

FraudTrack 2026

A closer look at the increasing sophistication of UK fraud

IDEAS | PEOPLE | TRUST

BDO

Contents

A word from Stephen Peters 1
2025 fraud trends at a glance 2
Sector impact 4
Fraud detection methods in the UK 5
The changing face of fraud 6
Evolving regulatory and legal landscape 7
Looking ahead to 2026 11

FraudTrack methodology

This report analyses reported UK fraud cases valued at £50,000 and above between 1 December 2024 and 30 November 2025. 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 reflects publicly reported matters and cases meeting our reporting threshold. As forensic accountants, we are typically engaged in higher-value, more complex cases, meaning our case profile may differ from the fraud landscape reflected in broader media reporting or practitioner datasets. Nevertheless, our findings broadly corroborate wider themes observed across sectors.

The reported items included in the data that was collected to identify the key themes in fraud and economic crime matters reported during the current period, as well as providing a basis to compare to reported data from previous years, has not been verified. Whilst attempts have been made to ensure the data underlying FraudTrack's analysis does not include duplicated reported cases, it is acknowledged that any unclear, overlapping or inaccurate reports could potentially affect the accuracy of the trends referred to in FraudTrack.

A word from Stephen Peters

Partner, Head of Investigations, Forensic Services



Looking back at 2025, what stands out is not only the scale of fraud, but its increasing sophistication.

And yet, though complexity continues to increase, at its core the motivations remain strikingly familiar. **Greed, glamour and gambling** continue to sit at the heart of fraudulent misconduct. What's changed is not the human impulse behind fraud, but the finesse with which it is executed. Despite significant advances in detection and prevention, **billions of pounds continue to be lost each year**. The threat is not diminishing – it is adapting.

Across the country, three dominant fraud typologies have shaped the threat environment and placed sustained pressure on enforcement capacity:

- **Social engineering fraud** continues to exploit weaknesses in payment processes and staff awareness
- **Cash and inventory fraud** persists where segregation of duties and control environments are weak
- **Misuse and misappropriation of assets** – from inappropriate expense claims to the deliberate diversion of organisational resources – remains a recurring feature of casework.

Geographically, **high-value fraud remains concentrated in London and the South East**, reflecting the density of financial activity and opportunity. However, no region is left untouched.

Sectoral exposure is equally broad. **Finance and Insurance, Public Administration, and Professional, Scientific and Technical Services** face particular concentration of risk, owing to their reliance on complex financial flows, high-trust environments and large volumes of sensitive data.

Detection frameworks, however, continue to expose structural weaknesses. Police and HMRC are still the bodies most likely to secure prosecutions or convictions, underscoring the central role of public enforcement. At the same time, firms face **heightened regulatory expectations** and increased scrutiny. The evolving legal landscape, combined with assertive enforcement and strategic oversight initiatives such as **HMRC's enhanced reward schemes** and the **Online Crime Centre**, underscores the need for organisations to strengthen internal controls and reporting mechanisms.

External auditors – despite their proximity to financial reporting and control systems – remain among the least likely to detect fraud. The implication is clear: **stronger internal reporting cultures and more integrated oversight mechanisms are essential** if intervention is to occur earlier.

The profile of offenders is equally varied. Individuals span a wide age range, operate across domestic and international borders, and increasingly leverage digital tools that blur the lines between organised crime, opportunistic misconduct and professional fraud networks. The **rapid evolution of fraud methodologies** – now accelerated by artificial intelligence – places sustained pressure on regulators, investigators and organisations alike.

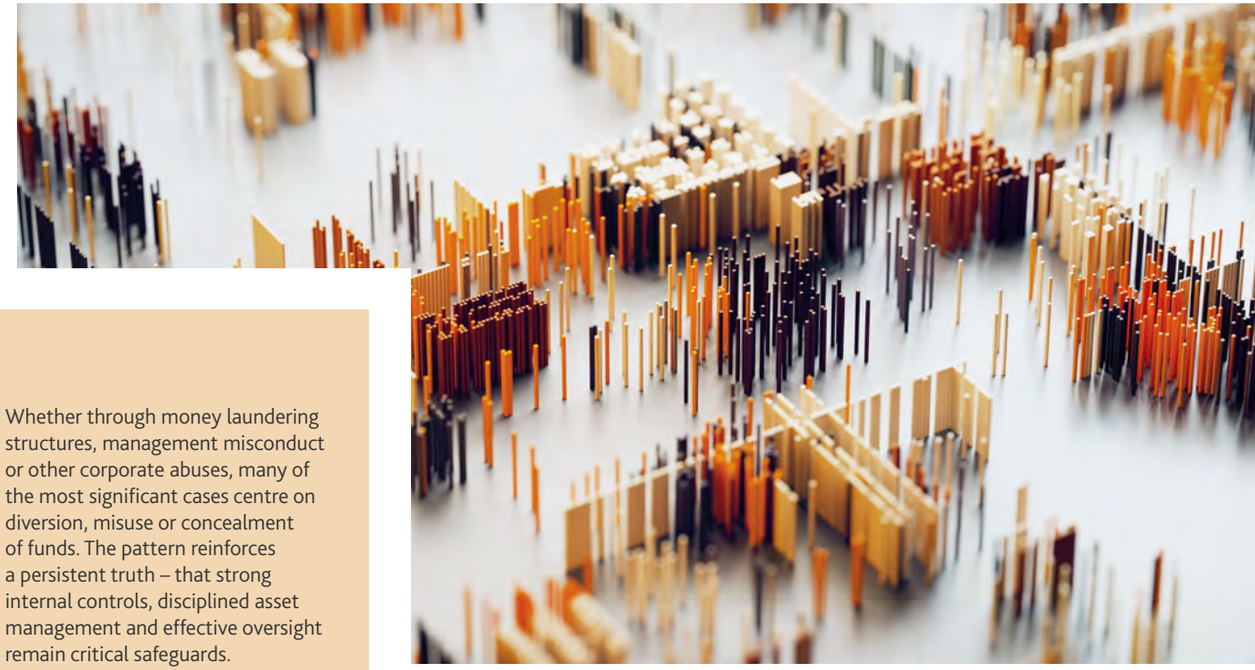
Our own financial crime casework reflects these dynamics. Across retail, manufacturing, and charity and not-for-profit sectors, we continue to observe recurring typologies consistent with the national picture. **Strengthening internal controls, investing in staff training and embedding effective fraud governance frameworks** remain critical steps in reducing exposure.

The direction of travel is unmistakable. **Fraud is becoming more technologically enabled, more adaptive and more resilient**. If regulatory and legal frameworks are to remain effective, they must evolve at pace. Renewed focus, modernised enforcement tools and genuine cross-sector collaboration will be required. Without sustained reform, the financial and societal costs will continue to rise.

Stephen Peters
Partner and Head of Investigations, London

2025 fraud trends at a glance

Billions lost to fraud, five cases dominating – is this the new face of UK fraud?

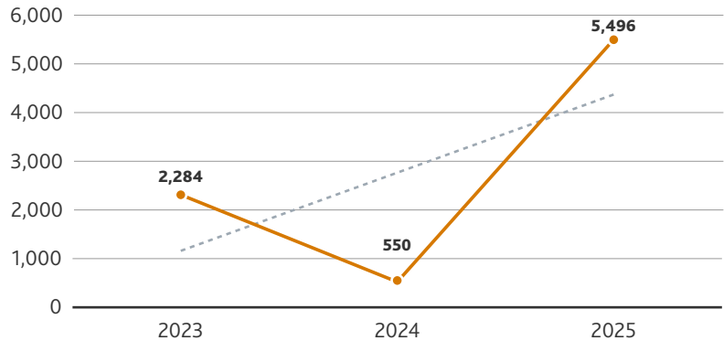


At first glance, 2025 figures appear disproportionate. Reported fraud increased from £550 million in 2024 to £5.5 billion in 2025 – an almost 900% rise in a single year. The three-year trend analysis, illustrated in Figure 1, captures the scale of this shift.

However, the headline figure tells only part of the story. A closer examination reveals that the surge in reported value is driven overwhelmingly by a very small number of cases. Five incidents alone accounted for approximately **94% of the total reported value in 2025.**

While these may be regarded as statistical outliers, they are nevertheless shaping the overall fraud profile for the year. In effect, a handful of exceptional cases have distorted the aggregate picture – though their impact, financial and systemic, is real. Several of these high-impact matters are examined in more detail later in this report.

Figure 1: Total value of reported frauds in last three years (£'m)



The rise of rogue management: UK's fastest-growing risk

Beneath the volatility of the headline figures, the underlying fraud categories remain familiar. Money laundering continues to dominate in value terms at £4.9 billion, while non-corporate fraud contributes a further £207 million, reinforcing long-standing patterns in the UK's fraud environment.

One shift, however, stands out. **Management fraud has risen more than seventeen-fold**, increasing from £11 million in 2024 to £195 million in 2025. It has rapidly become a defining feature of this year's data. This escalation signals growing vulnerability within organisational governance and oversight, particularly where senior individuals are able to override or circumvent established controls.

Across these dominant categories, a common thread emerges: the unauthorised use and misappropriation of assets.

Whether through money laundering structures, management misconduct or other corporate abuses, many of the most significant cases centre on diversion, misuse or concealment of funds. The pattern reinforces a persistent truth – that strong internal controls, disciplined asset management and effective oversight remain critical safeguards.



Collectively, these fraud types account for 97% of total reported fraud value in 2025, highlighting both the concentration of financial harm and the importance of targeted intervention.

"2025 marks a pivotal shift in the UK's fraud landscape. While a small number of extraordinary cases have driven the headline figures to historical levels, the deeper concern lies in the convergence of entrenched money laundering activity and the rapid escalation of management driven misconduct. These trends demonstrate how quickly assets can be diverted, concealed and legitimised when governance gaps exist. For global organisations, the message is clear: strengthening control environments, reinforcing oversight and ensuring that no individual, regardless of seniority, can exploit their position is now fundamental to safeguarding financial integrity and maintaining trust across markets."



Fiona Raistrick
Partner
Financial Services Advisory, London

2025 fraud trends at a glance

Continued



Motives behind UK fraud: Greed, Glamour and Gambling

Although the methods used to perpetrate fraud continue to evolve, the underlying motives remain consistent. Greed, the pursuit of a lavish lifestyle and gambling addiction continue to dominate case narratives in 2025.

This year's data shows a marked escalation in fraud linked to lifestyle ambition. Frauds associated with lavish spending **rose almost 140-fold**, increasing from **£36 million in 2024 to £5 billion in 2025**. Gambling-motivated offences also doubled over the same period, rising **from £5 million to £11 million**. These patterns suggest that fraud is moving from opportunistic to calculated.

In many cases, individuals committed offences to sustain lifestyles far beyond legitimate means or to pursue the perceived highs associated with gambling. Behind each case lies a complex mixture of pressure, desire and temptation. While economic strain may be a factor in some instances, the 2025 data reinforces that financial crime is frequently motivated by ambition rather than necessity.

High-value fraud persists across multiple UK regions

Fraud in 2025 remains geographically concentrated, though operationally diverse. Five regions account for the majority of reported value, with London and the South East continuing to dominate as the UK's primary fraud hotspot. Indeed, this region alone accounted for more than a quarter of all reported cases and **over 90% of total reported value**. The figures were driven both by volume and by exceptionally high-value incidents, including a £4.8 billion cryptocurrency money laundering scheme.

Yorkshire experienced one of the most significant shifts year-on-year. Rising from eighth place[1] in 2024 to second in 2025, the region reported **nearly £200 million in losses**. This surge was fuelled by major cases, including a £120 million cryptocurrency money laundering operation and a £32 million cyber-enabled fraud.

The Midlands and North West each reported values close to **£110 million**, largely driven by management-related and tax-related offences. Scotland completes the top five, with total reported losses approaching **£20 million**, primarily involving individuals, tax fraud and money laundering.

Together, these patterns demonstrate a fraud landscape that remains geographically concentrated but increasingly complex. Several regions appear to be experiencing sustained high-impact activity, reinforcing the persistence and evolution of large-scale fraud across the UK.

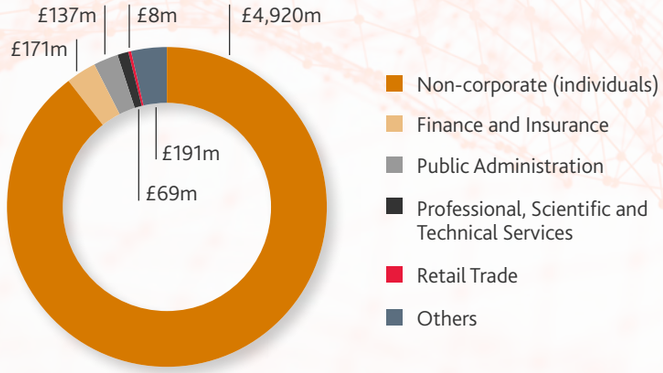
[1] "Place" refers to the position of a region when all regions are ordered from highest to lowest based on the total value of reported fraud. A higher rank means the region had reported more fraud value than others.

Sector impact

The UK Fraud Landscape in 2025

Examining the available industry data[2] reveals clear patterns in victimisation across sectors. In 2025, individuals became the largest victim group, followed by Finance and Insurance,[3] Public Administration,[4] and Professional, Scientific and Technical Services.[5] Collectively, these sectors accounted for 96% of all reported fraud value.

Figure 2: Total value of fraud losses by sector in 2025 (£'m)[6]



Individuals

Individuals accounted for **£4.9 billion** in reported losses in 2025, reflecting the continued rise of scams exploiting personal trust, digital communication channels and financial vulnerability.

The most prevalent threats included false advertising, social engineering attacks and investment fraud. These schemes rely heavily on behavioural manipulation, often combining emotional influence with increasingly sophisticated digital techniques. The scale of loss reinforces the persistent targeting of individuals by organised networks operating at volume.

Finance and Insurance

The Finance and Insurance sector reported losses of **£171 million**, continuing to rank among the highest-risk sectors.

The sector's exposure stems from high-value transactions, digital infrastructure reliance and complex payment flows. Key fraud typologies included phishing attacks, unauthorised use or misappropriation of funds, account takeover attempts and insurance-related fraud.

The concentration of risk within this sector highlights the need for strengthened authentication protocols, continuous monitoring and enhanced cyber resilience.

Public Administration

Public Administration reported **£138 million** in losses, largely driven by tax-related fraud, VAT diversion and avoidance, fraudulent tax rebate claims and misuse of public benefits.

Many schemes involved the creation of front companies and the use of stolen identities to exploit the scale and complexity of public systems. The breadth of activity in this sector underscores the importance of modernised data analytics, cross-agency information sharing and sustained regulatory vigilance.

Professional, Scientific and Technical Services

This sector recorded **£69 million** in reported losses. In many cases, fraud was perpetrated internally, involving employees or managers abusing positions of trust through invoicing schemes or misappropriation of company funds.

The prominence of internal actors reinforces the importance of segregation of duties, internal audit robustness and strengthened governance oversight within professional environments.

[2] Insufficient source data meant that £157 million value in reported cases could not be attributed to a sector. The analysis includes only those with clear sector information.
[3] Finance and Insurance refer to organisations that deliver a range of financial services, including banking, insurance (life, health, and other coverage), and related auxiliary financial and insurance services.
[4] Public administration refers to organisations owned, funded or controlled by the government which are responsible for implementing public policy and aim to provide essential services and support to society. These includes local councils and public agencies, such as His Majesty's Revenue and Customs (HMRC) and Department for Work and Pension (DWP).
[5] Professional, Scientific and Technical Services refers to organisations which sell specialised services, such as legal, accounting, architectural, engineering, IT, scientific research, and advertising services.
[6] For completeness, "Others" includes: (i) Accommodation and Food Services; (ii) Administrative, Support, Waste Management and Remediation Services; (iii) Agriculture, Forestry, Fishing and Hunting; (iv) Arts, Entertainment and Recreation; (v) Charity; (vi) Construction; (vii) Educational Services; (viii) Health Care and Social Assistance; (ix) Information; (x) Manufacturing; (xi) Other Services (except Public Administration); (xii) Real Estate and Rental and Leasing; (xiii) Transportation and Warehousing; (xiv) Utilities; (xv) Wholesale Trade; and those reported cases that could not be attributed to a specific sector.

Fraud detection methods in the UK

In 2025, fraud detection methods[7] across the UK continued to rely heavily on reactive mechanisms. The data paints a clear picture: financial crime is often uncovered only after significant harm has already occurred, rather than prevented at source.

Law-enforcement-led detection remained central. The police uncovered **£5 billion across 82 cases**, playing a pivotal role in dismantling large-scale operations. Their investigations exposed complex schemes, including a management-led investment scam that specifically targeted elderly victims. These cases demonstrate both the scale of organised financial crime and the critical importance of investigative capacity.

His Majesty's Revenue and Customs (HMRC) also played a significant role, pursuing **11 cases** valued at nearly **£100 million**. These investigations focused primarily on tax evasion, money laundering activity and fraudulent benefit claims. One notable case involved £22 million in reported losses, resulting in the conviction of seven individuals for offences including cheating the public revenue. Four were subsequently issued 10-year director disqualification orders. Such outcomes highlight the essential role of regulatory enforcement in protecting public funds and maintaining confidence in the system.

Sentencing data further illustrates the seriousness with which detected fraud is punished. Police-led cases resulted in average custodial sentences of over three and a half years, while those arising from HMRC investigations averaged over four years.[8] When fraud is successfully identified and prosecuted, the consequences are substantial, which reinforces the powerful deterrent of effective detection.

Within organisations, **internal audit identified £9 million across 35 cases**. This highlights the critical role of strong governance frameworks and proactive internal oversight.

Beyond these primary detection pillars, the 2025 data highlight a wider ecosystem of supplementary detection mechanisms. While smaller in scale, they collectively contribute to the UK's broader fraud defence infrastructure. These include:

- Trading Standards detected £12 million
- Management-led identification accounted for £4.3 million
- Staff reports uncovered £2.4 million
- Victim-led detection contributed £4.3 million.

Together, these channels demonstrate the value of a broad, multi-layered defence model in countering both sophisticated and lower-complexity fraud threats.

External audit: limited role in fraud detection

Notably, external audit identified only three of the 359 frauds reported in 2025, representing **less than 1%**. This reinforces a longstanding view that external audit is not an effective primary mechanism for detecting or deterring fraud.

The finding is consistent with the Association of Certified Fraud Examiners' (ACFE) 2024 Occupational Fraud Report,[9] which reports that external auditors detect approximately **3%** of occupational fraud cases.[10] Earlier ACFE studies in 2020[11] and 2022[12] recorded similar results, with detection rates of around **4%**. The pattern is therefore not new – reliance on external audit as a frontline fraud-detection tool has repeatedly proven limited.

There are structural reasons for this constrained role. External audits are primarily designed to assess financial statement accuracy and compliance with accounting standards, rather than to uncover concealed or complex fraud schemes. While fraud risk assessment procedures are required under International Standards of Auditing (ISA),[13] these procedures do not equate to specialist forensic investigation and are not intended to provide absolute assurance against fraud.



"Internal audit continues to be one of the most reliable lines of defence, but its impact is constrained when organisations underinvest in continuous monitoring, analytics, and integrated fraud risk management."



Cherry Cromarty
Partner
Risk Advisory, London

These findings underscore the importance of integrated detection strategies that combine regulatory bodies, law enforcement, strong internal controls, whistleblowing frameworks and public vigilance. A more intelligence-led and coordinated approach will be essential to reduce reliance on chance discovery and to strengthen the UK's overall resilience to financial crime.

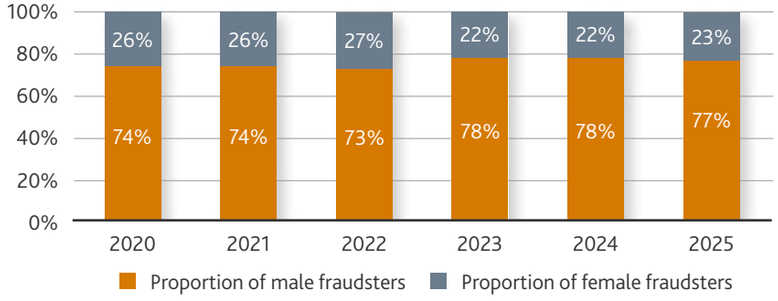
[7] The fraud-detection methods used included the Police, HMRC, Trading Standards, internal audit, victim identification, management identification, staff, chance, surrender, external audit, whistleblower.
[8] Data for sentencing was unavailable for some of the cases detected by the police and HMRC. Therefore, our analysis is based on a subset of cases where sentencing data was reported.
[9] Association of Certified Fraud Examiners' Occupational Fraud 2024: A Report to the Nations, page 24.
[10] Association of Certified Fraud Examiners describes Occupational Fraud as fraud committed by individuals against their employer, and is split into three primary categories: corruption, asset misappropriation, and financial statement fraud.
[11] Association of Certified Fraud Examiners' Report to the Nations 2020 Global Study on Occupational Fraud and Abuse, page 19.
[12] Association of Certified Fraud Examiners' Occupational Fraud 2022: A Report to the Nations, page 22.
[13] International Standards of Auditing, 240R, The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements.

The changing face of fraud

The 2025 data challenges any narrow assumptions about who commits fraud. While men continue to dominate reported cases, women are far from absent. The single largest fraud by value involved a woman in London charged with laundering Bitcoin – a reminder that high-value financial crime is not confined to one demographic profile.

Age patterns are equally revealing. **Offenders range from eighteen years of age to their late eighties**, demonstrating that fraud is not restricted to any particular stage of life.

Figure 3: Gender demographics of fraudsters over the last five years



At one end of the spectrum

An 85-year-old man received a two-year prison sentence for a management fraud that defrauded more than 100 investors of £1 million through his company.

At the other

A 37-year-old man in Yorkshire was charged with laundering over £120 million in cryptocurrency – the second largest fraud value reported in 2025.

Although no single dataset captures a complete demographic picture, Cifas[14] data on 'money muling'[15] (a common form of money laundering) provides additional context. Among identified offenders, **57% were aged 30 or under**,[16] while **41% fell within the 31–60 age range**. The contrast between these proportions and the high-value cases observed in our dataset likely reflects structural differences: many money muling incidents involve comparatively low financial values,[17] and underreporting persists across fraud categories.

What emerges is not a single archetype, but a spectrum. Men appear more frequently in reported cases, yet women are responsible for some of the largest losses by value. Young adults and pensioners alike feature in the data. Fraud in the UK does not belong to one age group, one gender or one background – it belongs to opportunity.



[14] Cifas is a fraud prevention service in the UK. It is a not-for-profit membership association representing organisations from across the public, private and voluntary sectors.
[15] According to the UK's National Crime Agency *money muling* happens when someone moves criminal money for others, sometimes for payment.
[16] https://www.fraudscape.co.uk/#6-month within the Cifas main website https://www.cifas.org.uk/newsroom/fraudscape-2025-record-fraud-levels.
[17] FraudTrack data collection is for reported frauds valued at £50,000 and over.

Evolving regulatory and legal landscape

In 2025, UK fraud data underscores a pivotal shift in regulatory and legal frameworks, sharpening the focus on financial crime, corporate misconduct, and emerging risks. This evolution is occurring amid intensified regulatory pressure, marked by the introduction of new corporate offences and significant reforms across supervisory and enforcement structures.

Rather than incremental adjustment, 2025 reflects structural change – a tightening of expectations around governance, prevention, and accountability.

Regulatory pressure intensifies

Regulatory pressure increased significantly following the introduction of the **Failure to Prevent Fraud offence**, which came into force on 1 September 2025 under the Economic Crime and Corporate Transparency Act 2023 (ECCTA).[18]

This new offence materially raises the stakes for large organisations, which can now be prosecuted if:

- They do not have reasonable prevention procedures in place
- An associated person commits a specified fraud offence that benefits the organisation.

The definition of an "associated person" is deliberately broad. It includes subsidiaries, employees, agents and other third parties acting on behalf of, or in business with, the organisation. This expansive definition makes it essential for firms to understand where external misconduct could create liability exposure.



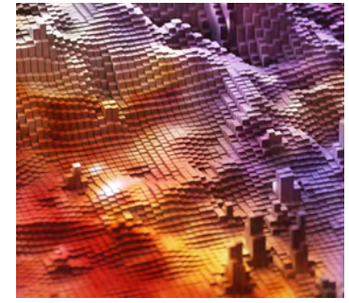
For example, if a contractor pays bribes to secure commercial contracts that benefit the organisation, the organisation may be held liable unless it can demonstrate that reasonable procedures were in place to prevent such conduct. This includes evidencing appropriate due diligence and controls when onboarding and managing contractors and suppliers.

While the offence applies to large organisations, it also captures non-UK entities with a UK connection, provided the group meets the statutory size threshold.

The wider regulatory environment

Beyond ECCTA, the broader regulatory landscape in 2025 reflects tightening oversight across **crypto assets**, **anti-money laundering (AML) supervision**, **fraud-enabling technologies**, and **whistleblowing incentives**.

Taken together, these developments show regulators moving rapidly to close gaps, address emerging risks, and align supervisory expectations with technological innovation.



Increased focus on crypto assets

On 2 September 2025, HM Treasury published The draft **Money Laundering and Terrorist Financing (Amendment and Miscellaneous Provisions) Regulations 2025**.[19] Among other updates, the draft introduced several changes affecting crypto asset business regulation.

The draft amendment proposed:

- Lowering the ownership change notification threshold for crypto asset firms **from 25% to 10%**
- Requiring enhanced due diligence for crypto-related correspondent relationships
- Prohibiting relationships with shell banks.

These measures form part of a broader effort to bring crypto assets more firmly within the regulatory framework established under the Financial Services and Markets Act.[20]

New cryptoassets regulatory framework

The UK is also advancing a comprehensive regulatory framework for crypto assets following the announcement of the draft **Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2025**. This statutory instrument is scheduled to come into force on 25 October 2027.

Under this framework, any firm undertaking newly regulated crypto asset activities will be required to obtain authorisation from the Financial Conduct Authority (FCA).

The legislation will introduce a dedicated regime covering admissions, disclosures, and market abuse for crypto assets, aligning the treatment of crypto markets more closely with traditional financial markets.

Collectively, these measures aim to strengthen market integrity by addressing fraud and financial crime risks while embedding crypto assets within established regulatory standards.[21]

[18] Economic Crime and Corporate Transparency Act 2023: Guidance to organisations on the offence of failure to prevent fraud (accessible)
[19] https://www.gov.uk/government/publications/proposed-amendments-to-the-money-laundering-regulations-draft-si-and-policy-note/the-draft-money-laundering-and-terrorist-financing-amendment-and-miscellaneous-provision-regulations-2025-policy-note.
[20] https://www.fca.org.uk/firms/new-regime-cryptoasset-regulation.
[21] https://www.fca.org.uk/publications/consultation-papers/cp25-41-regulating-cryptoassets-admissions-disclosures-market-abuse-regime-cryptoassets.

Evolving regulatory and legal landscape

Continued

Centralising AML supervision

One of the most significant AML reforms announced in 2025 is the UK Government's decision to **overhaul the current supervisory framework**.

Under the new model, responsibility for AML and counter-terrorist financing (CTF) supervision will be **removed from 22 existing professional body supervisors**. A new body – the Single Professional Services Supervisor – will give the FCA direct oversight of legal, accountancy, and trust and company service providers for compliance with the Money Laundering Regulations.

The FCA will also work more closely with the wider professional services sector, other regulators, and law enforcement agencies to strengthen the UK's defences against money laundering and terrorist financing.



This reform aims to:

- Reduce fragmentation in the supervisory landscape
- Improve consistency and quality of oversight
- Strengthen enforcement across professional services
- Enhance information-sharing across the UK's AML ecosystem.

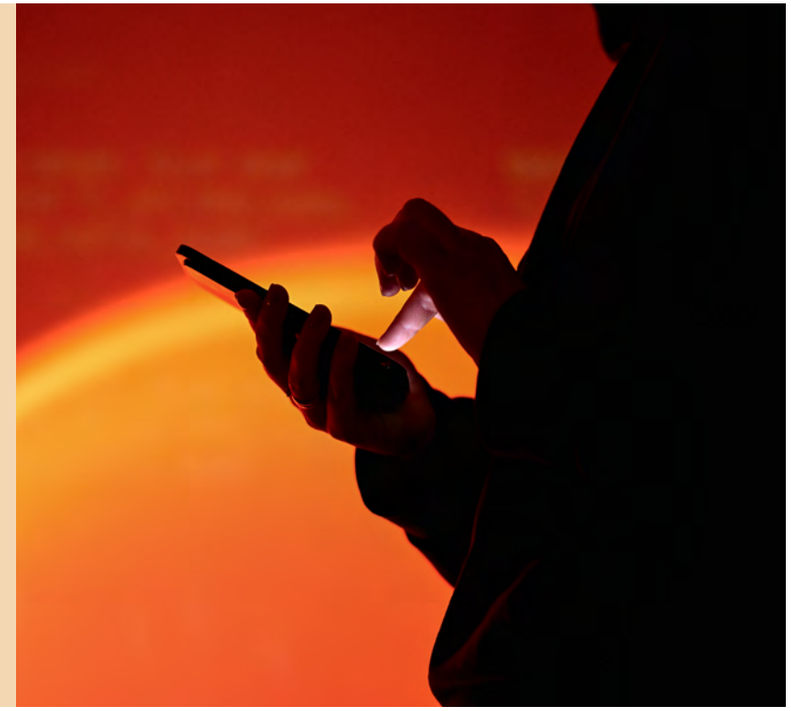
The direction of travel is clear: consolidation, consistency, and stronger central accountability.

Ban on SIM farms

In April 2025, the UK Government announced plans to ban the possession and supply of SIM farms,[22] making the UK the first country in Europe to introduce such a prohibition. The announcement followed data showing fraud **rising 19% in the year ending September 2024**[23] and accounting for around **40% of all reported crime** in England and Wales.

SIM farms – devices capable of holding dozens or hundreds of SIM cards – are widely used to send mass spam and phishing messages, facilitate account takeover attempts, and mask identities behind automated fraud campaigns.

Once the ban comes into force, possession or supply of a SIM farm without legitimate reason will constitute a criminal offence. The measure is intended to provide law enforcement with stronger tools to disrupt large-scale fraud infrastructure.



Public Authorities (Fraud, Error and Recovery) Act 2025

The Public Authorities (Fraud, Error and Recovery) Act received Royal Assent on 2 December 2025.[24] The legislation is designed to safeguard taxpayers' money by strengthening the ability of public bodies to identify, prevent and deter fraud and error across the public sector.

Under the Act, the Department for Work and Pensions (DWP) gains access to new data sources, modern analytical tools, and enhanced investigative powers to recover losses from benefit overpayments. This includes the ability to obtain relevant data from banks and financial institutions.

Access to this information is intended to ensure claimants receive appropriate support, reduce debt risks, and enable more effective detection of fraudulent claims.

[22] Major step for fraud prevention with landmark ban on SIM farms
[23] NSA 2025 - Fraud - National Crime Agency
[24] Fraudsters face tougher action as Government gains new powers to tackle benefit fraud

Evolving regulatory and legal landscape

Continued

Stronger whistleblower incentives

In November 2025, an enhanced reward scheme was introduced as part of efforts to reduce the tax gap.[25]

HMRC's Strengthened Reward Scheme is designed to encourage reporting of tax avoidance and evasion. Individuals who provide information leading to successful recovery of unpaid tax may receive a discretionary **reward of between 15% and 30%** of the tax collected, **where recoveries exceed £1.5 million**.

This represents a significant increase in available incentives and forms part of a broader strategy to intensify investigations into individuals and companies suspected of non-compliance.

"The strengthened HMRC reward scheme marks a significant shift in the UK's enforcement landscape. HMRC is signalling a more assertive stance in tackling avoidance and evasion. For businesses, this raises the bar on governance, transparency, and internal controls. Organisations should assume that any concern not escalated internally may now be escalated directly to HMRC."



David Lewis
Partner
Tax Dispute Resolution, London



UK Government launches new fraud strategy and online crime centre

In March 2026, the Secretary of State for the Home Department presented the Fraud Strategy 2026-2029 to Parliament. The key strategic objective is to combat crime, bolster economic resilience, and ensure justice. Recognising fraud as the most prevalent crime in England and Wales, the strategy addresses its impact on national security and economic stability.

It is structured around three key pillars: **DISRUPT**, **SAFEGUARD**, and **RESPOND**. The **DISRUPT** pillar aims to prevent criminals from accessing exploitable tools and systems, featuring initiatives like the Online Crime Centre and the Global Fraud Summit. **SAFEGUARD** focuses on enhancing resilience and reducing vulnerability through campaigns such as *Stop! Think Fraud* and support for cyber resilience centres. **RESPOND** seeks to improve victim support, strengthen law enforcement capabilities, and foster international cooperation.

Governance and accountability are central to the strategy, with leadership from the Home Office and collaboration with various stakeholders. Progress and effectiveness will be monitored using metrics and data, ensuring alignment with broader national security and crime prevention strategies.

In April 2026, The UK government launched a new **Online Crime Centre**, aimed at combating fraud through collaboration with government bodies, police, intelligence agencies, banks, mobile networks, and tech firms. This initiative is part of the broader fraud strategy and is backed by a £250 million investment over three years, designed to disrupt fraudsters and safeguard the public. The Online Crime Centre will focus on identifying and shutting down accounts, websites, and phone numbers used by organised crime groups, particularly targeting high-harm offenders.

The strategy aims to enhance data sharing between police and companies to develop a comprehensive understanding of global fraud networks. **International cooperation is emphasised**, with existing agreements with Nigeria and Vietnam leading to arrests and the dismantling of scam operations. The strategy also includes deploying AI to detect emerging fraud patterns, halt suspicious bank transfers, and utilise chatbots for intelligence gathering.



Victims will receive enhanced support through national standards for treatment, a fraud victims charter, and targeted prevention efforts in fraud hotspots. The strategy seeks to **expedite court processes and strengthen civil powers** to ensure swifter justice and tougher penalties for fraudsters. The Online Crime Centre will eventually integrate with the National Police Service to spearhead the national fight against fraud. Overall, the strategy underscores a coordinated, technology-driven, and international approach to counter the global threat of fraud, with shared responsibility among government, regulators, law enforcement, and industry.

[25] Reporting serious tax avoidance or evasion

Evolving regulatory and legal landscape

Continued

International perspective: US enforcement developments

In February 2025, an Executive Order triggered a temporary pause in U.S. Department of Justice (DOJ) enforcement activity under the Foreign Corrupt Practices Act (FCPA).

When enforcement resumed in June 2025, revised guidance narrowed prosecutorial focus to matters tied to U.S. national security or economic interests and prioritised serious, high-impact misconduct.

Simultaneously, the DOJ expanded its Corporate Whistleblower Awards Pilot Program,[26] increasing incentives for early self-reporting.

These developments reflect a more selective but strategically focused enforcement posture, placing renewed emphasis on internal detection, disclosure mechanisms and cross-border compliance management.

Comment from Glenn Pomerantz

Glenn Pomerantz, BDO's Global Forensic Leader who is based in the United States, confirms the significant shifts in regulatory enforcement priorities – especially those of the DOJ and SEC, "there can be no mistaking the administration's feelings towards, and influence on, financial regulatory enforcement including virtually no SEC enforcement matters, a significant slowdown in SEC whistleblower driven cases and a titanic shift away from SEC and DOJ FCPA cases." However, one should not dismiss the threat of fraud – occurrences of crimes against companies still proliferate and organisations are still paying attention to regulatory compliance despite the slowdown in enforcement. Additionally, civil matters related to fraud continue at a strong pace as do investigations and compliance, specifically related to digital assets and in everything to do with two sectors; healthcare and financial services.



Glenn Pomerantz
Principal
Global Forensics Practice Leader, New York, US

Consequences of the Evolving Regulatory Landscape

These revisions to legal and regulatory frameworks across borders, not only in the UK and the US but also in countries such as Vietnam and Nigeria – where existing agreements have led to arrests – makes it unmistakably clear that firms face heightened pressure to enhance governance, strengthen monitoring capabilities, and adapt to a more assertive and strategically focused regulatory environment.

[26] https://www.justice.gov/criminal/criminal-division-corporate-whistleblower-awards-pilot-program.

Looking ahead to 2026

The signals emerging from 2025 are already shaping the fraud landscape of 2026. This is reflected in the UK Government's Fraud Strategy 2026-2029, presented to Parliament in March 2026, and the new Online Crime Centre launching in April 2026.

The first months of 2026 confirm what 2025 data indicated: fraud is evolving in real time, and organisations must adapt just as quickly. Viewed through this lens, **2026 is not a reset but a continuation** of the patterns, anomalies, and behavioural shifts that intensified throughout 2025.

The fraud risk playbook is being rewritten through technological acceleration.

AI makes fraud faster, cheaper and harder to detect

AI is increasingly shaping the evolution of fraud. As tools become more widely accessible, they enable more personalised, automated, and sophisticated schemes.

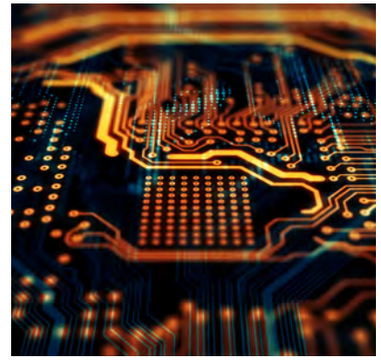
Existing and emerging AI-enabled methods include:

- Voice cloning
- Deepfake impersonation
- Synthetic identities
- Automated phishing and webpage generation.

These techniques allow fraudsters to scale traditional schemes with greater efficiency and realism.

Recent cases illustrate this shift. In 2025, a technology student was convicted for selling phishing kits used to scam victims out of **£100 million**. These kits included fake webpages designed to harvest login credentials and bank details. The case demonstrates how accessible AI-driven tooling can amplify familiar fraud methods, lowering barriers to entry while increasing impact.

Media reporting throughout early 2026 has highlighted a surge in hyper-realistic AI-enabled scams, reflecting the speed with which these technologies are being operationalised.



Deepfakes and business exposure

Deepfakes – AI-generated audio, video, images, and text that closely mimic real individuals – have become an acute fraud risk. Their realism increases the risk of executive impersonation, authorisation fraud, and misleading communications.

According to BDO's 2025 Financial Investigations Survey,[27] almost **one-quarter of respondents** reported being targeted by deepfake-related activity.

Because deepfakes appear to originate from trusted leaders or colleagues, employees may act quickly without verification, increasing exposure to financial loss and operational disruption.

Fighting fire with fire

AI is not solely a threat vector. It is also becoming central to fraud detection.

BDO's Financial Investigation Survey notes that **27%** of the businesses surveyed increased investment in fraud detection tools during 2025, including AI and advanced data analytics, reflecting a growing reliance on technology to identify anomalies, detect emerging threats, and protect operations.

Government data further illustrates the scale of the challenge. In 2025, approximately **eight million deepfakes**[28] were shared online, compared with around half a million two years earlier. This dramatic increase has made it significantly more difficult for individuals and organisations to distinguish genuine content from manipulated material, increasing scam risk and eroding trust in digital communications. In response, the UK Government has been actively harnessing AI-detection tools and has reportedly prevented fraudsters from stealing **hundreds of millions of pounds**[29] through enhanced technological safeguards.

The strategic importance of this technological shift was highlighted at the International Anti-Fraud Summit in London in September 2025, where the focus centred on deploying cutting-edge AI and data tools to stay ahead of fraudsters and protect public funds. This momentum has continued into 2026, with the Government Office for Science announcing a world-first deepfake detection evaluation framework, built in collaboration with technology companies, academics, and government specialists to strengthen the UK's ability to detect synthetic media and mitigate AI-enabled fraud.

[27] BDO's Financial Investigations Survey 2025 is sector agnostic and based on responses received from 500 senior business leaders from entities with 200 or more employees, providing real-time experiences across the UK business landscape.
[28] https://www.gov.uk/government/case-studies/science-led-collaboration-against-deepfakes.
[29] https://www.gov.uk/government/news/record-fraud-crackdown-saves-half-a-billion-for-public-services#:~:text=Announcing%20the%20record%20figures%20at%20an%20anti%2Dfraud,Minister%20Josh%20Simons%20said:%20Working%20people%20expect.



Looking ahead into 2026

Continued

Fraudsters adopting full automation

In 2026, organisations should anticipate a continued surge in AI-enabled fraud, particularly impersonation-based attacks.

Threat actors are advancing the use of deepfake technologies, voice cloning tools, and automated phishing kits, creating highly convincing and scalable social-engineering campaigns. This next wave will blend synthetic media with automated harvesting techniques, challenging traditional controls and detection systems.

The trajectory set in 2025 leaves little doubt: fraud risk is becoming more technologically sophisticated, more scalable, and more difficult to detect.

"Fraud in 2026 is simply the 2025 threat curve accelerating. AI has weaponised social engineering. Deepfakes, cloned voices, synthetic identities, and automated phishing kits are now standard tools. Attacks are faster, cheaper, and harder to spot. Only organisations that match this automation with AI driven detection and rapid response will keep pace with adversaries who are already operating at scale."



Jason Gottschalk
Partner
BDO Digital | Financial Crime Consulting, London

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

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

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

Copyright © May 2026 BDO LLP. All rights reserved. Published in the UK.

www.bdo.co.uk



26-01-4287