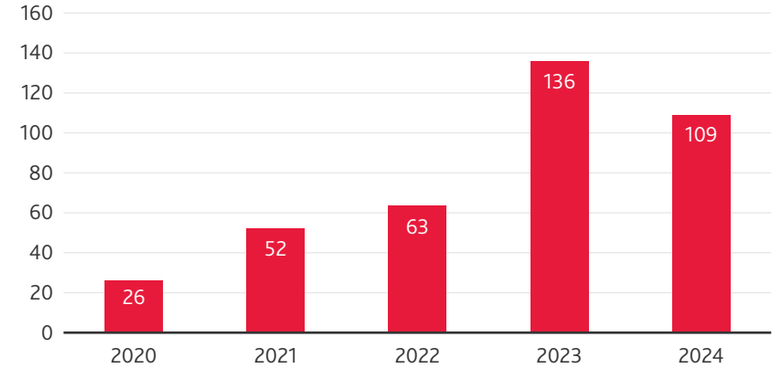
Non-corporate fraud tops the frequency charts

Reported non-corporate fraud amounted to £123 million in 2024 and was the most common fraud by volume. This category includes a range of frauds committed against individuals or third party entities such as phishing scams and identity theft. Non-corporate fraud represented 41% of the fraud cases reported in 2024 by number and is the second highest count of non-corporate frauds recorded over the past five years.

The largest non-corporate fraud case last year saw a five-member Bulgarian gang orchestrate a £50 million scam against the Department for Work and Pensions (DWP). Their scheme revolved around fraudulent Universal Credit claims, with thousands of recruits in Bulgaria falsely posing as UK residents and workers. To maximise payouts, the gang even created fictitious identities for children, exploiting the system on a massive scale.

Our observation that non corporate fraud was the most common reported fraud by volume is also consistent with the National Strategic Assessment 2024 of Serious and Organised Crime[3], which found that fraud against individuals remained the most commonly reported crime in the UK.

Figure 4: Total number of reported non-corporate fraud cases over past 5 years, 2020 to 2024



Third party fraud remains a consistent threat

Third party fraud remained one of the most prevalent types of fraud in 2024, typically involving businesses deceiving their customers or suppliers, or being defrauded by them. While the total value of these cases has dropped significantly (£46 million in 2024, down from £452 million in 2023[4]), third party fraud has consistently ranked among the top three fraud types over the past five years.

The largest third party fraud by value reported in 2024 was a £9 million pyramid scheme investment scam. Two individuals deceived various investors into contributing large sums, only to use these funds to repay other investors and sustain the scam.

With new regulations introducing measures to increase corporate accountability, organisations are under increasing pressure to strengthen their fraud prevention measures. Indeed, the introduction of the "Failure to Prevent Fraud" offence this year is expected to drive more businesses to implement robust safeguards, reducing the risk of third party fraud.

[3] https://www.nationalcrimeagency.gov.uk/images/campaign/NSA/2024/NSA_2024_Website_-_PDF_Version_1.pdf

[4] The 2023 third party fraud total included two large cases: a £260 million software-related fraud and a £150 million bid rigging fraud in the construction sector.

A deeper look into the granular fraud types reported

In order to gain a more nuanced understanding of the different forms of fraud faced by businesses and individuals today, we have conducted further analysis into the granular fraud types reported. This deeper insight can allow us to identify patterns, assess risks more accurately and develop more targeted strategies to prevent and combat fraud in the future.

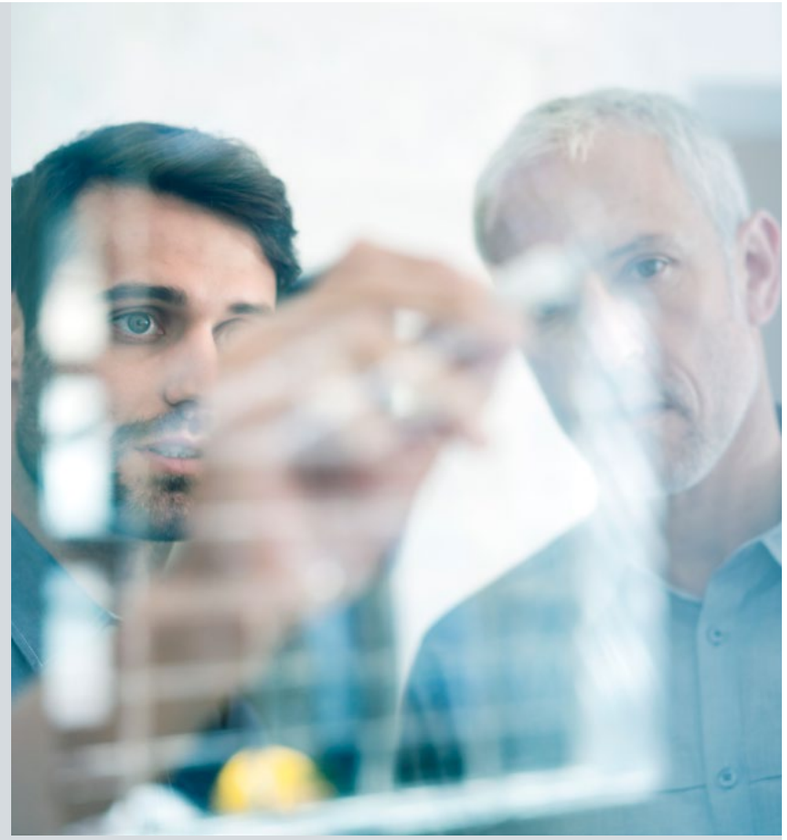
In 2024, the top three granular fraud types were:

- Financial investment fraud
- False claims and overpayments
- Unauthorised use/misappropriation of assets.

Together, these three methods of committing fraud made up £148 million, or 27% of the total reported fraud value, and nearly 40% of the total number of frauds reported in 2024. The table below shows these granular fraud types by monetary value for 2024 compared to 2023:

Table 1: Total monetary value of fraud cases for top 3 granular fraud types for 2024, compared with 2023

Granular fraud type	2024 (£m)	2023 (£m)
Financial Investment fraud	69.2	117.3
False claims and overpayments	60.1	8.3
Unauthorised use/misappropriation of assets	18.4	65.9

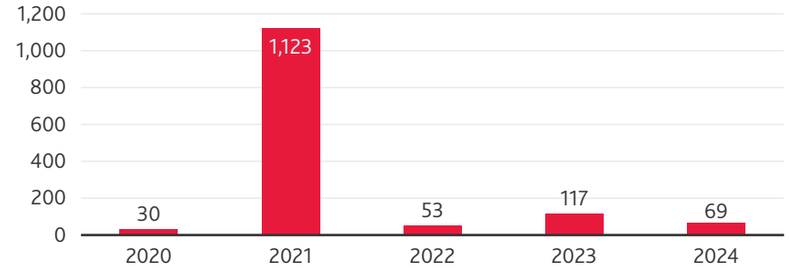


Financial investment fraud

Financial investment fraud involves deceiving victims into investing money in fraudulent schemes, typically with the promise of high returns. Instead, the fraudsters siphon off some or all of the funds with the investors losing out.

This is the largest reported granular fraud type by monetary value, totalling £69 million or 13% of all frauds in 2024, though it was dwarfed by the huge spike in the 2021 value. The value of financial investment fraud reported in 2024 represents a 41% decrease compared to 2023, a year inflated by three higher value cases each exceeding £20 million in value.

Figure 5: Total reported financial investment fraud values over past 5 years, 2020 to 2024 (£m)



This year the two most significant financial investment fraud cases reported were:

- **Fraudulent investment scam:** a 46-year-old individual misled approximately 240 people into investing around £19 million in a fraudulent investment scheme by providing misleading information about the scheme's operation and the profits it would generate
- **'Risk-free' investments case:** two accountants swindled clients out of nearly £9 million. They falsely promised risk-free investments with high returns, claiming the funds were securely held in Singapore. Instead, they spent the funds on luxury cars and holidays.

A deeper look into the granular fraud types reported

Continued

False claims and overpayment fraud

False claims and overpayment fraud typically involves the fraudster providing incorrect or misleading information to receive payments, reimbursements or benefits (e.g. government grants) that they are not entitled to.

This type of fraud ranks as the second largest granular fraud type by value, totalling £60 million or 11% of reported frauds in 2024. False claims and overpayment frauds saw a huge increase of over 600% in 2024 when compared to the £8 million reported in 2023. This is primarily due to the Universal Credits fraud case, which alone reached £50 million.

False claims and overpayment fraud also included the following cases:

- **COVID-19 support scam:** twelve members of a national organised crime group fraudulently claimed £2.5 million in COVID-19 support grants. They used non-trading businesses and stolen identities to secure grants, bounce back loans, and HMRC support payments
- **Home repair fraud:** A gang of criminals targeted over 20 elderly and vulnerable victims, charging them for unnecessary house repairs and subsequently leaving their homes in worse condition. The total value of this fraud was £1.2 million.

Unauthorised use and misappropriation of assets

This granular fraud type involves the theft or misuse of cash or non-cash assets. This can include fraudsters diverting funds from a corporate entity or an individual's bank account, for example where they have been nominated to act on their behalf.

In 2024, reported cases of this type of fraud totalled £18 million, accounting for approximately 3% of total fraud by value. These cases highlight the need for more vigilance among both individuals and corporate entities alike. To mitigate risk, businesses should implement strong internal controls, conduct regular internal and external audits, and maintain strong oversight to detect and prevent these types of fraud.

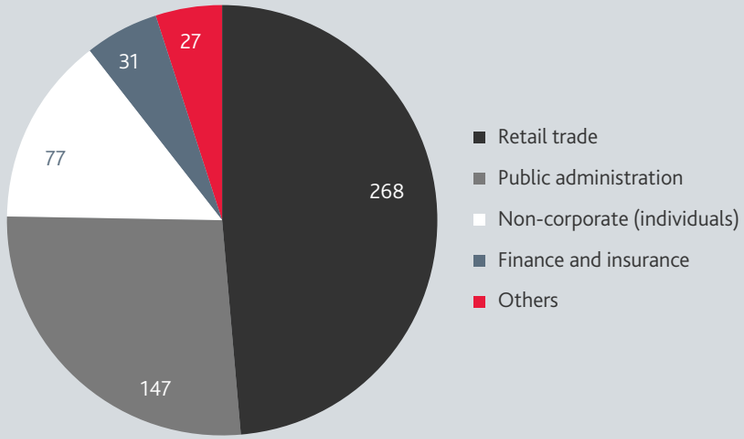
Some significant cases reported this year include:

- **Barristers' chambers embezzlement fraud:** a former credit control manager at a London barristers' chambers reportedly embezzled £2.75 million over five years. She was in charge of the bank account where fees due to barristers were deposited
- **The council fraud gambler:** a former finance officer at a local council stole nearly £1 million of taxpayers' money over almost 20 years, transferring funds into his own bank account to support his gambling addiction
- **The luxury lifestyle fraud:** a former council employee embezzled over £1 million, exploiting his position for over 17 years to fund holidays, luxury goods and personal expenses.

Fraud and economic crime trends across industry sectors

Examining industry data reveals clear distinctions between how hard different sectors were impacted by fraud and economic crime. In 2024, retail was the hardest hit, followed by public administration and fraud targeting individuals. Understanding these trends can help identify where fraudsters are striking most and how risks are evolving.

Figure 6: Total monetary value of fraud cases by industry sectors for 2024 (£m)



Retail trade sector

The retail sector saw a significant rise in reported fraud and economic crime in 2024, largely due to the high-value Gold Money Laundering case valued at £266 million. This significant rise represented an increase of over 1,200%, making retail the highest reported fraud sector of the year.

The retail sector presents a range of opportunities to commit fraud, particularly if monitoring and controls are not effectively managed. Key risk factors in retail include:

- **High transaction volumes,** making it easier for fraudulent transactions to go undetected
- **Cash handling,** which increases opportunities for theft, fraud and economic crime, including money laundering
- **Supply chain complexities,** creating opportunities for fraudulent invoicing, connected party frauds, sanctions risk and receipt of counterfeit goods
- **The rise of e-commerce,** which has expanded the threat landscape, exposing retailers to scams, payment fraud, and other online risks.

"Retail remains one of the most targeted sectors for fraud, with 2024 seeing a significant surge driven by large-scale money laundering, digital fraud and phishing scams. Ongoing vigilance and robust controls are essential as the sector continues to face complex and evolving threats."

Sophie Michael
Partner
Head of Retail

Fraud and economic crime trends across industry sectors

Continued

Public administration

The public administration sector continues to be heavily affected by fraud, consistently ranking among the top two sectors hit by fraud over the past five years.

In 2024, public administration faced significant challenges from fraud and economic crime such as false claims (e.g. government grants and benefits), money laundering, regulatory breaches and tax fraud. The persistence of fraud in this sector is driven by several factors, including fraudsters' access to advanced technology and the need for ongoing training and support for employees across what are often large multi-faceted organisations to ensure they are equipped to identify and respond to fraudulent activities effectively.

Given the significant impact of fraud on the sector, strengthening prevention and detection measures will likely remain a high priority on the government's agenda, driving initiatives to combat the issue.

Frauds against Non Corporates (individuals)

The most common fraud types committed against individuals were:

- **44%** in the form of financial investments, accounting for £34 million of fraud against individuals in 2024. Victims were often targeted by someone they thought they could trust, leading them to invest sometimes large sums into fraudulent schemes. The use of AI and other advanced technologies have provided fraudsters with a treasure trove of new fraud-enabling tools to dupe individuals and gain their trust
- **7%** of the total frauds against individuals reported this year were unauthorised use/misappropriation of assets, accounting for £5.7 million. This granular fraud type features high volumes of smaller value frauds including examples where elderly and vulnerable people were taken advantage of after trusting another person with their assets or cash.

Why do individuals remain the prime target for fraud?

While high-value corporate fraud persists, individuals often remain the primary target for fraudsters. Large-scale 'fraud farms', often linked to organised crime, use fraud-enabling technology to launch mass attacks on individuals via email and social media.

Although awareness of scams is improving, many vulnerable people – and more commonly than would be expected, sophisticated individuals, both young and old, still lack the knowledge to identify and avoid phishing, investment and other common fraud schemes. On top of this, the fraud landscape is constantly evolving. And as technology evolves, so do fraud methods and tactics, with criminals exploiting weaknesses before they can be addressed or exposed.

The true scale of fraud against individuals is likely far greater than reported. According to the National Crime Agency, only 13% of fraud against individuals are reported to Action Fraud.[5] The reasons for this underreporting will vary from individual to individual but may be impacted by embarrassment or shame and an uncertainty as to whether reporting the fraud would impact their situation.

[5] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

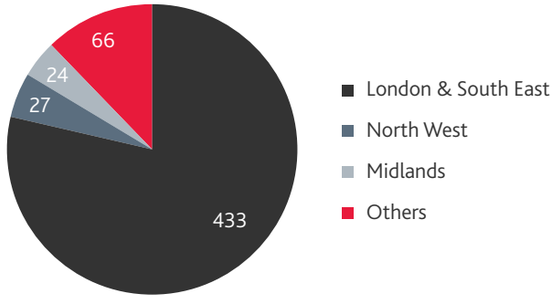
Spotlight on regional fraud

Fraud is not evenly distributed across the UK, with certain regions emerging as key hotspots for fraudulent activity. The top three fraud hotspots in 2024 were:

- **London and the South East** made up 79% of the total reported fraud value. This region has consistently been among the top three fraud hot spots over the last five years. However, the 58 cases reported in 2024 mark the lowest number recorded since 2020
- **The North West** was the second most prevalent region for reported fraud value, with £27 million or 5% of the total reported fraud value. This included a £19 million fraudulent investment scheme run by a Blackburn man
- **The Midlands** region is ranked third, accounting for 4% of the total reported fraud value. This included a case against a Worcester based supervisor, alleging around 4,000 fraudulent furlough claims totalling £7 million.

Identifying these hotspots is key to developing more effective fraud prevention and detection strategies, helping businesses become better prepared in the face of evolving threats.

Figure 7: Total monetary value of fraud cases by location in 2024 (£m)



Predictions

Fraud remains a widespread and deeply concerning global issue, impacting every country and region and posing a major threat to consumers and businesses across all industries. However, its true scale is often masked, whether due to the level of undetected or unreported cases, or delays in prosecutions caused by ongoing court backlogs and lengthy complex investigations.

Looking forward into 2025 and beyond, the key themes and fraud trends we expect to see include:

1 Artificial intelligence (AI)

Like any technology, AI can be misused and this is especially true when it comes to fraud. We have seen a huge step forward in the capability and accessibility of AI tools in recent times and that trend is expected to continue to offer fraudsters massive opportunities for technology-enabled fraud schemes. A recent survey by NatWest found that AI voice cloning scams appeared to be one of the fastest growing types of fraud in 2024, having targeted up to 30% of respondents.[6]

Synthetic identity fraud is also expected to become even more commonplace. Here, fraudsters create new identities based on stolen data from genuine individuals, that is then enhanced through generative AI. These scams often involve creating fake social media profiles, which are becoming increasingly challenging to detect.

Fraudsters will continue leveraging AI to increase the scale and success of their schemes. The challenge for the anti-fraud community is to harness AI prevention and detection while staying ahead of emerging threats. While technology already plays a crucial role in fraud risk management and fraud detection, there is still much more it could be doing. Automation can help in many areas, from data analytics and identifying suspicious transaction patterns, to AI driven risk assessment and detecting discrepancies between customer profiles and transaction behaviours.

In the BDO Fraud Survey 2024, we found:

- **17%** of businesses had increased IT security investment
- **14%** took specific steps to ensure their business data was more secure
- **13%** of businesses reported increased spending on fraud detection tools such as AI and data analytics.

These findings suggest that whilst some businesses have been proactive in their investment in technology, there appears to be considerable scope for others to step up their commitment to IT security.

The boom in the development of AI technology remains a double-edged sword in the fraud arena, serving as both a powerful tool for detecting and preventing fraud while also being a potential enabler. Which of these two competing adversaries will be most successful in utilising AI technology will have a big impact on shaping the results of future FraudTrack findings.

"Legislations such as the new ECCTA and the UK Companies Act are pivotal in shaping the landscape of financial crime detection and prevention. ECCTA's requirements for enhanced due diligence, suspicious activity reporting, and rigorous record-keeping align with the proactive approach needed to combat financial crime. These activities, coupled with risk assessment and training, can help businesses to identify and mitigate potential threats. Similarly, the Companies Act requires financial reporting, audits, and internal controls, fostering transparency and accountability. Together, these Acts drive the adoption of data analytics and AI as essential tools for fraud detection and prevention. By leveraging fraud scenario modelling and generative AI, companies can anticipate and counteract financial crime, staying ahead of potential misuse. This integration of technology with legislation and regulatory requirements positions data analytics and AI as key market drivers, ensuring robust defences against financial crime."

Marc Stephens
Partner
Forensic Accounting and Data Analytics

[6] Fastest growing scams of 2024 revealed, NatWest Group

Predictions

Continued

2 Organised cybercrime

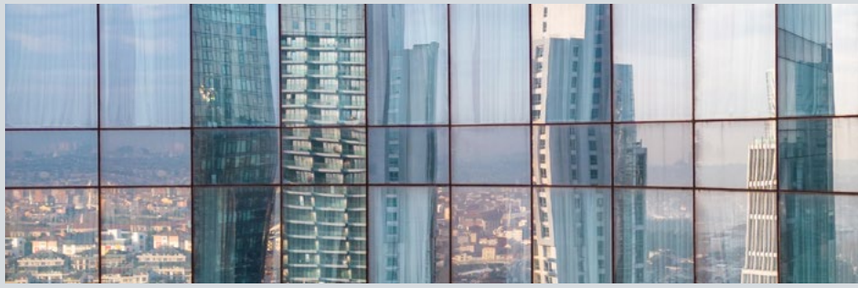
Organised cybercrime is a growing concern. As we move forward, the impact of these criminal activities is likely to increase, demanding more robust responses and strategies.

Technological developments have made it significantly easier for fraudsters to automate and scale up their deceptive practices. Fraudsters now have access to powerful AI tools, automation software and huge volumes of stolen data, enabling them to execute fraud on an unprecedented scale.

Fraud farms are expected to continue to represent a growing threat. These operations employ low-paid workers to carry out fraudulent activities in bulk, from manipulating social media, for example with fake reviews, to using stolen credentials for financial fraud.

The increased use of online payment technologies and e-commerce also present evolving risks, providing cyber criminals and fraudsters with new ways to scam victims, launder money and avoid detection. Even as fraud prevention measures improve, criminals will continue to find and exploit emerging weaknesses, whether through targeting individuals with highly personalised phishing attacks, or using chatbots to impersonate businesses and government agencies.

Without robust detection strategies, stronger regulation, and cross-border collaboration, the scale and complexity of organised cybercrime will likely continue to grow and prosper.



"Organised cybercrime has evolved into a sophisticated global enterprise, mirroring the efficiency, structure, and precision of legitimate organisations. Criminal networks now utilise advanced AI, deepfake technology, and real-time social engineering through chat apps and video calls, to execute highly convincing scams. Traditional email phishing has transformed into pinpoint attacks on platforms like Teams, WhatsApp, and through voice cloning, while fraud farms power mass operations, from fabricating online engagement to abusing stolen credentials. Despite advances in detection, cybercriminals adapt swiftly, exploiting weaknesses in digital payment systems and e-commerce with alarming effectiveness. Countering this rising threat demands more than cutting-edge tools, it requires agile, intelligence-led defence strategies and strong international cooperation to match an ever-evolving, relentless adversary."

Vijay Velu
Global Head of Offensive security/DFIR services

New legislation and regulations for tackling fraud

There have been a number of developments in fraud-related bills and legislation in recent years, which are expected to shape the actions and attitudes of both businesses and individuals moving forward. These include:

- **The new "failure to prevent fraud" offence within ECCTA** aims to drive stronger fraud prevention measures in organisations by holding businesses accountable if they benefit from fraudulent actions committed by their employees. While the act has not yet fully come into force, many organisations have already started to enhance their fraud risk assessment and management processes in anticipation of its implementation
- **ECCTA** also now requires companies to disclose their ultimate beneficial owners, which aims to enhance corporate transparency. The regulatory framework for crypto assets has also expanded to include enhanced due diligence measures and extends AML requirements to virtual asset service providers
- **The Money Laundering and Terrorist Financing (Amendment) Regulations 2023**,[7] which came into force in January last year, also introduced changes to customer due diligence measures for UK politically exposed persons (PEPs). These adjustments aimed to streamline the process, ensuring that enhanced due diligence is proportionate to the risk posed by domestic PEPs rather than applying a blanket approach
- **The Public Authorities (Fraud, Error and Recovery) Bill**, introduced in January 2025, looks to strengthen the government's ability to combat fraud and financial losses affecting public authorities. It extends beyond tax and benefits fraud, granting new powers to the DWP to tackle fraud and error in the benefits system and recover overpayment debt[8]
- **New Authorised Push Payment (APP) fraud reimbursement** rules came into effect in October 2024 to address the rising threat of APP fraud, where victims are tricked into transferring money to fraudsters. These rules require banks and payment providers to reimburse victims if they have taken reasonable care and the financial institution has failed to meet fraud prevention standards. The aim is to encourage stronger fraud prevention measures while offering greater protection to individuals, microenterprises, and charities.

Encouragingly, the recent BDO Fraud Survey 2024[9] released in November 2024 reported that 43% of the businesses surveyed have already seen an increase in fraud awareness among employees since the introduction of ECCTA and other fraud prevention legislations. As new legislation and regulations take effect and guidance continues to evolve, the true impact of these on fraud prevention will become clearer, helping to shape the ongoing fight against fraud.

[7] Money Laundering and Terrorist Financing (Amendment) Regulations 2023

[8] https://commonslibrary.parliament.uk/research-briefings/cbp-10183/

[9] BDO Fraud Survey 2024, page 12

Does your business need help investigating or detecting and preventing fraud and financial crime?

We can help you understand the specific risks relevant to your business and develop best practice procedures and solutions to protect you against the threat of economic crime.

If you suspect that your business has been a victim of fraud, we can conduct rapid response forensic investigations putting you in a position to make timely, reasoned decisions and advise on crisis management.

Stephen Peters
Partner, Head of Investigations
Forensic Accounting
+44 (0)20 7893 2790
stephen.peters@bdo.co.uk

Karen Bailey-Edwards
Director
Forensic Accounting
+44 (0)20 3219 4871
karen.edwards@bdo.co.uk

Richard Shave
Director
Forensic Accounting
+44 (0)20 7893 3546
richard.shave@bdo.co.uk

FOR MORE INFORMATION:

STEPHEN PETERS
+44 (0)20 7893 2790
stephen.peters@bdo.co.uk

RICHARD SHAVE
+44 (0)20 7893 3546
richard.shave@bdo.co.uk

KAREN BAILEY-EDWARDS
+44 (0)20 3219 4871
karen.edwards@bdo.co.uk

www.bdo.co.uk

25-02-4040